Proceedings of
The 3rd International Conference on
Information Science and Systems
ICISS 2020

March 19-22, 2020
Cambridge, UK

ISBN: 978-1-4503-7725-6

The Association for Computing Machinery
2 Penn Plaza, Suite 701
New York New York 10121-0701

ACM ISBN: 978-1-4503-7725-6

Table of Contents

Proceedings of the 3rd International Conference on Information Science and Systems

Preface

The 3rd International Conference on Information Science and Systems (ICISS 2020) was supposed to be held in Cambridge, UK, March 19-22, 2020. As the 2019-nCoV spreads all over the world, finally it was held online, which is a very unique experience for all the participants.

ICISS is a comprehensive conference which focuses on Information Science and Systems. The main theme of the conference is to address and deliberate on the latest developments and recent trends in the research and applications of Information Science and Systems. The purpose of the conference is to provide an opportunity for scientists, engineers, industrialists, scholars and other professionals from all over the world to interact and exchange their new ideas and research outcomes in related fields. The conference provided a unique opportunity for the participants to develop research collaborations in their respective fields.

ICISS 2020 was technically assisted by Cardiff University, UK; Edinburgh Napier University, UK; University of Salford, UK; Tokai University, Japan; Tokyo City University, Japan and Zhengzhou University of Light Industry, China. In addition to us, the organizing committee also invited two other accomplished experts in related research areas as speakers to give speeches at the conference. They were Prof. Graziano Chesi (IEEE Fellow) from The University of Hong Kong, China and Prof. Xiaodong Liu from Edinburgh Napier University, UK. All participants had the chance to discuss with the speakers online, which provided advice and suggestions to improve their studies and research.

The proceedings of ICISS 2020 contain 40 selected papers from the conference which were presented online and provide comprehensive and state-of-the-art knowledge in this field. In the proceeding, readers can learn cutting-edge knowledge about Information Science and Systems of researchers from different research groups all around the world. Each contributed paper was rigorously peer-reviewed by international reviewers who were drawn from the organizing and advisory committee members as well as other experts in the field from all over the world. The proceedings is divided into 5 chapters based on the different topics of the papers, namely, Software and Data Engineering; Image Intelligent Recognition and Analysis Method; Artificial Intelligence and Intelligent Computing; Internet of Things and Mobile Communication Technology; Computer and Information Science.

On behalf of the organizing committee, we would like to express our sincerely gratitude to all the reviewers for their great professionalism and efforts. A very big thanks all the participants without which the conference would not have taken place. We would like to acknowledge the valuable support and contributions from the sponsors of the ICISS 2020 conference. Let us wish ICISS the same success for next year.

Conference Chairs

Prof. Farid Meziane, University of Salford, UK
Prof. Alexander Balinsky, Cardiff University, UK

March 26, 2020

Conference Committee

Advisory Chair

Prof. Graziano Chesi, IEEE Fellow, The University of Hong Kong, China

Conference Chairs

Prof. Farid Meziane, University of Salford, UK
Prof. Alexander Balinsky, Cardiff University, UK
Prof. Harumi Watanabe, Tokai University, Japan

Program Chairs

Prof. Jamshid Dehmeshki, Kingston University, UK
Prof. Xiaodong Liu, Edinburgh Napier University, UK
Assoc. Prof. Nobuhiko Ogura, Tokyo City University, Japan
Assoc. Prof. Huaiguang Wu, Zhengzhou University of Light Industry, China

Steering Committee

Prof. Yulin Wang, Wuhan University, China
Prof. Dong Hwa Kim, Hanbat National University, South Korea

Technical Committee

Prof. Craig Kuziemsky, University of Ottawa, Canada
Prof. D. Chimgee, National University of Mongolia, Mongolia
Prof. Elcid A. Serrano, Mapua University, Philippines
Prof. Haowei Ti, Hong Kong Asia Business College, Hong Kong
Prof. Hoon Oh, University of Ulsan, South Korea
Prof. Horatiu Dragomirescu, Bucharest University of Economic Studies, Romania
Prof. Issam Moghrabi, Gulf University for Science and Technology, Kuwait
Prof. Jui-Pin Yang, Shih Chien University, Taiwan
Prof. Kazumasa Oida, Fukuoka Institute of Technology, Japan
Prof. Kolyo Onkov, Agricultural University, Bulgaria
Prof. Liudmila Astakhova, SUSU, Russia
Prof. Mary Jane C. Samonte, Mapua University, Philippines
Prof. Phillip Burrell, London South Bank University, UK
Prof. Rafidah Md Noor, University of Malaya, Malaysia
Prof. Ricardus Eko Indrajit, APTIKOM, Indonesia
Prof. S. Kumaran, University of Malaya, Malaysia
Prof. Sumiani Binti Yusoff, University of Malaya, Malaysia
Prof. Tatsuya Akutsu, Kyoto University, Japan
Prof. Tzung-Her Chen, National Chiayi University, Taiwan

Prof. Uma N. Dulhare, MuffKham Jah College of Engg. & Tech. Hyderabad, India
Prof. Zhaoxi Fang, Zhejiang Wanli University, China
Assoc. Prof. Akihito Nakamura, The University of Aizu, Japan
Assoc. Prof. Baijnath Kaushik, Shri Mata Vaishno Devi University, India
Assoc. Prof. Kazuteru Miyazaki, National Institution for Academic Degrees and Quality Enhancement of Higher Education, Japan
Assoc. Prof. Kenji Hisazumi, Kyushu University, Japan
Assoc. Prof. Luisito Lolong Lacatan, Ama University, Philippines
Assoc. Prof. Maria Christina R. Aragon, Technological Institute of the Philippines - Quezon City, Philippines
Assoc. Prof. Marina Mattera, Universidad Europea, Spain
Assoc. Prof. Md. Ruhul Islam, Sikkim Manipal Institute of Technology, India
Assoc. Prof. Mohamed Basel Almourad, Zayed University, United Arab Emirates
Assoc. Prof. Po-Hung Chen, National Chiao Tung University, Taiwan
Assoc. Prof. Rafidah Md Noor, University of Malaya, Malaysia
Assoc. Prof. Ravishankar Sharma, University of Canterbury, New Zealand
Assoc. Prof. Ruben Picek, University of Zagreb, Croatia
Assoc. Prof. Sayed Sayeed Ahmad, Al Ghurair University, UAE
Assoc. Prof. Shailender Kumar, Delhi Technological University, India
Assoc. Prof. Siamak Khatibi, Blekinge Institute of Technology, Sweden
Assoc. Prof. Sudipta Roy, Assam University, India
Assoc. Prof. Wen-Chung Chiang, Hsiuping University of Science and Technology, Taiwan
Assoc. Prof. Yau Wei Chuen, Xaimen University Malaysia, Malaysia
Asst. Prof. Felizardo Reyes Jr, Technological Institute of the Philippines - Quezon City, Philippines
Asst. Prof. Jasmin Caliwag, Technological Institute of the Philippines - Quezon City, Philippines
Asst. Prof. Paula Jean M. Castro, Technological Institute of the Philippines - Quezon City, Philippines
Asst. Prof. Reynaldo E. Castillo, Technological Institute of the Philippines - Quezon City, Philippines
Asst. Prof. Roxanne Ancheta, Technological Institute of the Philippines - Quezon City, Philippines
Asst. Prof. Xuping Huang, Advanced Institute of Industrial Technology, Japan
Senior Lecturer Ismail Ahmedy, University of Malaya, Malaysia
Dr. Abhijit Sen, Kwantlen Polytechnic University, Canada
Dr. Albert K. Chong, University of Southern Queensland, Australia
Dr. Beatriz De La Iglesia, University of East Anglia, UK
Dr. Feno Heriniaina Rabevohitra, Chongqing University, China
Dr. Gbolahan Olasina, University of KwaZulu-Natal, South Africa
Dr. Hirokazu Shimauchi, Tokyo Institute of Technology, Japan
Dr. Jan Kubicek, VSB-Technical University of Ostrava, Czech Republic
Dr. K. K. Soundra Pandian, Pdpm-Indian Institute of Information Technology Design and Manufacturing, India
Dr. Khaironi Yatim Shariff, Shibaura Institute of Technology, Japan
Dr. Nasser Nassiri, Higher Colleges of Technology, United Arab Emirates
Dr. Olarik Surinta, Mahasarakham University, Thailand
Dr. Patcharawadee Poolsamran, Burapha University, Sakaeo Campus, Thailand

Dr. Phan Duy Hung, FPT University, Viet Nam
Dr. Pi-Hsia Yen, Yu Da University of Science and Technology, Taiwan
Dr. Po-Chun Huang, Taipei Tech, Taiwan
Dr. Radu Laura-Diana, FEAA, Romania
Dr. Slamet Riyadi, Universitas Muhammadiyah Yogyakarta, Indonesia
Dr. Tan Phan Xuan, Shibaura Institute of Technology, Japan
Dr. Waraporn Viyanon, Srinakharinwirot University, Thailand

Chapter 1

Software and Data Engineering

Unrolled PRINCE Cipher based Glitch Physically Unclonable Function

Yusuke Nozaki
Meijo University
1-501 Shiogamaguchi, Tenpaku-ku
Nagoya, Aichi, Japan
+81-52-832-1151
143430019@ccalumni.meijo-u.ac.jp

Masaya Yoshikawa
Meijo University
1-501 Shiogamaguchi, Tenpaku-ku
Nagoya, Aichi, Japan
+81-52-832-1151
dpa_cpa@yahoo.co.jp

ABSTRACT
Physically unclonable functions (PUFs) have attracted attention as authentication technologies in integrated circuits (ICs). A PUF utilizes IC manufacturing variation as a unique device's ID. Several PUFs have been proposed, and a glitch PUF is superior to other PUFs in terms of resistance against malicious attacks. A glitch PUF uses the variation of glitch waveforms in AES's S-BOX circuit which requires large area to embed, while IoT devices have strict area constraint. It is important to satisfy the area constraints when a glitch PUF is applied to IoT devices. This study proposes a new glitch PUF using a lightweight cipher which can be embedded into small area. The proposed PUF is based on an unrolled PRINCE low-latency cipher. Experiments using a field programmable gate array (FPGA) prove the validity of the proposed PUF.

CCS Concepts
• **Security and privacy→Security in hardware.**

Keywords
Hardware security; lightweight cipher; PRINCE; physically unclonable function; glitch PUF.

1. INTRODUCTION
Lightweight ciphers have been attracted attention as technologies to ensure the security of embedded devices used in internet of things (IoT). Lightweight ciphers can be used in small-area, low-power, and low-latency; therefore, they are suitable for embedded devices instead of advanced encryption standard (AES) which is widely used. PRENSET [1] and CLEFIA [2] lightweight ciphers are standardized in ISE/IEC 29192-2. In addition, several lightweight ciphers, including a small-area cipher SIMECK [3], a low-power cipher Midori [4], a low-latency cipher PRINCE [5], and so on, have been proposed.

As technologies to enhance the security of LSI, physically unclonable functions (PUFs) have attracted attentions [6]–[8]. The PUF utilizes the LSI manufacturing variation to generate a device's unique ID called response against input called challenge. The LSI manufacturing variation such as signal propagation delay is difficult to control it, so that the PUF circuit cannot be duplicated physically. Hence, the generated ID by PUF can be used in device's authentication and key information of cryptographic circuit. Several PUFs have been proposed [6]–[8], and the glitch PUF [8] is a superior PUF because it has a good performance and the resistance against modeling attack [8][9].

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388207

The glitch PUF uses glitch variations of S-BOX circuit in AES encryption for ID generation [8]–[12]; however, the study of glitch PUF using other circuits except for AES has not been reported. To enhance the security of IoT system, it is important that studies about PUF applications of lightweight cipher expected to be used in embedded devices.

This study proposes a new glitch PUF using a lightweight cipher. Concretely, a structure of low-latency cipher PRINCE [5], which can encrypt with 1-clock, is used for PUF. Experiments using a field programmable gate array (FPGA) show the effectiveness of the proposed PUF.

The rest of the paper is organized as follows. Section 2 describes the outline of PRINCE cipher, glitch PUF, and PUF performance indicators as preliminaries. The proposed PUF based on PRINCE cipher is presented in section 3. The PUF performance evaluation results of the proposed PUF are presented in section 4. Finally, section 5 concludes this paper.

2. PRELIMINARIES
2.1 PRINCE Cipher [5]
PRINCE [5] is a lightweight cipher proposed by J. Borghoff et al. in 2012. In particular, PRINCE is operated with low-latency when it is implemented by unrolled architecture. An unrolled architecture is an implementation method which realizes a whole encryption circuit with combinational circuit. An unrolled PRINCE can be implemented on small circuit scale 100 times and low-latency 2 times more than AES circuit [13]. In addition, unrolled PRINCE can encrypt with 1-clock; thus PRINCE is expected to apply for memory encryption, encryption of real-time communication in automobile system, and so on.

Figure 1 shows the outline of PRINCE cipher. PRINCE is a block cipher of SPN structure with 64-bit block length and 128-bit key length. As shown in figure 1, PRINCE consists of a constant addition processing (0th round), processing by round function R (1st from round to 5th round), a middle processing, processing by inverse round function R^{-1} (from 6th round to 10th round), and a constant addition processing (11th round). PRINCE does not have a key-schedule part, and 64-bit partial keys (k_0, k_1, and k_0') used in

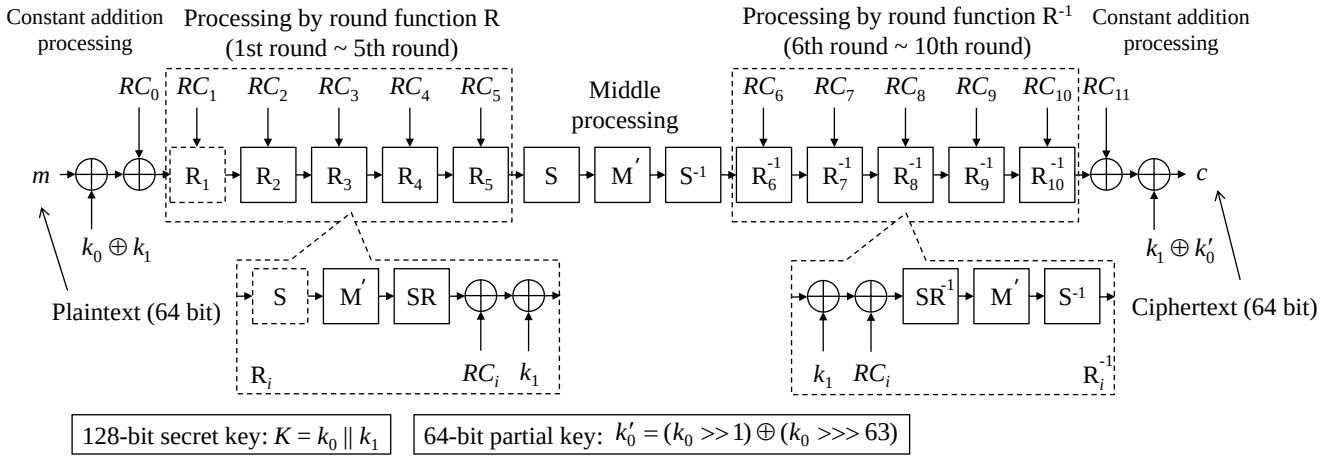


Figure 1. PRINCE cipher.

each processing are generated from a 128-bit secret key *K*. For each operation, RC_i is a round constant of *i*th round, *S* and S^{-1} are non-linear processing by S-BOX tables, SR is a linear processing by permutation, and *M*' is a linear processing by matrix operation [5].

2.2 Glitch Physically Unclonable Function [8]

The glitch is narrow spikes of output signal which is caused due to the difference of signal propagation delay in input signal of a combinational circuit. Concretely, an input signal in each logic gate has a different signal delay due to a wiring length or a wiring load, thus an unstable interval of output is generated by the difference of arrival time of input signal in combinational circuit. Since the signal propagation delay is fluctuated by the LSI manufacturing variation, the glitch waveform is also differed in each device. The glitch PUF uses thus difference of glitch waveforms for the ID generation [8].

Figure 2 shows the outline of glitch PUF. The glitch PUF consists of a combinational circuit for generating glitch waveforms (called glitch generator), a sampling circuit of glitch, and a response generator [8]. For the operation, in first, an input value of the glitch generator is provided to a data register as a challenge. Next, using the sampling circuit, a shape of glitch waveforms is obtained. Finally, the response generator generates a response of 0/1 from even-odd number of transitions. Moreover, the improved glitch PUF for small scale circuit called second glitch PUF is also proposed [9]. In the second glitch PUF, a sampling circuit and a response generator are simplified. Specifically, the output of glitch generator is directly connected to a toggle flip-flop (TFF). Since TFF inverts the output at the rising edge of the input signal, when the number of transitions is even, output of TFF is zero; otherwise, that is one. Thus, the output of TFF can be used as PUF response.

For the glitch PUF, not only evaluation with FPGA [8][9][11] but also that with application specific integrated circuit (ASIC) [10] has been performed, so that the glitch PUF has a good performance has been reported. In addition, in paper [13], the proposal of a method extending challenge set and the detailed security evaluation are performed.

The glitch PUF uses glitch variations of S-BOX circuit in AES encryption for ID generation [8]–[13]; however, the study of glitch PUF using other circuits except for AES has not been reported.

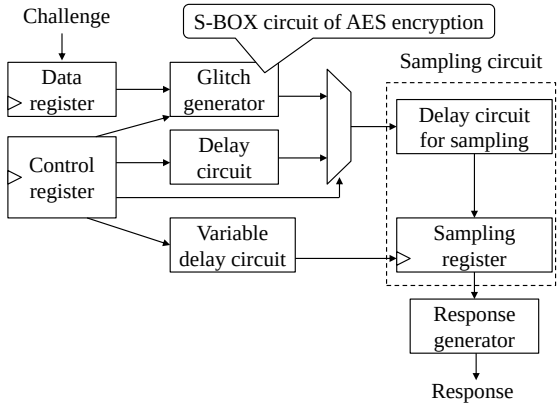


Figure 2. Outline of glitch PUF [8].

2.3 PUF Performance Indicators

Uniformity, steadiness, diffuseness, and uniqueness are typically used for the PUF performance evaluation [14]. Uniformity is the indicator which evaluates the appearance frequency of 0/1 in ID. Steadiness is the indicator which evaluates whether same ID is generated stable or not. Diffuseness is the indicator which evaluates whether ID is changed against different input or not. Uniqueness is the indicator which evaluates whether ID is changed between different devices against same input or not.

Each indicator can be evaluated by ID's Hamming weight (HW) and Hamming distance (HD) between IDs. Uniformity can be evaluated with the ID's HW, and steadiness, diffuseness, and uniqueness can be evaluated by the HD between IDs. Specifically, steadiness is evaluated by HD between IDs with same device against same challenge called same challenge intra-HD (SC Intra-HD), and diffuseness is evaluated by that against different challenge called different challenge intra-HD (DC Intra-HD). In addition, uniqueness is evaluated by HD between IDs with different devices against same challenge called same challenge inter-HD (SC Inter-HD).

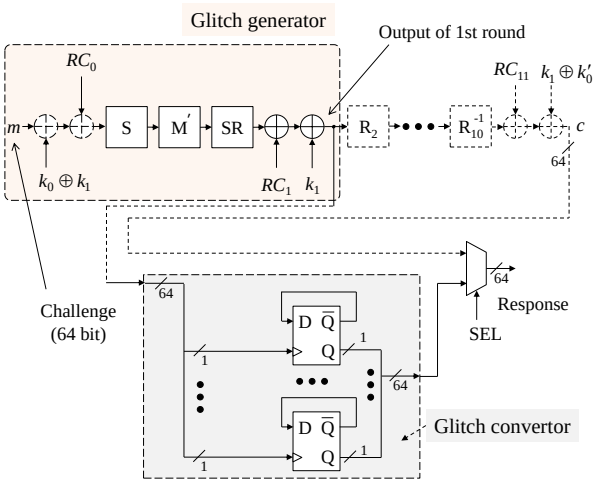


Figure 3. Outline of the proposed method.

For the evaluation, the response of $L \times K \times N \times T$ bits is used where L is ID length, K is kind of IDs, N is the number of devices, and T is the number of trials for same ID generation.

3. PROPOSED METHOD

This study proposes a new glitch PUF utilizing a lightweight cipher circuit. In particular, the proposed method targets an unrolled architecture which can extract glitch efficiently.

Concretely, the proposed method does not use AES's S-BOX but PRINCE cipher as glitch generator. The proposed method generates response bits by connecting outputs of glitch generator to a response generation circuit. At this time, from the preliminary experimental results, when a whole circuit of PRINCE was used as the glitch generator, the steadiness of PUF response decreased drastically due to a large glitch noise. Therefore, the proposed method uses a partial part of PRINCE cipher as glitch generator.

Figure 3 shows the outline of the proposed PUF. As shown in figure 3, the proposed PUF uses a part from input to 1st round's output in PRINCE as glitch generator. At this time, since output of glitch generator is 64 bits, they are connected to 64 TFFs. Therefore, the proposed PUF can generate a 64-bit response in one operation.

4. EXPERIMENT

4.1 Experimental Environment

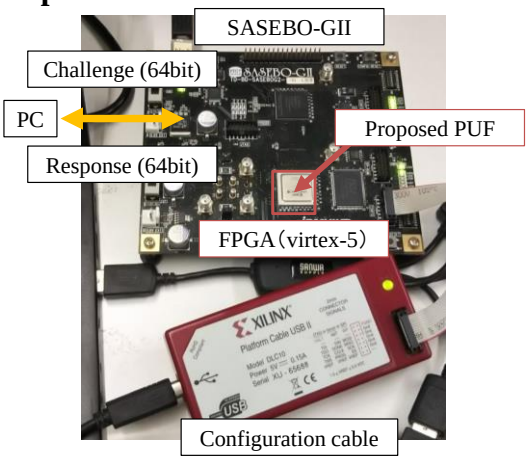


Figure 4. Evaluation system.

Experiments used SASEBO-GII FPGA boards. The SASEBO-GII mounts two types of Xilinx FPGAs: Virtex-5 XC5VLX30/50 and Spartan-3A XC3S400A. Figure 4 shows the evaluation system. The proposed PUF was implemented into a Virtex-5. For the evaluation, randomly generated challenges were used, and the responses of $L \times K \times N \times T$ bits were obtained where parameters L, K, N, and T were 128, 128, 5, and 100.

4.2 Experimental Result

In experiments, uniformity, steadiness, diffuseness, and uniqueness were evaluated. Figures 5, 6, 7, and 8 show the experimental results. In those figures, the vertical line is frequency of each metrics, and the horizontal line is the ID's HW or HD between IDs.

For the evaluation of uniformity, the mean of ID's HW was 64.73, as shown in figure 5. The mean of HW was closer to 64, which was half of ID size, that is, response of 0/1 was appeared uniformly. Therefore, the proposed PUF has high uniformity.

For the evaluation of steadiness, as shown in figure 6, the mean of SC Intra-HD was 3.981, which was closer to 0. This means that same ID was generated stable against same challenge. Thus, the proposed PUF has a high steadiness.

For the evaluation of diffuseness, the mean of DC Intra-HD was 62.51, which was closer to 64, as shown in figure 7. In other words, the ID was changed against different challenges. Consequently, the proposed PUF has a high diffuseness.

For the evaluation of uniqueness, the mean of SC Inter-HD was 44.46, as shown in figure 8. The mean of SC Inter-HD was closer to the half of ID size; thus the uniqueness was a good performance. For the authentication, since the proposed PUF has high steadiness, it can identify devices sufficiently even if SC Inter-HD is not closer to 64 completely.

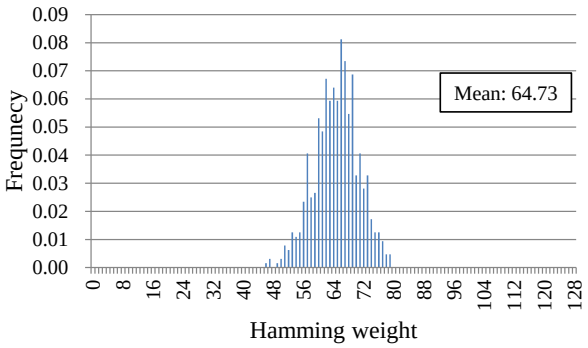


Figure 5. Result of uniformity.

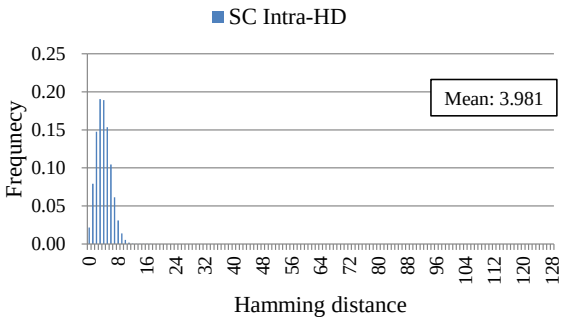


Figure 6. Result of steadiness.

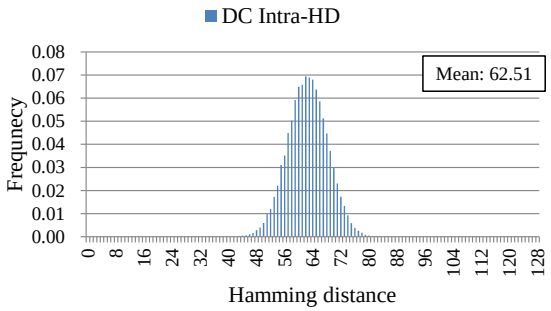


Figure 7. Result of diffuseness.

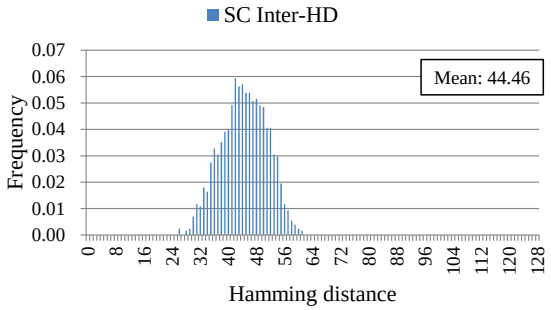


Figure 8. Result of uniqueness.

5. CONCLUSION

This study proposed a new glitch PUF using a structure of lightweight cipher. The proposed PUF is based on the unrolled PRINCE low-latency cipher. For the PUF ID generation, output with the first round of unrolled PRINCE cipher is used. In experiments, the proposed PUF was implemented into an FPGA, and the performances were evaluated using typical PUF performance indicators: randomness, steadiness, diffuseness, and uniqueness. Experimental results clarified that the proposed PUF had a good performance.

In the future, we will develop the glitch PUF about other lightweight ciphers.

6. ACKNOWLEDGMENTS

This paper is based on results obtained from a project commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

7. REFERENCES

[1] Bogdanav, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., and Vikkelsoe, C. 2007. PRESENT: An Ultra-Lightweight Block Cipher. In *Proceedings of 9th International Workshop on Cryptographic Hardware and Embedded Systems* (Vienna, Austria, September 10–13, 2007). CHES 2007. Springer-Verlag LNCS 4727, 450–466. DOI= https://doi.org/10.1007/978-3-540-74735-2_31.

[2] Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T. 2007. The 128-Bit Blockcipher CLEFIA (Extended Abstract). *In Proceedings of 14th International Workshop on Fast Software Encryption* (Luxembourg, Luxembourg, March 26–28, 2007). FSE 2007. Springer, LNCS 4593, 181–195. DOI= https://doi.org/10.1007/978-3-540-74619-5_12.

[3] Yang, G., Zhu, B., Suder, V., Aagaard, M. D., and Gong, G. 2015. The Simeck Family of Lightweight Block Ciphers. In *Proceedings of 17th International Workshop on Cryptographic Hardware and Embedded Systems* (Saint-Malo, France, September 13–16, 2015). CHES 2015. Springer-Verlag LNCS 9293, 307–329. DOI= https://doi.org/10.1007/978-3-662-48324-4_16.

[4] Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., and Regazzoni, F. 2015. Midori: A Block Cipher for Low Energy. In *Proceedings of 21st Annual International Conference on the Theory and Application of Cryptology and Information Security* (Auckland, New Zealand, November 29 – December 3, 2015). ASIACRYPT 2015. Springer-Verlag LNCS 9453, 411–436. DOI= https://doi.org/10.1007/978-3-662-48800-3_17.

[5] Borghoff, J., Canteaut, A., Güneysu, T., Kavum, E. B., Knežević, M., Knudsen, L. R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S. S., and Yalçın, T. 2012. PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications. In *Proceedings of 18th Annual International Conference on the Theory and Application of Cryptology and Information Security* (Beijing, China, December 2–6, 2012). ASIACRYPT 2012. Springer-Verlag LNCS 7658, 208–225. DOI= https://doi.org/10.1007/978-3-642-34961-4_14.

[6] Lee, J. W., Lim, D., Gassend, B., Suh, G. E., Dijk, M. V., and Debadas, S. 2004. A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications. In Proceedings of IEEE VLSI Circuits Symposium (Honolulu, USA, June 17–19, 2004). IEEE, 176–179. DOI= https://doi.org/10.1109/VLSIC.2004.1346548.

[7] Suh, G. E. and Devadas, S. 2007. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In Proceeding of 44th ACM/IEEE Design Automation Conference (San Diego, USA, June 4–8, 2007). DAC 2007. ACM/IEEE, 9–14. DOI= https://doi.org/10.1145/1278480.1278484.

[8] Suzuki, D. and Shimizu, K. 2010. The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes. *In Proceedings of the 12th International Conference on Cryptographic Hardware and Embedded Systems* (Santa Barbara, USA, August 17–20, 2010). CHES 2010. Springer-Verlag LNCS 6225, 366–382. DOI= https://doi.org/10.1007/978-3-642-15031-9_25.

[9] Shimizu, K., Suzuki, D., and Kasuya, T. 2012. Glitch PUF: Extracting Information from Usually Unwanted Glitches. *IEICE TRANS. Fundamentals of Electronics, Communications and Computer Sciences*, E95-A, 1 (Jan. 2012), 223–233. DOI= https://doi.org/10.1587/transfun.E95.A.223.

[10] Suzuki, D., Shimizu, K., Sugaware, T., Shiozaki, M., and Fujino, T. 2013. LSI Implementation of Device Key Generator using Glitch PUFs. *In Proceedings of the 30th Symposium on Cryptography and Information Security* (Kyoto, Japan, January 22–25, 2013). SCIS 2013. IEICE, 1–8. (in Japanese).

[11] Shimizu, K., Suzuki, D., Tsurumaru, T., Sugawara, T., Shiozaki, and M., Fujino, T. 2014. Unified Coprocessor Architecture for Secure Key Storage and Challenge-Response Authentication. *IEICE TRANS. Fundamentals of Electronics, Communications and Computer Sciences*, E97-A, 1 (Jan. 2014), 264–274. DOI= https://doi.org/10.1587/transfun.E97.A.264

[12] Yamamoto, D., Hospodar, G., Maes, R., and Verbauwhede, I. 2012. Performance and Security Evaluation of AES S-Box-based Glitch PUFs on FPGAs. *In Proceedings of International Conference on Security, Privacy, and Applied Cryptography Engineering* (Chennai, India, November 3–4, 2012). SPACE 2012. Springer LNCS 7644, 45–62. DOI= https://doi.org/10.1007/978-3-642-34416-9_4.

[13] CRYPTREC Lightweight Cryptography Working Group. 2017. CRYPTREC Cryptographic Technology Guideline (Lightweight Cryptography). https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016en.pdf

[14] Hori. Y., Yoshida, T., Katashita, T., and Satoh. A. 2010. Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs. *In Proceedings of International Conference on Reconfigurable Computing and FPGAs* (Quintana Roo, Mexico, December 13–15, 2010). ReConFig 2010. IEEE, 298–303. DOI= https://doi.org/10.1109/ReConFig.2010.24.

Ontology of Crop Pest Control

Kolyo Onkov
Department of Mathematics and Computer Science
Agricultural University, 12 Mendeleev str.,
4000 Plovdiv, Bulgaria
+359 32 251324
kolonk@au-plovdiv.bg

ABSTRACT
Domain ontology of crop pest control consists of hierarchically structured biological and chemical information and concepts on crops, pests, pest control measures and relations among them. Despite vertical relations in hierarchies, the knowledge about crop protection measures leads to horizontal relations between classes biological and chemical objects. There is analogy between class objects in biological classification of crops, pests and pest control measures from one hand and from the other hand class objects and instances of object oriented programming. The developed domain ontology has characteristics of task ontology because it leads to building analytical models, data analysis and solving practical problems. Classification of tasks and applications based on the domain ontology is in the scope of this work, as well.

The main aim of the ontology is the development of intelligent computer based systems intended to satisfy specific informational needs of the professionals and practitioners in agronomy, crop protection, plant medicine, economics and business.

CCS Concepts
•Computing methodologies→Ontology engineering.

Keywords
Pest control information; Domain ontology; Framework; Hierarchical structures; Relational database; Object oriented approach.

1. INTRODUCTION
Crop pest control in agriculture consists of biological, chemical, physical techniques and measures applied by agricultural specialists that depress the development of crop pest populations. The scientific and expert information in pest control domain is usually heterogeneous and multi-disciplinary – biological, chemical, agrarian and legal.

Domain ontology is formal descriptions of the classes of concepts and the relations among them that illustrate an application area [1]. Assessing the quality of domain ontologies for their suitability to potential applications remains difficult, even though a variety of frameworks have been developed [2]. Agriculture as an application area presumes building ontologies including conceptualization of crops and crop products, farms located in geographical regions and soil and climate information, concepts related to crop rotations and cultivation choices available to farmers, agricultural activities as a coherent set of crops [3-6] or only one crop [7-8]. Domain ontology on crop cultivation is considered as static information during plant growing (soil, seed and agricultural machines) while task ontology builds on the point of plant process: soil selection, seed selection, fertilization [9]. Crop pest control is a specific domain of agriculture. The ontology of this domain is characterized with symbolic knowledge representation schemes built by scientific defined concepts and tasks and services based on the ontology [10-13]. AGROVOC, National Classifications and Thesaurus, Semantic Web technologies, OWL, Protégé, multi-agent methods and graphical tools are used for building ontology in crop pest control [1, 14, 15 and 16].

This paper aims to present domain ontology of crop pest control and basic tasks regarding information, knowledge services, data modeling and analysis.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388208

2. CROP PEST CONTROL ONTOLOGY
General model of crop pest control consists of related datasets on crops, pests and pest control measures (figure 1). Each dataset contains classes of biological or chemical objects. The names of classes and objects can be used to define complex relationships among them. "Damage and disease" present the natural processes in the path „crops -> pests". "Treatment" of damaged crops includes human control measures and biological enemies of pests usually encouraged by human in order to protect the crops.

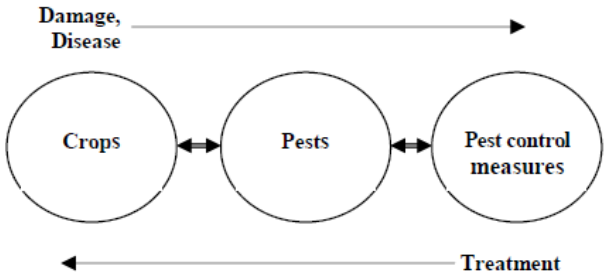


Figure 1. General information model of crop pest control.

Ontological framework of crop pest control is presented on the figure 2. Biological nature and scientific classification (taxonomy) of crops and pests predetermine hierarchical structures that contain class biological and chemical objects. The crops hierarchy is realized based on agronomic purpose of crops. The class of

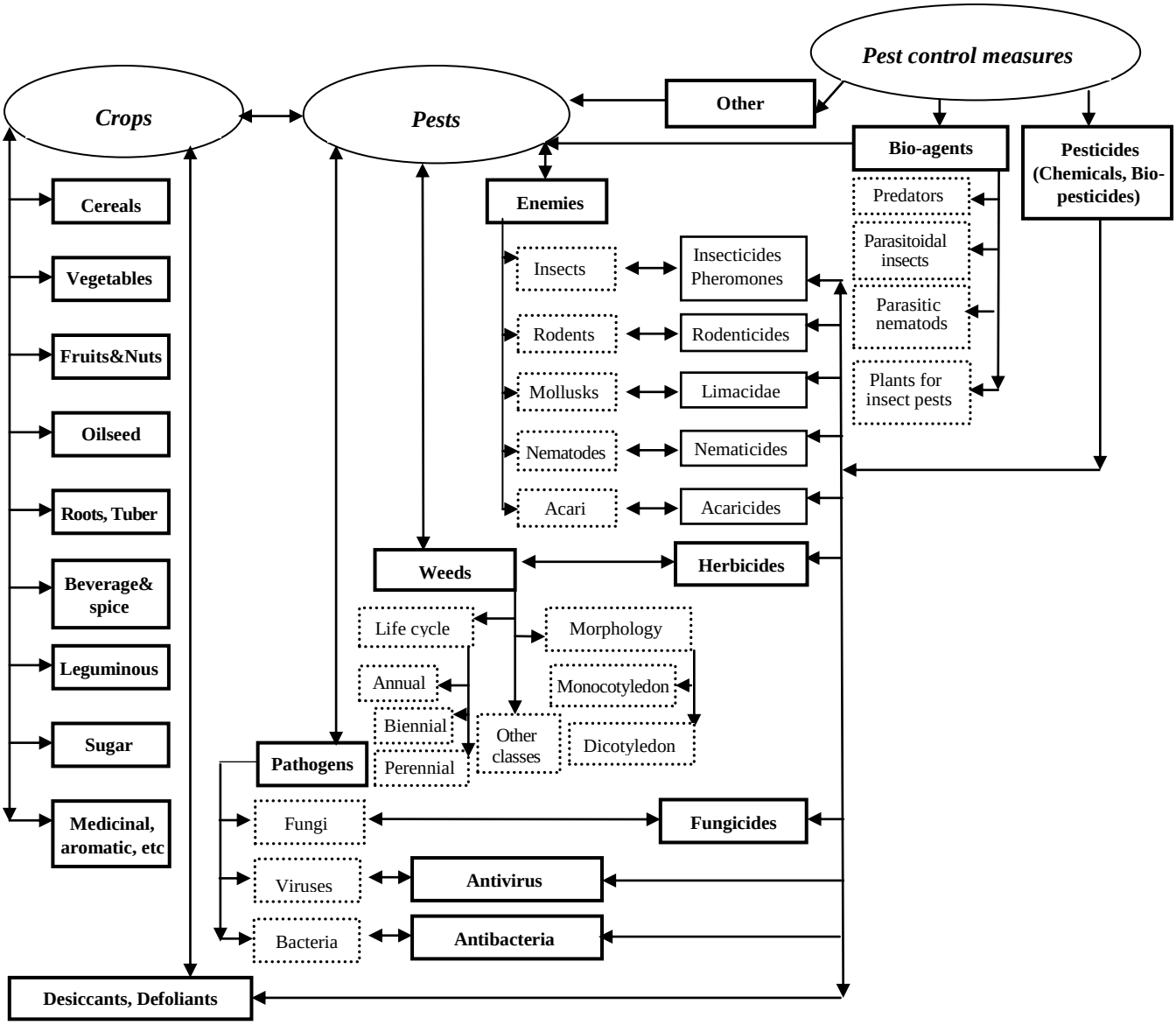


Figure 2. Ontological framework of crop pest control.

pests consists of three hierarchies: Pathogens, Weeds and Enemies. Class Pest control measures covers sub-classes Pesticides (Chemicals and Bio-pesticides), Bio-agents and „Other" measures. Vertical arrows in hierarchies mean relations "class –> sub-class –> object (s)". Despite vertical relations in hierarchies, the knowledge about crops pest control leads to horizontal relations between biological and chemical classes, sub-classes and objects. Horizontal relations here have the following meanings: diseases of crops caused by pathogens, negative influence of weeds and enemies and pest control measures (treatments) by pesticides, bio-agents and other practices. The real existing relations are in both directions: "crops –> pests –> pest control measures" and "pest control measures –> pests –> crops". There is a strong correlation between sub-classes and entities of pests (fungi, viruses, insects etc) and pesticides (fungicides, antivirus, insecticides etc). Each entity in the figure 2 contains a list of items. Let's have 3 examples: a) cereal crops: rice, wheat, barley, oats, and rye; b) insects: Myzodes persicae, Tribolium castaneum, Thrips and many others; c) insecticides: Carate Zeon, Confidor, etc. "Other" pest control measures include information on practices in agriculture, host plant resistance, technologies to introduction or encouragement of antagonistic organisms. Such kind of information is usually presented in easy accessible form, for example text documents in PDF. Concepts from Multilingual Thesaurus AGROVOC are used in building the ontology.

Presented crop pest control ontology is typical domain ontology. It has features of task ontology because it provides knowledge and information needed for task definition and problem solving in the domain. This ontology aims at creating intelligent computer based systems to meet the users' requirements for knowledge, information and data analysis. Relational approach is proper solution to store semantically related biological and chemical data in easy accessible and retrievable database. The fundamental concepts of Object oriented approach fully correspond to the ontology of crop pest control giving opportunity for data modeling and analysis.

3. RESULTS AND DISCUSSION

This chapter goes through domain ontology issues to task ontological issues. Task oriented capabilities of crop pest control ontology provides information and knowledge services based on the contemporary information methods and technologies. Tasks classification is done as follows:

- Creating and exploring relational database and software. Strong points of the relational software are managing the relationships between objects, querying and visualization of related data in the path "crops –> pests –> pest control measures" and back. Information services are oriented to wide range of users: agronomists and farmers responsible for crop protection measures, students, administrators, people working in pesticides business;
- Data modeling and analysis is required by scientists and experts in biology, chemistry, plant medicine and agriculture working in governmental, scientific and educational organizations. The core of object oriented modeling and analysis consists of managing classes of objects and relations among them. The analogy between classes and subclasses in biology and chemistry and class objects and instances of object oriented approach is a base for flexible data modeling. The object oriented models can be developed through using the classes of crops, pests, pesticides (chemicals and natural products) and bio-agents. In many cases data querying in relational database is not enough, because of the need for more deep data analysis. This descends from close properties of the objects from definite class, but also from variations of the objects in the definite class and variations among classes. Object oriented models and software can be developed for making data analysis. As well, object oriented approach provides instance level modeling that allows working with real names of cultivated crops, pests, pesticides and other terms from the domain. The experts would be triggered by the real data analysis in order to research and develop more effective measures for crop protection as well as to improve the governmental rules, regulations and control mechanisms.
- Building intelligent computer based systems (Decision support systems, Multi-dimensional databases, Platforms etc.) through integration of information, knowledge and software. Integration of pest control information with spatial data on climate and soil, temporal data on pesticides used for previous time period and agro technical information would be useful. Managers of pest control business will benefit from applying economic models such as control of inventories, cost-benefit models and risk assessment. In this sense the integration of economic models and pest control models is needed. Linking of software systems in agribusiness organization with analytical knowledge from the domain of pest control will support business functions, strategies and decision making processes.

Important role of crop pest control ontology is to convert the unstructured or semi-structured data into structured one – relational database. Bulgarian "Phytopharmacy" database is built using ideas of the presented domain ontology (figure 2). Coding system is applied in the creation of database model to define semantic relations among sets of identified text objects: names of crops, pests and pesticides [17]. Reference book presenting the information on permitted pesticides in semi-structured form is used for building "Phytopharmacy" database. This database stores detailed data on pesticides use: product, manufacturer, active ingredient, dose, minimum lethal dose (MIN_LD), guarantee period (PHI days), use category and application (figure 3). Agronomists and farmers can easily explore information in the path "crops –> pests –> pesticides" while specialists in plant medicine usually follow the path "pesticides –> pest –> crops". Bulgarian "Phytopharmacy" database manages data on 137 cultures, 273 pests and 741 pesticides. This database does not include bio-pesticides and bio-agents.

Other database applications on registered pesticides for crop protection can be found in Internet sites of the European and Mediterranean Plant Protection Organization and Pesticide Action Network, North America.

Example of object oriented modeling and analysis of Bulgarian "Phytopharmacy" database is presented in [12]. Combined use of pesticides is important because of pest resistance and lowering the costs. Regarding this issue, flexible analytical model is developed for joint resolving two or more tasks for data processing on combined use of several pesticides against identified pests for

Phytopharmacy

Pest_Groups

Fungi&Viruses$Bacteria

Pests	Picture					
Peronospora tabacina						
Product, Manufacturer	Active ingredient	Dose	MIN_l	PHI days	Use cat	Application
Acrobat MZ BASF Agro B.V.	90g/kg dimethomorph + 600 g/kg mancozeb	0.2%	1750	14	3	10-14 days. PP 40-80 l/decare
ANTRACOL 70WG, Bayer CropScience	700 g/kg propineb	0,20%	5000	7	1	7-10 days
VERITA WG Bayer CropScience	44 g/kg fenamidom + 667 g/kg alumine fosetil	0.15%	2028	30	3	7-10 days
DITAN M-45 WP Indofil Industries Limited	800 g/kg mancozeb	0.2 %	5000	20	3	7-10 days. PP 30-60 l/decare
CURZATE M DF DuPont IO	4% cymoxanil + 40% mancozeb	0.3%	2000	20	3	7-10 days. PP 30-100 l/decare

Figure 3. "Phytopharmacy" database: access and visualization of information.

selected crops. The developed object oriented software includes procedures for basic set operations – union and intersection. As well as, the data processing provides variations regarding the different pesticides use. Following the relations between classes of the ontology (figure 2) the developed object oriented software strongly facilitates the sequence of operations in practice: information extraction, modeling, analysis and finally decision support. The next step of data modeling and analysis pays respect to miscibility of the pesticides. It is logical to incorporate or link the expert information on pesticides miscibility to Bulgarian "Phytopharmacy" database. Then the analytical software can be improved to provide completed information services regarding combined pesticide use.

Expert information and knowledge on tobacco production is multi-aspect, heterogeneous, semi-structured and stored in different information sources. Multidimensional database "Tobacco_BG" integrates expert information on tobacco in Bulgaria, an important crop for the country [18]. This database stores information in four dimensions:

- Phytopharmacy – pests and permitted for use pesticides for tobacco under rules and regulations in the country;
- Varieties – tobacco groups and varieties including description of their special characteristics: genealogy, botanical and morphological features, soil and climate requirements; conditions for production: plant population, breaking, picking, curing etc.; chemical composition of tobacco and tobacco smoke: nicotine, tar, total nitrogen, etc. (figure 4);
- Statistics – statistical time series on harvested areas and quantity of production;
- Legislation – laws and normative documents on tobacco production in PDF form.

The database "Tobacco_BG" is a systematic solution with high operability that facilitates flexible data access, visualization, querying and updating. It abstracts information classification, substantial relations among entities as well as spatial and temporal details in datasets. This application is an intelligent system which provides integrated information on one crop including concepts of pest control ontology. Multidimensional database "Tobacco_BG" is an open type solution regarding the number of dimensions giving opportunity to be used as a platform for building databases on diverse crops in Bulgaria and other countries.

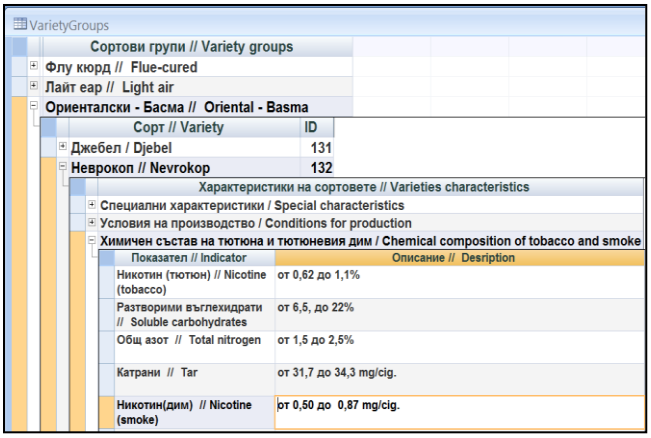


Figure 4. Tobacco groups and varieties in "Tobacco_BG" database.

4. CONCLUSION

Crop pest control ontology is developed taking into consideration the significance and complexity of pest control in agriculture. This domain ontology could be determined also as "task ontology" because it provides information and knowledge needed for task definition and problem solving. Classification of tasks based on ontology is done. Applications of the ontology give opportunities to provide knowledge, information and data analysis for experts and scientists in plant medicine and agriculture as well as information services for agronomists, farmers and agribusiness managers. Crop pest control ontology can be useful for application software developers because of systematizing expert information and knowledge from the domain.

Hierarchical structures of crop pest control ontology consisting of classes biological and chemical objects are considered persistent. The list of pesticides is changeable, but the concepts of ontology and data structures in applications remain the same.

Still there is lack of intelligent computer solutions based on pest control ontology. Major routes in the future work could be as follows:

- Databases enrichment. The databases in domain store usually data on chemicals for crop protection against pests. The extension of these databases with information on bio-pesticides and bio-agents would be right decision. This is valid for Bulgarian "Phytopharmacy" database;
- Extension of tasks based on crop pest ontology. Tasks regarding pesticides miscibility and evaluation of economic effectiveness are very prospective. Moreover, the climate and environmental changes will lead to ecological regulations requiring new tasks and analytical models on pest control measures;
- Information, knowledge and software integration. Integration or linking of software systems in agribusiness organization with information and knowledge from pest control domain will support decision making processes.

5. REFERENCES

[1] Musen, M. A. 1998. Domain ontologies in software engineering: use of Protege with the EON architecture. Methods of Information in Medicine, 37(04/05), 540-550. https://scholar.google.bg/scholar?hl=bg&as_sdt=0%2C5&q=%22Domain+ontologies+in+software+engineering%22&btnG=

[2] McDaniel, M., and Storey, V. C. 2019. Evaluating Domain Ontologies: Clarification, Classification, and Challenges. ACM Computing Surveys (CSUR), 52(4), 70. https://dl.acm.org/citation.cfm?doid=3359984.3329124

[3] Athanasiadis, I. N., Rizzoli, A. E., Janssen, S., Andersen, E., and Villa, F. 2009. Ontology for seamless integration of agricultural data and models. In Research Conference on Metadata and Semantic Research (pp. 282-293). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04590-5_27.

[4] Sun, X., Zhu, H., Gu, J., Wu, H., and Feng, C. 2009. Research on the semantic web-based technology of knowledge integration for agricultural production. In 2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery (Vol. 2, pp. 361-366). IEEE. https://ieeexplore.ieee.org/document/5359472.

[5] Xiao, H., Qiu, T., and Zhou, P. 2013. Integration of heterogeneous agriculture information system based on interoperation of domain ontology. In 2013 Second International Conference on Agro-Geoinformatics (Agro-Geoinformatics) (pp. 476-480). IEEE. DOI: 10.1109/Argo-Geoinformatics.2013.6621966.

[6] Deb, C. K., Marwaha, S., Malhotra, P. K., Wahi, S. D., and Pandey, R. N. 2015. Strengthening soil taxonomy ontology software for description and classification of USDA soil taxonomy up to soil series. In 2015 2nd International Conference on Computing for Sustainable Global Development, pp. 1180-1184. IEEE. https://ieeexplore.ieee.org/abstract/document/7100434/authors#authors

[7] Wang, Y., Wang, Y., Wang, J., Yuan, Y., and Zhang, Z. 2015. An ontology-based approach to integration of hilly citrus production knowledge. Computers and electronics in agriculture, 113, 24-43. https://doi.org/10.1016/j.compag.2015.01.009.

[8] Chougule, A., Jha, V.K. and Mukhopadhyay, D. 2019. Decision support for grape crop protection using ontology, Int. J. Reasoning-based Intelligent Systems, Vol. 11, No. 1, 24–37. https://scholar.google.bg/scholar?hl=bg&as_sdt=0%2C5&q=Decision+support+for+grape+crop+protection+using+ontology&btnG=

[9] Li, D., Kang L., Cheng X., Li D., Ji L., Wang K. and Chen Y. 2013 An ontology-based knowledge representation and implement method for crop cultivation standard. Mathematical and Computer Modelling, 58(3-4), 466-473 https://doi.org/10.1016/j.mcm.2011.11.004

[10] Huai-guo, Zheng. 2009. Study on the Ontology Model Construction in Plant Pest Control. Journal of Anhui Agricultural Sciences, (2), 177. http://en.cnki.com.cn/Article_en/CJFDTotal-AHNY200902177.htm

[11] Rafea, A. 2010. Web-Based Domain Specific Tool for Building Plant Protection Expert Systems. Expert Systems, Petrica Vizureanu (Ed.), 193-202. https://scholar.google.bg/scholar?hl=bg&as_sdt=0%2C5&q=Web-Based+Domain+Specific+Tool+for+Building+Plant+Protection&btnG=

[12] Onkov, K. 2011. Object Oriented Modelling in Information Systems Based on Related Text Data. In Artificial Intelligence Applications and Innovations, 212-218. Springer, Berlin, Heidelberg. https://link.springer.com/content/pdf/10.1007/978-3-642-23960-1_26.pdf

[13] Damos, P. 2015. Modular structure of web-based decision support systems for integrated pest management. A review. Agronomy for sustainable development, 35(4), 1347-1372. https://doi.org/10.1007/s13593-015-0319-9

[14] Min, Z., Bei, W., and Chunyuan, G. 2011. Application study of precision agriculture based on ontology in the internet of things environment. In International Conference on Applied Informatics and Communication (pp. 374-380). Springer, Berlin, Heidelberg. 2011. 374-380. https://doi.org/10.1007/978-3-642-23226-8_49

[15] Malik, N., and Sharan, A. 2016. Semantic Web Oriented framework for Knowledge Management in Agriculture Domain. IJWA, 8(3), 71-79. https://pdfs.semanticscholar.org/4637/33bdb95a22a751c26ad3153294c10dcb07d2.pdf

[16] Zhitomirsky-Geffet, M. and Mograbi, C. Z. 2018. A New Framework for Collaborative Ontology Construction for an Agricultural Domain from Heterogeneous Information Resources. Journal of agricultural & food information, 19(3), 203-227. https://doi.org/10.1080/10496505.2017.1378105

[17] Dimova, D. 2010. An Algorithmic Solution for Management of Related Text Objects with Application in Phytopharmacy. Serdica Journal of Computing, 4(4), 487–504. http://serdica-comp.math.bas.bg/index.php/serdicajcomputing/article/view/111

[18] Onkov, K., Bozukov, H. and Kasheva M. 2015. Integrating expert information on tobacco production, Global Journal on Technology 07, 07-13. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.736.2925&rep=rep1&type=pdf

Systematization of Digital Twins: Ontology and Conceptual Framework

Linard Barth
Institute of Marketing Management,
Zurich University of Applied Sciences
Theaterstrasse 17
CH-8401, Winterthur
+41 58 934 68 67
linard.barth@zhaw.ch

Matthias Ehrat
Institute of Marketing Management,
Zurich University of Applied Sciences
Theaterstrasse 17
CH-8401, Winterthur
+41 58 934 66 31
matthias.ehrat@zhaw.ch

Rainer Fuchs
Institute of Marketing Management,
Zurich University of Applied Sciences
Theaterstrasse 17
CH-8401, Winterthur
+41 58 934 70 56
rainer.fuchs@zhaw.ch

Jens Haarmann
Institute of Marketing Management,
Zurich University of Applied Sciences
Theaterstrasse 17
CH-8401, Winterthur
+41 58 934 61 52
jens.haarmann@zhaw.ch

ABSTRACT

The development and progress in information and communication technologies will transform traditional products into smart products and allow to offer novel smart services [1]. Herein, the digital twin (DT) concept is regarded as a key technology to create value with smart services [2]. Although the research and applications of DTs emerge continuously many concerns are to be scrutinized [3]. The lack of a shared conceptual framework for DTs with an unambiguous terminology [4] complicates cross-functional discussions. Therefore, a systematization of the main dimensions of DTs is proposed in the form of an ontology and a conceptual framework thereof derived. The research questions addressed in this paper are a) «Which dimensions are used to classify and structure DTs in academic literature?», b) «What are the fundamental differences or specifications within these dimensions?» and c) «How do these different specifications relate to each other?» The focus of the research is on the objective to find classification systematics that are a) representing the entire spectrum of DTs, b) universally valid in all DT related domains and c) applicable in research and practice. A systematic literature review on the relevant aspects of DTs was conducted and the findings iteratively advanced within workshop sessions with academic experts. DTs are considered as integrators of physical and digital worlds as well as internal and external value creation. Further, the creation of DTs requires per definition the use of digital data. Hence, the proposed ontology and conceptual framework for DTs include the following main dimensions to consider for every DT: Data resources, external value creation and internal value creation. The main subdimensions of the **data resources** are the data sources to obtain the data, the data categories and the data formats. The main subdimension of the **external value creation** are the attributes of the services as the basis of the value propositions, the level of smartness of the connected products and the actors on the different levels of the ecosystem. The main subdimensions of the **internal value creation** are the lifecycle phases of products, the product management levels and the different generations of both. The proposed ontology and conceptual framework support researchers and practitioners in positioning and structuring their intended DT activities and communicating them to internal and external stakeholders. The holistic view on the data resource dimension further allows to easily deduct the needed data for certain applications or deduct possible applications from already available data.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388209

CCS Concepts

• Computer systems organization→Embedded and cyber-physical systems • Computing methodologies→Modeling and simulation.

Keywords

Digital Twin; systematization; ontology; conceptual framework.

1. INTRODUCTION

The development and progress in information and communication technologies will transform traditional products into smart products and allow to offer novel smart services [1, 5, 6, 7]. Herein, the digital twin (DT) concept, originated by Grieves [8], is regarded as a key technology for the seamless integration and fusion of smart connected products (SCP) and smart services within a cyber-physical system (CPS) [9] and as a way to seize the manifold opportunities to create value with new smart services [2]. In 2012, the concept of DTs was revisited by the National Aeronautics and Space Administration (NASA), which defined the DT as a "multiphysics, multiscale, probabilistic, ultrafidelity simulation that reflects, in a timely manner, the state of a corresponding twin based on the historical data, real-time sensor data, and physical model" [10]. This is still the most used

definition of a digital twin in academic publications [2, 11, 12, 13, 14, 15, 16, 17, 18, 19]. It is important to note, that different from CAD (that exclusively focuses on the digital world) and IoT (that heavily concentrates on the physical world), DTs are characterized by the two-way interactions between the digital and physical worlds and thereby create new possibilities [10]. The Digital Twin is accordingly ranked on 4th place within the top 10 strategic technology trends from Gartner, which are "not yet widely recognized trends that will impact and transform industries through 2023" [20] and is closely connected to most of the other top trends. Especially the other top 5 trends are related to digital twins, as they form the basis or a potential output of the digital twin technology: Autonomous things, augmented analytics, AI driven development, digital twin and empowered edge [20]. Even though the digital twin concept is relatively young, the market is estimated to grow from USD 3.8 billion in 2019 to USD 35.8 billion by 2025, at a CAGR of 37.8% [21]. The importance of DTs for the future is widely recognized and therefore the approach is increasingly emphasized by both academia and industry, which is evidenced by the increasing publications and patents on DTs during the past few years [2, 18], as seen in figure 1.

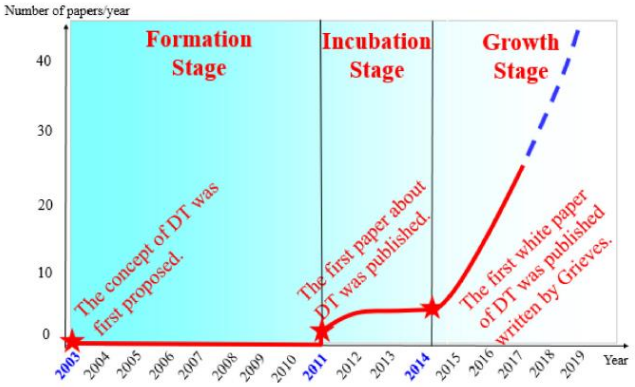


Figure 1. Development trend of the DT research [18].

The stimulation of the DT research around 2011, as seen in figure 1, was triggered by the technological advancement in other areas such as cloud computing, big data, IoT and sensor technologies which experienced a rapid growth since 2003. However, the business value and return of DT investments in practice is often hard to see, as the challenges of this complex topic are spread in different domains and as they have a high impact on internal and external processes [22]. Additionally, due to the plethora of existing solutions and concepts of DTs across industries, a diverse and incomplete understanding of this concept exists [17, 18, 23, 24]. Although the research and applications of DTs emerge continuously, the systematic research is rare, thus many concerns are to be scrutinized [3]. Establishing value adding and sustainable DT-based service proposition concepts and business models involves collaboration between experts from various disciplines inside and outside a company [25, 26]. However, this collaboration is hindered by the lack of a shared conceptual framework for DTs, the unambiguous terminology [4] and the missing common language based on a sufficiently abstract, intuitively understandable and easy-to-use reference model [25]. Hence, cross-functional discussions turn out to be intricated especially in practice. It thus becomes evident that further dimensions for structuring DTs are required in order to get a differentiated yet understandable perspective, especially on their value contribution [27]. Therefore, a systematization of the main dimensions of DTs is proposed in the form of an ontology and a conceptual framework derived thereof for the use in practice.

2. MATERIAL AND METHODS

Within this framing the research questions addressed in this paper are a) «Which dimensions are used to classify and structure DTs in academic literature?», b) «What are the fundamental differences or specifications within these dimensions?» and c) «How do these different specifications relate to each other?» The focus of the research is on the objective to find classification systematics that are a) representing the entire spectrum of DTs, b) universally valid in all DT related domains and c) applicable in research and practice. A systematic literature review on the relevant aspects of DTs was conducted [28]. Table 1 summarizes the scope of the literature review according to Cooper's taxonomy [29].

Table 1. Review scope

Characteristic		Categories			
1	Focus	Research outcomes	Research methods	Theories	Applications
2	Goal	Integration	Criticism	Central issue	
3	Organization	Historical	Conceptual	Methodological	
4	Perspective	Neutral presentation	Espousal position		
5	Audience	Specialized scholars	General scholars	Practi-tioners	General public
6	Coverage	Exhaustive	Exhaustive & selective	Representative	Central/ pivotal

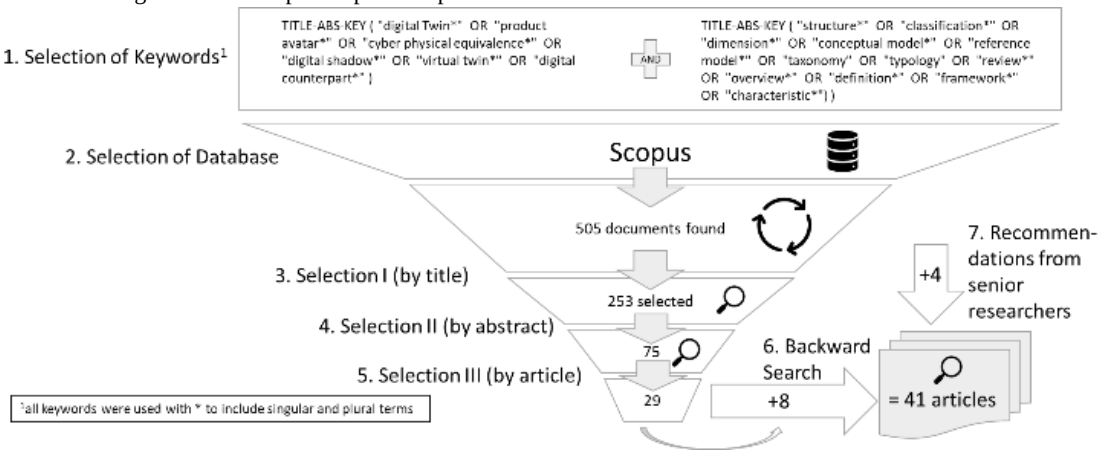


Figure 2. Process of systematic filtering of literature for the review.

For the selection of the database, the comparative research [30, 31] was applied and finally Scopus was selected due to its completeness in the area of peer-reviewed contributions [32]. 505 papers found have been filtered in several steps and finally 41 academic articles have been studied in detail after some additional papers have been added by backward research and based on the recommendations by senior researchers, as seen in figure 2.

A first draft in form of a concept map was developed and iteratively advanced within six workshop sessions with academic experts from the mainly involved disciplines to create an ontology and ultimately a conceptual reference framework as a useful artefact for the use in practice. After each workshop the pre-final versions of the graphical representation of the relations between the found dimensions and subdimensions were consolidated and then served as the initial basis for the next workshop iteration. This process was proceeded until only minor changes regarding the terms to describe the subdimensions were discussed.

3. RESULTS

DTs are considered as integrators of both, physical and digital worlds as well as internal and external processes of value creation [22]. A study performed by Meierhofer & West [27] confirms this finding, as the main beneficiaries of DT are "services" (external value creation) and operations (internal value creation), as seen in figure 3.

To establish these benefits in services and operations, DTs require the collaboration between experts from various disciplines inside and outside a company, which emphasizes the need for a holistic conceptual framework. The DT-based value proposition offered to customers depends strongly on the customer himself and on his individual situation and context, within IoT ecosystems this means, that the designer of a service-oriented digital twin needs to understand on which hierarchical level he operates on, which comprehension level of internal product management operations he wants to cover and which data categories are needed to provide the intended services. Hence, the proposed ontology seen in figure 4 and conceptual reference framework for DTs include the following main dimensions to consider for every DT: a) Data resources, b) external value creation and c) internal value creation.

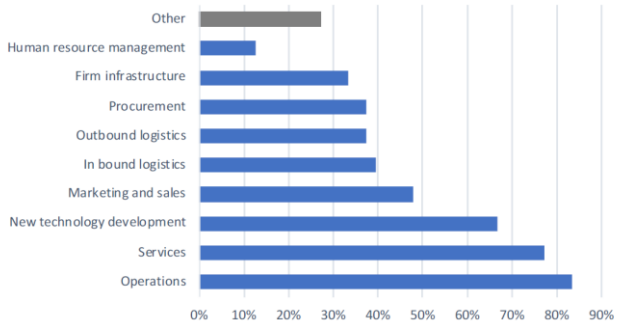


Figure 3. Beneficiaries of service value from the digital win [27].

3.1 Data Resources

Data resources are the fuel of every DT application as value creation is not possible without the necessary data in the needed form. Massive user/product generated data serves as the key for value creation, while effective data analytics tools enable its success [33]. The main subdimensions in the proposed framework are thus a) the data sources to obtain the data from, b) the data categories they relate to and c) the data format.

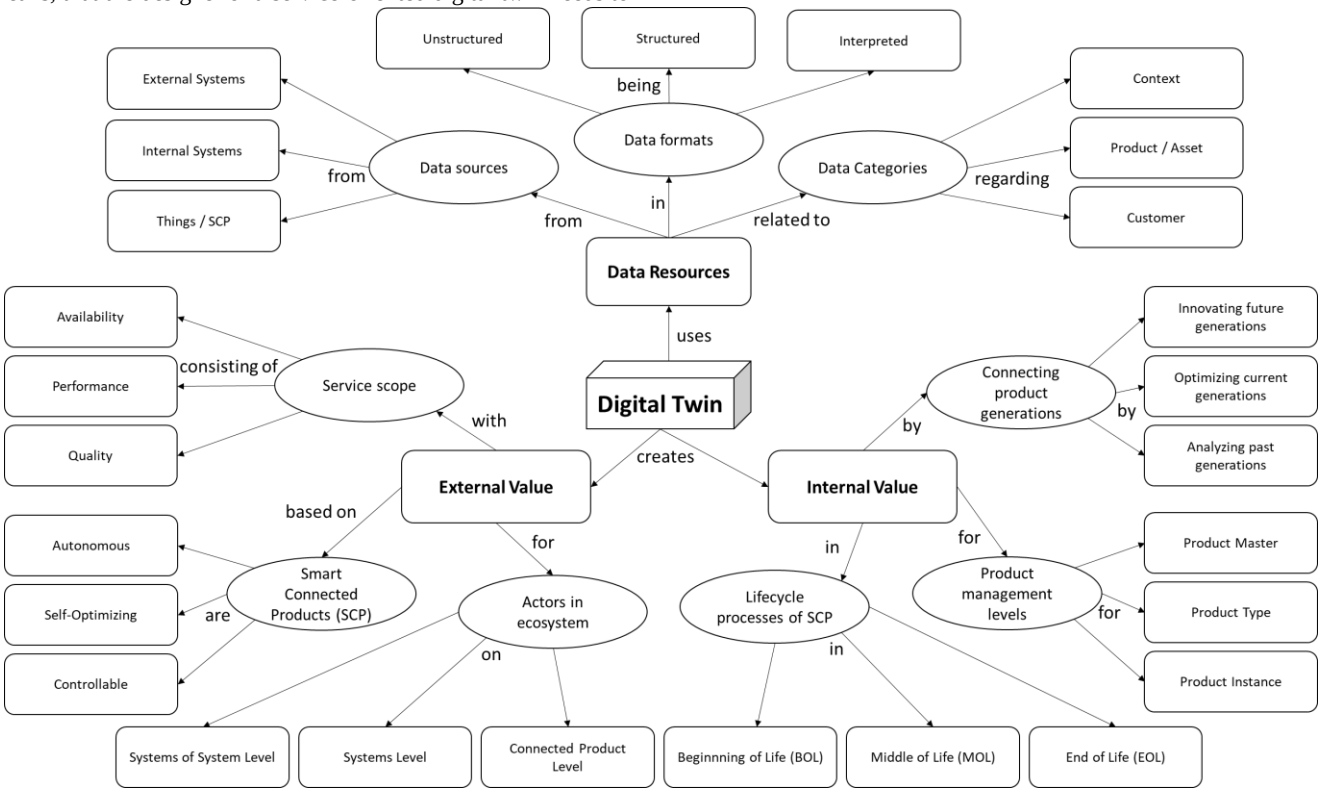


Figure 4. Digital twin ontology.

3.1.1 Data Sources

Traditionally companies collect data from various sources such as on-board systems of the product, internal enterprise systems and third-party sources and store it in scattered legacy systems. In result, information is divided in silos across enterprise divisions and product lifecycle phases. Consolidating these islands of information in a DT lays the foundation for any data-based innovation of services and processes. For each product or asset instance, or more generally referred to as "thing" in accordance with the widely used term "internet of things", the meta-data model is a template that defines the elements of the DT and it obtains the data, especially on the instance-level, directly from the embedded information systems (EIS) of the thing itself. Utilizing the DT as a single source of truth for instance-related data minimizes redundant data and potentially conflicting information from heterogeneous systems [11]. These non-embedded systems can be divided into internal and external information systems connected to the DT. Firstly DT concepts utilize, integrate, and recombine contents from several internal enterprise information systems such as authoring systems, PDM, ERP, CAD, CRM and others for specific objectives [34]. An overview of IT systems storing DT relevant data is illustrated in figure 5. Secondly the DT may utilize, integrate, and recombine contents directly from corresponding systems of other companies as well as from third-party data providers offering valuable data via API or IoT platforms, this group of sources is referred to as "external systems". In the proposed framework the different data sources for DT are therefore divided into things, internal systems and external systems.

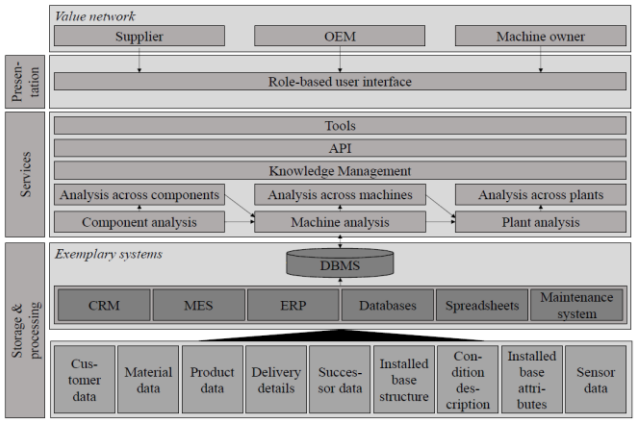


Figure 5. Conceptual model of the information architecture [35].

3.1.2 Data Categories

The illustration of IT systems storing product information seen in figure 5 also gives a first hint about the data categories utilized, integrated, and recombined by DTs, as they are a representation of a product [12] and its processes [24] and therefore consist of datasets describing the state (product) and behavior (process-performance) of a product or asset. Grieves & Vickers [12] elaborate what data can be contained in a DT. Depending on the use case they state that a complete 3D model of the physical instance and its components, a Bill of Materials (BoM) that lists current and replaced components and a Bill of Processes (BoP) that lists the operations that were performed during manufacturing can be included. In addition, the results of any measurements and tests on the instance, a service record that describes past services and all available sensor data from the instance should be added to the DT. To make sense and form the base for knowledge-based decision making, the second category often described contains contextual data [e.g., 11, 17, 36, 37, 38], such as instance environment data (e.g. temperature, humidity) and any other contextual data relevant for the intended internal or external value creation (e.g. exchange rates, weather data, market data) which is not directly related to the state or behavior of the product or asset itself. Academia and practice show that the value of digitized products for the user of a DT increases with the access to data from the surrounding ecosystem [5, 6]. The third category to distinguish are customer-related data, such as data about the actual owner, his configuration and usage preferences, as well as other customer relationship management relevant data [39]. This customer-related data is already gathered before the actual purchase or contract signing of services by the customer, as the customer experience lifecycle already provides valuable data during the earlier phases, as seen in the lower part of figure 6. Such combined data sets will not only describe how the SCP performs its processes and services, how its state evolves due to deterioration, wearing down and replacement of components, but also how it is used by customers and other actors, such as other SCPs and their DTs. Additionally through the addition of contextual information all obtained data can be set into relation to the context and therefore are potentially unveiling completely new insights that rend enormous business opportunities, as these comprehensive DTs illustrate the current lifestyle of users [26] and ultimately unexploited or future customer needs and demands. Hence, service-oriented DTs can be the source of several new knowledge-driven business opportunities [40], as it is also illustrated in figure 6.

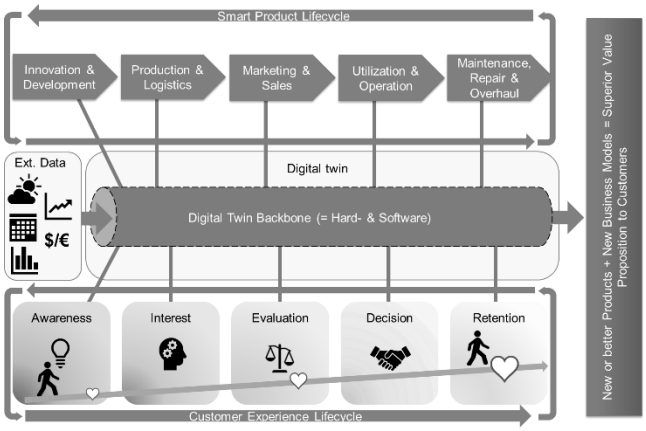


Figure 6. DT as integrator of product and customer lifecycle [39].

3.1.3 Data Formats

The amount of data available and to manage grows significantly with the implementation of a DT, especially with the introduction of a SCP delivering data from the field, maybe even in real-time. But the sheer size of the generated data lake is not pivotal. To create internal and external value the data must be structured and interpreted to achieve DT based decision- and sense-making. According to the data lifecycle for DTs defined by Tao et al. [16] eight different steps can be distinguished: Data collection, data transmission, data storage, data integration, data processing, data cleaning, data analysis and data mining. The DT requires a novel data-structure permitting piecemeal refinement of the observed data for big data analytics and mining of data from different sources and in different formats. Therefore, after collecting, transmitting and storing the data, the integration, processing and cleansing of data are the crucial steps to achieve compatible,

structured data formats for the analysis and interpretation phases. In the ontology and conceptual reference framework this process is simplified to the three main categories of unstructured, structured and interpreted data in accordance to the few publications in the review which mentioned this subtopic regarding DT [17, 22, 41, 42]. Unstructured as well as semi-structured data require formatting efforts according to the requirements of analyzing and processing methods before they can be interpreted, therefore semi-structured data is not further distinguished from unstructured data in the model. Examples for unstructured data are photography, video and recordings often delivered by the SCP itself, as in the use-case of autonomously driving cars perceiving their environment mainly by cameras. Semi-structured data features some kind of structure which reduces the efforts for integrating, processing and cleaning data. However, semi-structured data is still not compatible with data from other sources and not ready for interpretation and ultimately decision- and sensemaking. Typical semi-structured data are either preprocessed unstructured data, for example the transcripts of recordings, or have origin in external systems using different structuring standards, for example customer reviews, comments and complaints in the web or equipment maintenance orders. Structured data on the other hand is either the result of proper data processing or has its origin in external sources providing data-as-a-service. Structured data is characterized by a high degree of organization, clarity and consistency [17], hence most data in internal information systems can be considered as structured [41], but also many external data providers deliver structured data, for example market information, such as exchange rates or sales numbers, search engine advertisement data or weather data. Traditional design methods, data lifecycle management tools and databases are developed to interpret structured information and therefore they are not suitable for dealing with the unstructured information generated without any predefined models or formats [17]. Different authors embrace the topic how to improve the data lifecycle management in the DT context to achieve interpreted information which can be potentially used for automated decision- and sense-making. Patel et al. [42] elaborate on the suitability of different open source formats such as Sensor-based Linked Open Rules (S-LOR), which is a data set of interoperable rules used to interpret data produced by sensors. Detzner and Eigner [11] propose a data aggregation layer for the DT that allows to organize the data hierarchically. Zhang et al. [41] mention that semi-structured and unstructured data can be stored in Hadoop Distributed File Systems. Damjanovic-Behrendt & Behrendt [36] discuss the adequacy of semantic and relational database models for structured data of DTs.

3.2 External Value Creation

The external value creation is realized in the market, in cooperation with customers, partners and other actors, such as other SCP and their DTs in the business ecosystem. The main subdimensions are a) the attributes of the services corresponding the value propositions, b) the level of smartness of the connected products and c) the actors on the different levels of the ecosystem.

3.2.1 Attributes of the Service

At present, the research how the various components of digital twins are encapsulated to services and used is just in its infancy [14]. However, the integration between DTs and services is a promising research direction, as not only new services can be enabled, but also existing services can be enhanced by the new data supplied by DTs [18]. The common aim of the DT is to support the realistic model of system behavior that can support often already established services such as performance prediction and optimization [13]. But with regard to the concept of everything-as-a-service (XaaS), services could fully release the potential of DTs [14], as the DT lends itself to contribute to the value proposition by supporting all of the actors around the product-service-system (PSS), in particular by relieving the pains and increasing the gains of the actors in new ways [27]. The attributes of a DT-based service can be defined in line with the widely recognized and used concept of overall equipment effectiveness (OEE) that was introduced in 1971 by Japan's JIPM (Japan Institute of Plant Maintenance) and ultimately evolved into Total Productive Manufacturing (TPM). According to Nakajima [43], OEE measurement is an effective way of analyzing the efficiency of a single machine or an integrated manufacturing system. OEE is a function of availability, performance and quality rate and is calculated as the product of its three contributing factors [44]. Especially in the context of smart manufacturing and industrial IoT this encapsulation of DT-based services seems promising, as the OEE-concept is not only widespread but also clearly defined by several norms for certain purposes such as DIN 8743 for packaging machines and packaging installations [45]. However, to be able to achieve a holistic perspective on DT-based services the definition of OEE is too narrow, but it can be supplemented with an overall service effectiveness (OSE) concept applicable to describe data-based service [46]. The main contribution factors are still availability, performance and quality rate thus the overall services effectiveness can be defined as:

$$Overall\ Service\ Effectiveness\ (OSE) = Availability * Performance * Quality$$

Each of the three contribution factors is composed of main drivers of potential losses that may occur. Bange [46] elaborates an example of a tools company in Germany where the main drivers of potential losses can be described as follows: Availability or time of the service is represented by the time needed between the occurrence at the customer triggering the need and the delivery of the service satisfying the need. The performance or cost contribution factor describes the relation between input and output from the view of the customer, hence it's the price to pay for the service in relation to the value received. The quality is affected by the discrepancy between the offered service and the actually delivered service. The concept of OSE can be applied to any industry, however the main drivers of potential losses need to be tailored for every business case and are therefore only described generically [46].

3.2.2 Level of Smartness

Intelligence and connectivity enable an entirely new set of product functions and capabilities, the benefits on unit/item/instance level can be structured and modelled according to Porter and Heppelmann [5] in four increasing levels: 1) monitoring, 2) control, 3) optimization, and 4) autonomy. In the proposed ontology and conceptual reference model the level of monitoring is not included, as a product which is only monitored but not able to be controlled cannot be regarded as smart and the model is only respecting SCP. A SCP can be controlled through remote commands or algorithms that are built into the device or reside in the product cloud [5]. This allows the SCP to respond to specified changes in its condition or environment, if certain thresholds are exceeded the SCP can perform a predetermined reaction. The benefits of controlling described by Porter and Heppelmann [5] are the customization of product performance and the personalization of the customers interaction with the product. On the level of optimization the product still reacts to certain triggers

from the environment, but in contrast to the control level the product now can optimize its reaction due to past experiences derived of the data collected by itself or identical SCP that stored their experiences in the DT of the product type. The highest level of smartness described in theory and practice and thus also in the proposed conceptual reference framework is autonomy. The paradigm of an ideal SCP is provided by the research stream of cybernetics which studies the concepts of control and communication in living organisms, machines and organizations, including self-organization [47]. It studies how a system, either biological system or artificial system, processes information and depends on information to make decisions and take actions. A remarkably concept in this regard that might be adaptable also to autonomously acting SCP, such as self-driving cars offering Uber-like services to customers without any human interaction, is the viable systems model developed by Beer [48], in which the systems' ultimate goal is to maximize its viability against all perturbations. The viable systems model is based on the research and conclusions of W. Ross Ashby and his "law" of "requisite variety", which states that for a system to be stable, the number of states that its control mechanism is capable of attaining (thus its variety) must be greater than or equal to the number of states in the system being controlled [49]. Cybernetics thus provides the theoretical foundation for developing smart systems, which can collect, process and understand various self-related and contextual information [26] to make smart decisions with the purpose of viability. However, the smartness is not fully embedded in the physical product, as it can be made more intelligent to actively adjust its real-time behavior by receiving recommendations from the DT [17] which has access to vastly more data and computing power.

3.2.3 Different Levels of the Ecosystem

Most of the analyzed sources [e.g. 14, 15, 19, 37, 50, 51] suggest dividing the DT into different levels of hierarchy. The number of hierarchy levels mentioned differ, ranging from two [13, 42, 52] up to six [26, 27], however the most common and comprehensible hierarchy determination based on the conducted research distinguishes three levels, mostly referred to as "component" or "unit", "system" and "system-of-systems" [2, 9, 23, 53, 54]. Structuring DTs according to such a three-tier hierarchy is also in line with the well-known model of Porter and Heppelmann [5, 6] explaining the innovation from SCPs to Systems and System-of-Systems. Especially when it comes to the realization of value creation with services, the appropriate granularity of the DT of a SCP or CPS and the corresponding "family of twins" [27] forming a system or system-of-systems needs to be determined. DTs of systems composed in such manner may access the DTs of subordinate units or components and simultaneously may have a common objective and be aggregated to a composite system-of-systems DT [e.g. 14, 19, 52]. The actors in such ecosystems therefore might often be other SCPs, systems or system-of-systems or rather their DTs requesting data-driven services. Therefore it is important, that the designer is aware of the intended hierarchy level within the ecosystem as the value proposition needs to be designed specifically for each actor of the ecosystem [55], as they require value propositions that fit their jobs to be done, as well as relieve pains and realize gains alongside these jobs [27]. It is further important to note, that rather than locally and individually optimizing single products (e.g. production machines) as it was mainly done and researched until today, there will be major efficiency and effectivity gains when the generated data and interactions are analyzed and optimized at higher system hierarchy levels [41, 56].

3.3 Internal Value Creation

The internal value creation is realized within the own company and can influence all processes of the value chain. The main subdimensions are a) the lifecycle phases of products, b) the product management levels and c) the different generations of both.

3.3.1 Lifecycle Phases

Another body of research on the DT concerns the application of DTs along the product lifecycle [e.g. 14, 57, 58] and the integration of the DT into PLM [e.g. 59] as DT-based services can provide value in every phase of a units or systems lifecycle phase, as it is also illustrated in figure 6. Inherently, DT concepts embrace the whole product lifecycle "from cradle to cradle" [34], however so far more than 70% of the DT applications take place either in production or prognostics and health management (PHM) as seen in figure 7. Even though most research is performed in the field of optimization of the usage phase there is also vivid discussion of the potential of DTs to optimize product design, engineering, shop floor design, supply chain management, customer demand analysis and service and value proposition design [e.g. 9, 14, 26, 54, 57, 58]. While the DT emerged as a concept for aerospace application, thus started with the monitoring and optimization of a single physical entity (referred to as "instance" in figure 9), it has later started to show promise also in and during production [e.g. 14, 41, 42]; however, there is also a plethora of possibilities of DT applications in any other PLM discipline, which are not yet fully explored [e.g. 13, 27, 60].

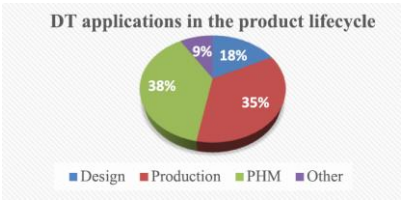


Figure 7. Distribution of DT publications in different areas [18].

3.3.2 Product Management Levels

To enable the full potential of DT in product management it is necessary to distinguish the different abstraction or meta-levels of product lifecycle management (PLM) integration. Even though most authors, especially in the field of PLM only differentiate instance and type [e.g. 22, 25], some authors are starting to distinguish a third meta-level, which can be referred to as «product master» [11, 26, 61, 62] or even more general «product aggregate» [9, 12]. The different levels of product management are connected to each other via several learning, feedback and validation loops, as illustrated in figure 8.

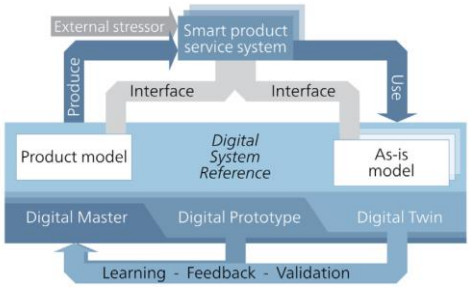


Figure 8. Smart products and digital master, digital prototype and digital twin [26].

The DT of an instance is directly interconnected to the physical asset and represents a bidirectional reflection from both the expected, digital world derived from the type and the real, physical world observed from the instance. It mainly fulfills three different functions, that can be described as follows, in accordance to Boschert & Rosen [57] and Tao et al. [9]: The first function is to integrate various types of data from the physical entity to map its state in real-time as accurate as possible. The second function is to exist and coevolve along the lifecycle of the physical entity to accumulate knowledge about it. The third function is to optimize the physical instance based on variance analyses with the digital model. To fulfill the third function the DT instance must reflect the expectations on how the product ought to be physically structured, function, behave, interact with customers and respond to uncertainties. These expectations are derived from the product type which is the concept of a product or can also be referred to as a blueprint from which the instances are derived. It is the offering presented on the market and includes all data that is needed to promote, sell, build, operate, servitize [63, 64], and recycle product instances. Examples of data describing a product type are product requirements, BoMs, operation plans, manufacturing methods and recycling instructions. Also, configuration knowledge for the sales process or instructions and tools to fulfill a service are typical items that are described in a product type dataset [25]. While the definition of product types is continuously changed and improved, the instances follow their own lifecycle and might or might not be affected by changes of their type. In some cases, the average lifecycle of an instance can be substantially longer than of its type, for example in case of cars that are still on the road but are not built anymore in such specifications. Equivalently to the relation of DT instance and DT type, the DT master monitors and optimizes the lifecycle of the product types with data from different sources. The DT product master provides design, systems, supply chain, product and value proposition engineers with the possibility to examine the lifecycle data of instances and types generated by the DTs, in order to discover patterns and to gain insights to optimize and innovate the product types. These patterns may also unveil changing customer demands that may be matched with novel product and service concepts [65] to be implemented in future product types and instances. Congruent to the physical product instances their digitized versions on all product management levels also comprise a lifecycle where they are iteratively developed and produced, used and maintained, and in some cases also recycled [66]. The separation of master, type and instance is a fundamental concept in the presented model and a greatly relevant difference to traditional models.

3.3.3 Different Generations

The DT concept represents a holistic model-based description of a product for current and future lifecycle stages [34] as it refers to a comprehensive physical and functional description, which includes a wealth of information that is useful not only in the current but also in subsequent life cycle phases [67, 68]. But not only the current and future concepts need to be stored in the DT, also historic data about former states of instances, types and masters are valuable for optimization and innovation processes. Historic information for example about previous software versions or parts built into a product instance can be essential to determine the root cause of a problem [11]. Further, the next generation often has similar problems that could have been avoided by using knowledge about the predecessors [12], but today the knowledge about the behavior of instances, systems or system-of-systems is often lost when they are retired. Through DTs structured in at least three distinctive generations (historic, current, future), additional value can be created especially within internal processes. The research is still scarce; however, some authors discussed the potentials of such DT concepts applied especially in product design. Tao et al. [17] suggest a DT-driven product design and underline that their research is in the initial stage. Also Landahl et al. [13] note that approaches that use design data related to products in use to form new concepts are rare and discuss the development of several generations of products and production systems based on the same platform, as especially manufacturing companies seek to be able to meet the needs of a wide range of customer needs with modular concepts. To generate new concepts with the use of platforms, knowledge of previously developed designs needs to be represented and structured to be sufficiently reused [13], which is underlining again the need for DTs separating historic, current and future concepts. According to Qi et al. [14] product design can be more effective with such DTs as they allow to reduce the inconsistencies of expected behavior and design behavior, lower costs and greatly shorten design cycles. Such DTs would also create the possibility to mine the through-life data in order to discover patterns and to gain insights about novel design concepts – ultimately enabling a wide exploration of the design space [65]. However, no clear direction is given on how to improve blending new customer needs and demands into product masters with data of historic and currently existing product instances and types currently in use [13]. To do so, the DT must be conceptualized to an appropriate abstraction level suited for the conceptual stages as proposed in the model at hand. The applicability of DTs for product design in practice, with respect to how and in what ways the communication, synergy and coevolution between a physical product instance and its representing DT instance can lead to more efficient and effective design process thus still needs additional research [17].

3.4 Digital Twin Conceptual Reference Framework

The conceptual reference framework proposed based on the discussed findings consists of nominal categories and hierarchical ordinal variables forming three distinctive but connected matrixes for the main dimensions of DTs as seen in figure 9: Data resources, internal value creation and external value creation. The three-dimensional order of each matrix leads to $3x3^3 = 81$ different DT subcategories that can conveniently be distinguished, discussed and combined, forming the composite DT for any specific use case.

For example, regarding the **external value creation**: Any value which is proposed to actors on different levels of the ecosystem is encapsulated in a service with attributes in the three proposed categories and is based on the level of smartness of the DT of the SCP. Not all levels of smartness might be available for all actors, therefore not all 27 cubes in the matrix might be occupied. Regarding the **internal value creation** the focus of a first DT application in a company might be focused only on the optimization of the middle of life phase of current instances, in this case only one of the 27 cubes in this matrix would be occupied and still there would already be potential value creation. In case of the **data resources** it seems obvious, that every kind of data needs to have a source, belongs to at least one of the three categories and is available in a particular format. A certain DT depicted in this conceptual reference framework is therefore representing a snapshot of the historic, current or future state of a certain company, its value proposition in the ecosystem, its digital

representation of the internal value creating processes and the data resources used for both. It is therefore a unique combination of the whole DT spectrum which is holistically represented with the total of 81 cubes in the three matrixes. The majority of existing DT literature suggest that data is fed from sensors of the existing physical assets to high-fidelity simulation models of the digital state that are then fed back to, for example, optimize the performance of the existing physical things. But recent interpretations of the DT concept have moved away from the idea that all available data can or should be included in every DT. Instead a selection of data must be performed depending on the use case [11]. It is important to understand, that authenticity does not describe a DTs quality, because abstract models specified for the task at hand can support knowledge-based decision-making more efficiently [19], for example on the product master level. Hence it is not the target to fill out all the 81 cubes depicted in the conceptual reference model, but to find composite DT combinations that are efficiently and effectively creating internal and external value with the least possible efforts regarding data resources. With regard to the effectivity of DT projects and activities there will be major efficiency gains when the interactions of SCP and actors in the ecosystem are optimized at the system or system-of-systems level, rather than locally and individually optimizing the performance of SCP, as it is mainly done today. Porter & Heppelmann [5] already noted, that the value of the coordination of SCP with other products and systems can grow exponentially as more and more products become connected.

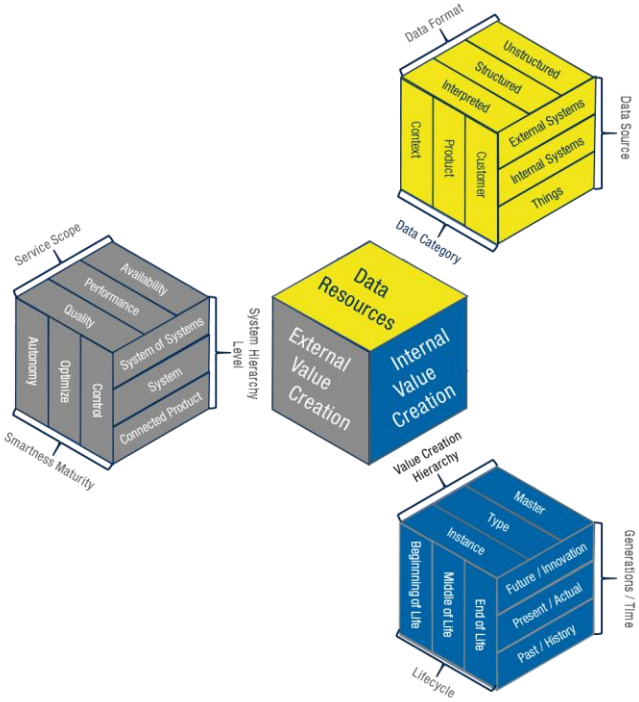


Figure 9. Digital twin conceptual reference framework.

4. CONCLUSION

This paper summarizes a systematization approach to structure DT applications by identifying major distinguishing characteristics of the different approaches and summarizing them in three qualitative dimensions. The current research leads to the assumption, that each dimension can occur in different specifications, which have been outlined in this paper. The motivation for the proposed ontology and conceptual reference model is to contribute towards a common understanding of the DT and to develop the theoretical foundation of the concept as well as providing practitioners a profound understanding of the inherent structuring dimensions of DTs. Ontologies and conceptual reference frameworks are considered as useful artefacts for the requirements engineering of specific instances of the mapped topic. A conceptual model's primary objective is to convey the fundamental principles and basic functionality of the system which it represents. Also, a conceptual model must be developed in such a way as to provide an easily understandable system interpretation for the model's users. A conceptual model, when implemented properly, should satisfy four fundamental objectives [69].

- Enhance an individual's understanding of the represented system

Apart from technical challenges, the successful implementation of DTs requires a holistic understanding of value delivering ecosystems, internal value creation with PLM of products and services and data resource management. The developed conceptual framework enhances individual's understanding of the relation and context of DT based innovation by providing a holistic and comprehensive systematization of the coherence.

- Facilitate efficient conveyance of system details between stakeholders

By using the conceptual framework as a reference for DT based projects, the stakeholders, for example in different internal functional departments, all share the same big picture, develop a common language and can use the framework visually to facilitate conveyance of system details between them. In academic education, the authors already use the reference model to provide structure to their courses. The reference model thus forms the framework for putting the subject areas of the DTs of smart connected products into context.

- Provide a point of reference for system designers to extract system specifications

This paper will give practitioners a profound understanding of the underlying architecture of DTs and provides practical ways to organically integrate DT models that create internal and external value. The holistic view on the data resource dimension further allows to easily deduct the needed data for certain applications or deduct possible applications from already available data.

- Document the system for future reference and provide a means for collaboration

The proposed ontology and conceptual framework support researchers and practitioners in positioning and structuring their intended DT activities and communicating them to internal and external stakeholders. At the same time the framework provides an effective guide to systematically classify and compare DTs of all kinds according to the internal value creation, external value creation and data resources management.

Eventually, the developed conceptual reference framework might contribute to model the profile of the DT in the servitization area, outline future research avenues and support the implementation in practice. Therefore, the usefulness of the created artefacts will be further validated and the approach how to deduct specific instances will be further investigated. The generalizability of the concept to different industries and products must be examined in

more detail and in an encompassing manner. A key research topic regarding generalizability will be the validation of the linkage between external and internal value creation and the associated data resources. As research conducted for this paper as well as the study of Barbieri et al. [2] revealed, there is no common understanding of how this interaction and integration between the digital and the physical world is done in a way to realize value creating smart services. However, several limitations of the proposed conceptual model need to be considered. The differentiating dimensions and their values enclose vague expressions due to the avoidance of features which relate to specific fields, such as industries or implementation technologies. The literature basis was further limited to Scopus database and therefore the research might by missing particular publications, however through the backward research and the recommendations by senior researchers the essential publications are covered. The approach must evolve, as the development of the DT especially in practice is still at the outset and research as well as real cases in the field are just emerging. Prospective research and use cases may validate and refine the proposed systematization and three-dimensional representation of DTs. This might lead to adding new dimensions or refining the definitions and categories of dimensions outlined in this paper.

5. REFERENCES

[1] Dawid, H., Decker, R., Hermann, T., Jahnke, H., Klat, W., König, R., & Stummer, C. (2016). Management science in the era of smart consumer products: challenges and research perspectives. Central European Journal of Operations Research, 25(1), 203–230. doi:10.1007/s10100-016-0436-9

[2] Barbieri, C., West, S., Rapaccini, M. & Meierhofer, J. (2019). Are practitioners and literature aligned about digital twin? 26th EurOMA Conference Operations Adding Value to Society. Conference Paper.

[3] Zheng, Y., Yang, S., & Cheng, H. (2018). An application framework of digital twin and its case study. Journal of Ambient Intelligence and Humanized Computing, 10(3), 1141–1153. doi:10.1007/s12652-018-0911-3

[4] Schleich, B., Anwer, N., Mathieu, L., & Wartzack, S. (2017). Shaping the digital twin for design and production engineering. CIRP Annals, 66(1), 141–144. doi:10.1016/j.cirp.2017.04.040

[5] Porter, M. W. & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. Harvard Business Review 92: 64–88.

[6] Porter, M. W. & Heppelmann, J. E. (2015). How smart, connected products are transforming companies. Harvard Business Review 93: 97–114.

[7] Wuenderlich, N. V., Heinonen, K., Ostrom, A. L., Patricio, L., Sousa, R., Voss, C., & Lemmink, J. G. A. M. (2015). "Futurizing" smart service: implications for service researchers and managers. Journal of Services Marketing, 29(6/7), 442–447. doi:10.1108/jsm-01-2015-0040

[8] Grieves, M. (2014). Digital twin: Manufacturing excellence through virtual factory replication, White Paper.

[9] Tao, F., Zhang, M. & Nee, A.Y.C. (2019). Digital twin driven smart manufacturing. First Edition. United Kingdom, London Wall: Elsevier Inc.

[10] E. Glaessgen & D. Stargel (2012) : "The digital twin paradigm for future NASA and U.S. Air Force vehicles," in Proc. 53rd AIAA/ASME/ASCE/AHS/ASC Struct. Struct. Dyn. Mater. Conference. https://doi.org/10.2514/6.2012-1818

[11] Detzner, A., & Eigner, M. (2018). A digital twin for root cause analysis and product quality monitoring. Proceedings of the DESIGN 2018 15th International Design Conference, 1547-1558. doi:10.21278/idc.2018.0418

[12] Grieves, M., & Vickers, J. (2016). Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. Transdisciplinary Perspectives on Complex Systems, 85–113. doi:10.1007/978-3-319-38756-7_4

[13] Landahl, J., Panarotto, M., Johannesson, H. Isaksson, O. & Lööf, J. (2018). Towards Adopting Digital Twins to Support Design Reuse during Platform Concept Development. NordDesign 2018 August 14 – 17, 2018 Linköping, Sweden.

[14] Qi, Q., Tao, F., Zuo, Y., & Zhao, D. (2018). Digital Twin Service towards Smart Manufacturing. Procedia CIRP, 72, 237–242. doi:10.1016/j.procir.2018.03.103

[15] Shangguan, D., Chen, L., & Ding, J. (2019). A Hierarchical Digital Twin Model Framework for Dynamic Cyber-Physical System Design. Proceedings of the 5th International Conference on Mechatronics and Robotics Engineering - ICMRE'19. doi:10.1145/3314493.3314504

[16] Tao, F., Cheng, J., Qi, Q., Zhang, M., Zhang, H., & Sui, F. (2017). Digital twin-driven product design, manufacturing and service with big data. The International Journal of Advanced Manufacturing Technology, 94(9-12), 3563–3576. doi:10.1007/s00170-017-0233-1

[17] Tao, F., Sui, F., Liu, A., Qi, Q., Zhang, M., Song, B., Guo, Z., Lu, S.C., & Nee, A.Y. (2019). Digital twin-driven product design framework.

[18] Tao, F., Zhang, H., Liu, A., & Nee, A.Y. (2019). Digital Twin in Industry: State-of-the-Art. IEEE Transactions on Industrial Informatics, 15, 2405-2415.

[19] Uhlenkamp, J.-F., Hribernik, K., Wellsandt, S., & Thoben, K.-D. (2019). Digital Twin Applications: A first systemization of their dimensions. 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC). doi:10.1109/ice.2019.8792579

[20] Panetta, K., (2018). Gartner Top 10 Strategic Technology Trends for 2019. Published online October 15, 2018. https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/ Accessed 12 August 2019.

[21] Rais, A. (2019). Growth of the digital twin market. Published online August 2, 2019. https://www.maschinenmarkt.international/growth-of-the-digital-twin-market-a-851571/ Accessed 12 August 2019.

[22] Voell, C., Chatterjee, P., Rauch, A., & Golovatchev, J. (2018). How Digital Twins Enable the Next Level of PLM – A Guide for the Concept and the Implementation in the Internet of Everything Era. IFIP Advances in Information and Communication Technology, 238–249. doi:10.1007/978-3-030-01614-2_22

[23] Lee, J., Kao, H.-A., & Yang, S. (2014). Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment. Procedia CIRP, 16, 3–8. doi:10.1016/j.procir.2014.02.001

[24] Rosen, R., von Wichert, G., Lo, G., & Bettenhausen, K. D. (2015). About The Importance of Autonomy and Digital Twins for the Future of Manufacturing. IFAC-PapersOnLine, 48(3), 567–572. doi:10.1016/j.ifacol.2015.06.141

[25] Nyffenegger, F., Hänggi, R., & Reisch, A. (2018). A Reference Model for PLM in the Area of Digitization. IFIP Advances in Information and Communication Technology, 358–366. doi:10.1007/978-3-030-01614-2_33

[26] Tomiyama, T., Lutters, E., Stark, R., & Abramovici, M. (2019). Development capabilities for smart products. CIRP Annals, 68(2), 727–750. doi:10.1016/j.cirp.2019.05.010

[27] Meierhofer, J. & West, S. (2019). Service value creation using a digital twin. Conference Paper. 2019 Naples Forum on Service. Italy.

[28] Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R. & Cleven, A. (2009). Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process, ECIS, 2206-2217.

[29] Cooper, H.M. (1988). Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews. Knowledge in Society, 1: 104-126.

[30] Bakkalbasi, N., Bauer, K., Glover, J. and Wang, L. (2006). Three options for citation tracking: Google Scholar, Scopus and Web of Science, Biomedical Digital Libraries, Vol. 3 No. 7.

[31] Falagas, M. E., Pitsouni, E. I., Malietzis, G. A., & Pappas, G. (2008). Comparison of PubMed, Scopus, Web of Science, and Google Scholar: strengths and weaknesses. The FASEB Journal, 22(2), 338–342. doi:10.1096/fj.07-9492lsf

[32] Elsevier (2019). About Scopus, https://blog.scopus.com/about (Accessed: 09.08.2017).

[33] Rymaszewska, A., Helo, P. & Gunasekaran, A. (2017), "IoT powered servitization of manufacturing – an exploratory case study", International Journal of Production Economics, Elsevier, Vol. 192, pp. 92–105.

[34] Holler, M., Uebernickel, F. & Brenner, W. (2016): Digital Twin Concepts in Manufacturing Industries - A Literature Review and Avenues for Further Research. 2016. - 18th International Conference on Industrial Engineering (IJIE). - Seoul, Korea.

[35] Dreyer, S., Olivotti, D., Lebek, B., & Breitner, M.H. (2017). Towards a Smart Services Enabling Information Architecture for Installed Base Management in Manufacturing. Wirtschaftsinformatik.

[36] Damjanovic-Behrendt, V., & Behrendt, W. (2019). An open source approach to the design and implementation of Digital Twins for Smart Manufacturing. International Journal of Computer Integrated Manufacturing, 32(4-5), 366–384. doi:10.1080/0951192x.2019.1599436

[37] Malakuti, S., Goldschmidt, T., & Koziolek, H. (2018). A Catalogue of Architectural Decisions for Designing IIoT Systems. Lecture Notes in Computer Science, 103–111. doi:10.1007/978-3-030-00761-4_7

[38] Wuest, T., Hribernik, K., & Thoben, K.-D. (2015). Accessing servitisation potential of PLM data by applying the product avatar concept. Production Planning & Control, 26(14-15), 1198–1218. doi:10.1080/09537287.2015.1033494

[39] Fuchs, R. & Barth, L. (2018). Wie Smart Connected Products Kunden emotionalisieren. In: Rueger, et al. (2018): Emotionalisierung im digitalen Marketing: Erfolgreiche Methoden für die Marketingpraxis, 89–103.

[40] Longo, F., Nicoletti, L. & Padovano, A. (2019): Ubiquitous knowledge empowers the Smart Factory: The impacts of a Service-oriented Digital Twin on enterprises' performance, Annual Reviews in Control, https://doi.org/10.1016/j.arcontrol.2019.01.001

[41] Zhang, H., Zhang, G., & Yan, Q. (2018). Digital twin-driven cyber-physical production system towards smart shop-floor. Journal of Ambient Intelligence and Humanized Computing. doi:10.1007/s12652-018-1125-4

[42] Patel, P., Ali, M. I., & Sheth, A. (2018). From Raw Data to Smart Manufacturing: AI and Semantic Web of Things for Industry 4.0. IEEE Intelligent Systems, 33(4), 79–86. doi:10.1109/mis.2018.043741325

[43] Nakajima, S. (1988), "Introduction to Total Productive Maintenance", Cambridge, MA, Productivity Press.

[44] Leflar, J. (1999). TPM at Hewlett-Packard. 10th Total Productive Maintenance Conference, Las Vegas, NV, Productivity, Inc.

[45] VDMA - Mechanical Engineering Industry Association, DIN 8743 information available under https://www.vdma.org/en/v2viewer/-/v2article/render/27106441

[46] Bange, U. K. (2019): Overall Service Effectiveness - Eine Adaption des OEE-Modells auf die Digitalisierung von After-Sales/Service. Retrieved from: https://www.linkedin.com/pulse/overall-service-effectiveness-eine-adaption-des-auf-udo-k-bange/

[47] Novikov, D. (2016). Cybernetics. Studies in Systems, Decision and Control. doi:10.1007/978-3-319-27397-6

[48] Beer, S. (1972): Brain of the Firm; Allen Lane, The Penguin Press, London, Herder and Herder, USA.

[49] Ashby, W.R. (1956): An introduction to Cybernetics. Wiley, New York.

[50] Hartmann, D., Herz, M., & Wever, U. (2018). Model Order Reduction a Key Technology for Digital Twins. Reduced-Order Modeling (ROM) for Simulation and Optimization, 167–179. doi:10.1007/978-3-319-75319-5_8

[51] Wagner, C., Grothoff, J., Epple, U., Drath, R., Malakuti, S., Gruner, S. & Zimermann, P. (2017). The role of the Industry 4.0 asset administration shell and the digital twin during the life cycle of a plant. 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). doi:10.1109/etfa.2017.8247583

[52] Malakuti, S., & Grüner, S. (2018). Architectural aspects of digital twins in IIoT systems. Proceedings of the 12th European Conference on Software Architecture Companion Proceedings - ECSA '18. doi:10.1145/3241403.3241417

[53] Guo, N. & Jia, C. (2017). Interpretation of Cyber-Physical Systems. Whitepaper. Information Technology & Standardization, 2017;(4): 36-47.

[54] Zheng, P., Lin, T.-J., Chen, C.-H., & Xu, X. (2018). A systematic design approach for service innovation of smart

product-service systems. Journal of Cleaner Production, 201, 657–667. doi:10.1016/j.jclepro.2018.08.101

[55] West, S., Gaiardelli, P., Resta, B., Kujawski, D. (2018): Co-creation of value in Product-Service Systems through transforming data into knowledge, IFAC-PapersOnLine, vol. 51, iss. 11, pp. 1323-1328

[56] Canedo, A. (2016). Industrial IoT lifecycle via digital twins. Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis - CODES '16. doi:10.1145/2968456.2974007

[57] Boschert, S., Rosen, R. (2016): Digital twin - the simulation aspect. In Mechatronic Futures: Challenges and Solutions for Mechatronic Systems and Their Designers, 59-74. doi:10.1007/978-3-319-32156-1_5

[58] Tao, F., & Zhang, M. (2017). Digital Twin Shop-Floor: A New Shop-Floor Paradigm Towards Smart Manufacturing. IEEE Access, 5, 20418–20427. doi:10.1109/access.2017.2756069

[59] Abramovici, M., Göbel, J. C., & Dang, H. B. (2016). Semantic data management for the development and continuous reconfiguration of smart products and systems. CIRP Annals, 65(1), 185–188. doi:10.1016/j.cirp.2016.04.051

[60] Negri, E., Fumagalli, L., & Macchi, M. (2017). A Review of the Roles of Digital Twin in CPS-based Production Systems. Procedia Manufacturing, 11, 939–948. doi:10.1016/j.promfg.2017.07.198

[61] Stark, R., Fresemann, C., & Lindow, K. (2019). Development and operation of Digital Twins for technical systems and services. CIRP Annals, 68(1), 129–132. doi:10.1016/j.cirp.2019.04.024

[62] Tharma, R., Winter, R., & Eigner, M. (2018). An approach for the implementation of the digital twin in the automotive wiring harness field. Proceedings of the DESIGN 2018 15th International Design Conference. doi:10.21278/idc.2018.0188

[63] Baines, T. and Lightfoot, H. (2013) Made to Serve: How Manufacturers Can Compete through Servitization and Product Service Systems. Wiley.

[64] Vandermerwe, S., & Rada, J. (1988). Servitization of business: Adding value by adding services. European Management Journal, 6(4), 314–324. doi:10.1016/0263-2373(88)90033-3

[65] West, T. D., & Pyster, A. (2015). Untangling the Digital Thread: The Challenge and Promise of Model-Based Engineering in Defense Acquisition. INSIGHT, 18(2), 45–55. doi:10.1002/inst.12022

[66] Terzi, S., Bouras, A., Dutta, D., Garetti, M. & Kiritsis, D. (2010). Product Lifecycle Management – From Its History To Its New Role, International Journal of Product Lifecycle Management 4(4), pp. 360-389.

[67] Cerrone, A., Hochhalter, J., Heber, G., & Ingraffea, A. (2014). On the effects of modeling as-manufactured geometry: Toward Digital Twin. International Journal of Aerospace Engineering, 2014 . doi: 10.1155/2014/439278 . ArticleID 439278

[68] Söderberg, R., Wärmefjord, K., Carlson, J. S. & Lindkvist, L. (2017). Toward a Digital Twin for real-time geometry assurance in individualized production. CIRP Annals, 66 (1), 137–140.

[69] Kung, C. H., & Solvberg, A. (1986): Activity Modeling and Behavior Modeling, In: Ollie, T., Sol, H. & Verrjin-Stuart, A.: Proceedings of the IFIP WG 8.1 working conference on comparative review of information systems design methodologies: improving the practice. North-Holland, Amsterdam, pp. 145–171.

Research on Parallel Data Currency Rule Algorithms

Xuliang Duan
College of Computer Science, Sichuan University
Chengdu 610065, China
+8615008305394
duanxuliang@sicau.edu.cn

Bing Guo*
College of Computer Science, Sichuan University
Chengdu 610065, China
+8613980664852
guobing@scu.edu.cn

Yan Shen*
School of Control Engineering, Chengdu University of Information Technology
Chengdu 610065, China
sheny@cuit.edu.cn

Yuncheng Shen
College of Computer Science, Sichuan University
Chengdu 610065, China
+8613887086156
403953413@qq.com

Xiangqian Dong
College of Computer Science, Sichuan University
Chengdu 610065, China
+8613551092851
dongxiangqian@nsu.edu.cn

Hong Zhang
College of Computer Science, Sichuan University
Chengdu 610065, China
+8613608210882
945389781@qq.com

ABSTRACT
Data currency is a temporal reference of data, which is related to the value of data and affects the results of data analysis and mining. The currency rules that reflect the time series features of data can be used not only for data repairing, but also for data quality evaluation. However, with the rapid growth and dynamic update of data volume, both the forms and algorithms of basic currency rule are facing severe challenges in application. Therefore, based on the research on data currency repairing, we extended the basic currency rule form, and proposed rule extraction and incremental updating algorithms that can run in parallel on dynamic data set. The experimental results show that, compared with non-parallel methods, the efficiency of parallel algorithms is significantly improved.

CCS Concepts
• Information systems→Data cleaning • Computing methodologies→Massively parallel algorithms.

Keywords
Data currency; data currency rule; parallel algorithm; dynamic data.

1. INTRODUCTION
Currency is an important feature of data, it is a temporal reference that reflects the degree to which the data is current with the world it models. Scholars carried out research on data quality through direct observation, social investigation, theoretical derivation, etc., and obtained the characteristics that have great influence on data availability: accuracy, completeness, consistency, currency and entity identity [1]. In 2002, an expert report pointed out that in the field of business, at least 2% commercial data is obsolete every month due to changes in customer information [2,3]. There are a lot of time-disrupted data in our data sets, if we can't identify which one is "latest", data queries may return incorrect results, and data analysis may lead to ambiguous conclusions, followed by data quality degradation and data value reduction.

In the era of big data and artificial intelligence, personal big data as a valuable asset is growing exponentially. But the vague of property-right, chaotic in management and difficulty in liquidity severely affect the regular development of personal big data market [4]. Individuals' various types of data are decentralized in different platforms and systems, the data quality problems caused by obsolescence and inaccurate currency become more and more serious. Personal data is a typical kind of dynamic data. The data reflecting the status of people's work and life is constantly changing with time, and the changing feature is also the biggest challenge in the data cleaning process. The time attributes of these multi-source heterogeneous data are often inaccurate, which brings great challenges to data quality and data value [5]. For some attributes of the data, different times correspond to different values or different states, such as a person's degree changes, marital status changes, etc. If the timestamp is incomplete or inaccurate, the order of the records cannot be determined which will brings great difficulties in data analysis and value-added application.

Around 2011, Fan et al. proposed the currency-repairing method based on data semantics. Under the assumption that one entity may have multiple tuples in datasets, Fan et al. conducted in-depth research on the fields of model for data currency, reasoning about data currency and currency preserving copy functions, etc., and formalized the related definition and concepts, and promoted basic research in this field [6,7]. On the basis of this work, a series of fruitful researches have promoted the research progress of data currency-repairing in theory and practice. Fan et al. [8] inferred the available time information of the data according to the currency order of the data, determined the latest value of the data according to the currency rules and constant conditional dependency function, and solved the inconsistency of different tuple attributes of the same entity to a certain extent. Li et al. carried out researches on data currency and currency evaluation,

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388210

proposed a series of solutions to improve data currency, domain knowledge can be directly expressed by the antecedents and consequents of rules, and the statistical information can be described by the distribution table of each rule [9].

Based on the requirements of repairing data currency order, Duan et al. proposed a data currency rule model that does not require domain knowledge [10]. The algorithm extracts the currency rules and their support value by scanning the state changes of an attribute value of the data set. The currency rules can be used to repair data that missing currency order, and also provides feasibility solution for the quality evaluation of data currency.

Take the following student's course selection records as an example, shown in Table 1, Eve's Database semester is missing, it is possible for us to repair it according to certain rules. For Alice and Bob, the following 3 rules "C Programming→Data Structure", "C Programming→Database", "Data Structure→Database" all exist in their course selection sequence. Therefore, although Eve's Database semester is unknown, but as Eve has chosen a "Data Structure" in his second semester, we can infer that the semester of Eve's "Database" will not be earlier than that of "Data Structure" according to Alice and Bob's rule "Data Structure→Database". Although it is not certain whether the semester is 3 or 4, we know that it has a high probability of being greater than 2, so we can determine the order of the two records of Eve.

Table 1. Student's course selection tuples

TID	EID	Name	Course	Semester
t1	S1	Alice	C Programming	1
t2	S1	Alice	Data Structure	2
t3	S1	Alice	Database	4
t4	S2	Bob	C Programming	1
t5	S2	Bob	Data Structure	2
t6	S2	Bob	Database	3
t7	S3	Eve	Database	NULL
t8	S3	Eve	Data Structure	2

Liang and Duan et al. analyzed and mined the students' course selection data set based on the currency rules and decision trees [11]. This is an application study of currency rules for data currency quality evaluation, they evaluated each student's course selection data based on the mean value of the rules' supports, and found that data with poor currency quality often correspond to some abnormal situations of students, which can be used for abnormal warning in teaching management.

2. RELATED WORKS

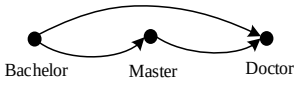
Currency rules for attribute states. On the relationship R, all the non-repetitive state values of the attribute A_i are a finite set, and the currency rules state diagram are expressed by a directed graph G(V, E), wherein the vertex set V represents the finite set of attribute values (states), and the directed edge set E represents the direction of state transition with chronological order. For the two tuples t_1 and t_2 of the same entity on the relationship R, the values of the attributes A_i are v_1, v_2, and v_1 and v_2 are the state nodes in the graph G. If t_2 is newer than t_1, for the nodes v_1 to v_2 is reachable and meanwhile v_2 to v_1 is unreachable, we call $v_1 \rightarrow v_2$ is a state currency rule, which is expressed as follows:

$$\forall t_1, t_2 \in R, t_1[EID] = t_2[EID], t_1[A_i] = v_1, t_2[A_i] = v_2, \\ v_1 \in G, v_2 \in G, t_1 \prec t_2 \rightarrow (v_1 \rightarrow v_2 \wedge v_2 \nrightarrow v_1)$$

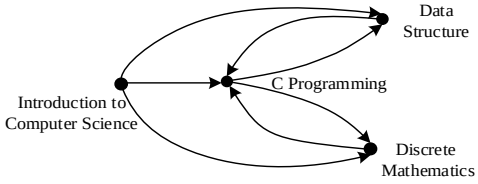
Similarly, on a consistent data set, we can determine:

$$\forall t_1, t_2 \in R, t_1[EID] = t_2[EID], t_1[A_i] = v_1, t_2[A_i] = v_2, \\ v_1 \in G, v_2 \in G, (v_1 \rightarrow v_2 \wedge v_2 \nrightarrow v_1) \rightarrow t_1 \prec t_2$$

The transition of attribute states can be represented by state diagrams. Figure 1 shows two sample state transition diagrams. It should be noted that in the degree state transition diagram, *Bachelor* to *Master*, *Master* to *Doctor* are all irreversible transition, and even if the intermediate state *Master* is ignored, the *Bachelor* to *Doctor* transition is also irreversible. Similar situation exists in the course election transition diagram.



(a) One's degree states at different periods



(b) Course selection states of different semesters

Figure 1. Degree and course selection state transition diagrams.

3. PARALLEL CURRENCY RULE ALGORITHMS

3.1 Extending for the Basic Currency Rule

Duan et al. proposed the basic form of the currency rule is {*rule*, *support*}, and the rules are extracted by scanning all the records of a data set [10]. After extraction, if new records are added to the data set, it is necessary to scan the entire new data set to update previous currency rule set. Moreover, the currency rules updating can only be performed on a single node, the cost is high for dynamic, large-scale data set. In order to achieve the parallelization of the algorithms, we improved and extended the form of basic currency rule. The extended currency rule extraction and updating algorithms can not only run on multiple nodes in parallel, but also incrementally update the currency rule set on a dynamic data set.

The extended currency rule retains more information in the form of {*rule*, *obey*, *violation*, *pathlength*}. The *obey* is the number of entities that satisfy the rule in the data set. The *violation* indicates the number of entities that violate the rule in the data set. The *pathlength* represents the average number of edges between the start and the end state in the rule. After expansion, the support and strength values can be dynamically calculated when needed by *obey* and *violation*. The *pathlength* of each rule is calculated as follows:

$$PL = \frac{\sum L(r_o) + \sum L(r_v)}{|O(r)| + |V(r)|}, r_o \in O(r), r_v \in V(r)$$

Where $L(r)$ represents the path length of the rule in the record set of an entity, $\sum L(r_o)$ indicates the sum of the path lengths obeying the rule, $\sum L(r_v)$ is the sum of the path lengths that violate the rule, and $|O(r)|$ indicates the number of entities obeying the rule, $|V(r)|$ indicates the number of entities that violate this rule.

3.2 Currency Rule Extraction Algorithm

Currency rule extraction algorithm is shown in **Algorithm 1**. The input data set consists of records from multiple entities, each

entity has multiple records, and each record tuple has an order label attribute. The input data set should be preprocessed, cleaned and consistent data. The output is a currency rule set extracted from the input data set in the form of {*rule*, *obey*, *violation*, *pathlength*}.

Algorithm 1. Currency Rules Extraction Algorithm

Input: A data set containing multiple entities for rule extraction;
Output: Currency rule set presented by hash table;
initialize RuleHash; //{rule, obey, violation, pathlength}
for each e∈E do{
Re = select * from R where eid=e.eid order by timespan ASC;
// Sort all records of entity *e* in ascending
for(i=0;i<Re.Count;i++){
currentTimesindex = Re[i].timeindex;
currentStatus = Re[i].status;
for (int j = i + 1; j < Re.Count; j++) {
nextTimeindex = Re[j].timeindex;
nextStatus = Re[j].status;
ruleLength= nextTimeindex – currentTimesindex;
if (nextTimeindex > currentTimeindex) {
rule = currentStatus → nextStatus;
if (!RuleHash.ContainsKey(rule)) {
RuleHash.Add(rule,{obey=1,violate=0,length= ruleLength});}
else {
RuleHash[rule].length = (RuleHash[rule].length* RuleHash[rule].obey+ruleLength)/(RuleHash[rule].obey + 1);
RuleHash[rule].obey= RuleHash[rule].obey+1; } }
}
}
}
return RuleHash;

The extended currency rule supports incremental updating. As the currency rules have been extracted, and the *obey*, *violation*, *length* values of each rule have been calculated, assuming that some records are added to the original data set, there is no need to scan the entire set, but only need to scan the newly added data and update the previously generated rule set, the rule set can be incrementally updated. Incremental updates enhance the flexibility and adaptability of the algorithm.

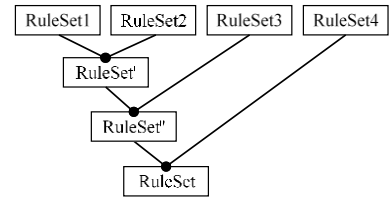
3.3 Rule Sets Merging Algorithm

The currency rule extraction algorithm can run in parallel. A possible parallel solution is to divide a large data set into multiple small ones and distribute them on different nodes, each node independently runs currency rule extraction algorithm, finally, the **Rule Sets Merging Algorithm** merges these rule sets extracted from small data sets into a complete currency rule set. The merge algorithm solves the problem of parallel rule extraction, at same time, it also supports incrementally updating the rule set on dynamic increasing data. Algorithm 2 shows the merging process:

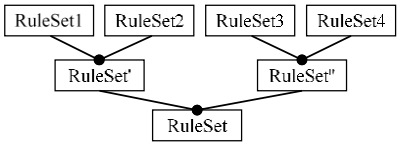
Algorithm 2. Currency Rule Sets Merging Algorithm

Input: two rule sets *RuleSet*1, *RuleSet*2, merge *RuleSet*2 into *RuleSet*1
Output: A complete *RuleSet*1
Merge(RuleSet1,RuleSet2)
foreach(rule<key,value> in RuleSet2)
if(RuleSet1.Contains(key))
RuleSet1[key].length=(RuleSet1[key].obey* RuleSet1[key].length + value.obey * value.length) / (value.obey + RuleSet1[key].obey);
RuleSet1[key].obey=value.obey + RuleSet1[key].obey;
RuleSet1[key].violate=value.violate + RuleSet1[key].violate;
else RuleSet1.add(key,value);
return RuleSet1;

When merging rule sets, two strategies can be used. The first strategy is to merge the 2, 3, 4, ... *n* rule set into the first set. After the last set is merged, the first set is a complete rule set. This strategy can't be executed in parallel, and the time complexity is $O(n\text{-}1)$; The second strategy, rule sets merging can be run in parallel on different nodes and finally be merged into a complete rule set, the time complexity is $O(\log(n))$. The two strategies diagrams are as shown in Figure 2:



(a) Merging rule sets in order



(b) Merging rule sets in parallel

Figure 2. Two rule sets merging strategies.

4. EXPERIMENT AND ANALYSIS

4.1 Experimental Platform and Data

The experimental platform is a host allocated from a hyper-converged server. The host is configured with Intel T7700 2.4GHz CPU, 20 cores, 16G RAM and Windows 10 operating system. The algorithms are all written in C#, running on .Net Framework 4.5. The test datasets and rules set are stored in MySQL 5.7 database.

Test Dataset. The experimental data set is derived from the course elective data of students in a university from 2014 to 2019. The data consistency is high and there is no abnormal data. The data fields include the course name, class number, student number, and semester. In the test dataset, there are total 741809 courses elective records, the data covers from the first to the sixth semester of 12278 students, with an average of about 60 records per student. The relevant terms mentioned in the experiment are explained as follows:

(1) **State**. State refers to the node in the state diagram. In the experiment, we select the course name as the state, the same course name represents the same state, and different course names represent different states. The test courses election datasets have a total of more than 2,200 courses, which means that the number of nodes in the entire state diagram will not exceed the number of courses.

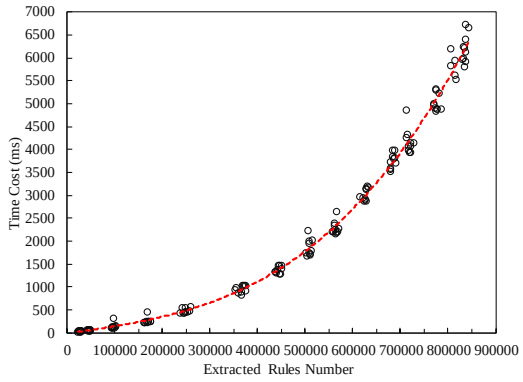
(2) **Entity**. The entity in the experiment is the student ID. In the test dataset, an entity has multiple data records, that is, one student

has multiple courses elective records, and the records with the same student ID are the same student's elective data.

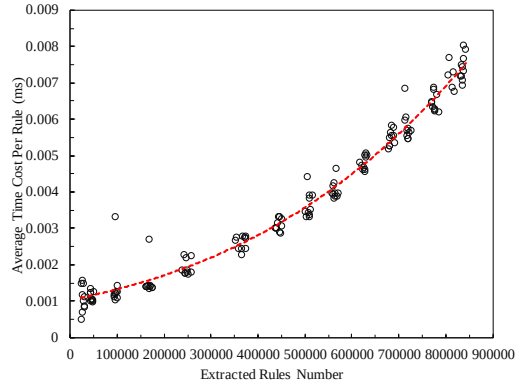
4.2 Performance Testing for Rules Extraction

For the rule extraction performance test, currency rules are extracted from 15 entities sets of different sizes, test 10 rounds. Test entities are randomly selected from the test dataset, and the number of entities in the test sets are sequentially incremented in a certain gradient. There are 10 entities in the first(smallest) set, and 2700 entities in the last(largest) set. Since the test entities are randomly selected, even if the number of entities of the test set is the same, the number of rules extracted from the set is generally different. Of all 10 rounds, the minimum number of rules for the set of 10 entities is 20482, and the maximum number for the set of 2700 entities is 852131.

(1) Non-parallel test for rules extraction algorithm. The results of 150 tests for all 10 rounds are shown in the Figure 3 below. The horizontal axis indicates the number of rules and the vertical axis indicates the time consumed (in milliseconds). Figure 3 (a) shows the time-cost of extracting rules for each set varies as the rules number increases. Figure 3 (b) shows the average time-cost of each rule varies as the rules number increases. In the best case, 23,403 rules are extracted per millisecond, and in the worst case, only 622 rules are extracted per millisecond. Due to computer storage and computational resource limitations, the rules extraction time consumption and the rules number do not show a linear growth trend of ideal conditions. In the Microsoft Excel, a trend line and a fitted polynomial function are added to the scatter plot, and it can be found that the time cost and the rules number shows a polynomial growth trend. A similar situation also occurs in the average time cost of each rule.



(a) Total time cost of rules extraction



(b) Average time cost of each rule.

Figure 3. Performance test for rules extraction algorithm.

(2) Parallel Test for Rules Extraction Algorithm. From the test dataset, 1,771,292 records of 28,076 entities are selected for doing parallel test. The total number of currency rules is 5,573,732. The test run 10 rounds, for each round, we set 1 to 24 parallel threads to test the algorithm performance under different parallel threads. Take the average as the result in the case of the same parallel threads number.

The experimental results show that the parallelization has obvious improvement on the algorithm efficiency. For test task, single-threaded operation takes 90,352.75 milliseconds, and when 15 threads are paralleled, it reaches a minimum of 22,399.22 milliseconds, resulting in an efficiency increase of 75.20%. The experimental results also show that when the of parallel number is greater than 10, due to server storage, disk IO, etc., continuing to increase parallel threads does not continuously reduce time consumption. Test results are shown in **Figure 4**.

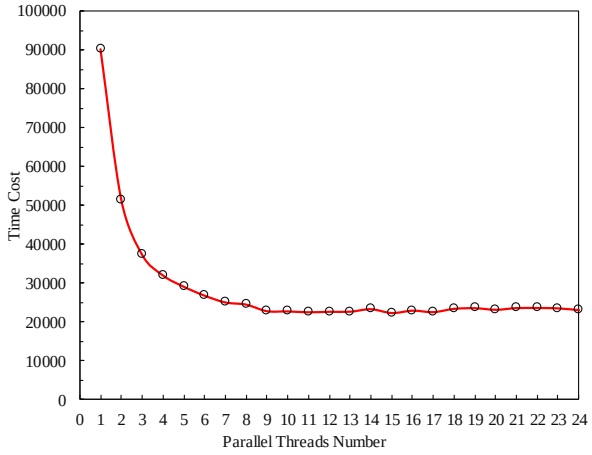


Figure 4. Parallel test for rules extraction algorithm.

4.3 Performance Test for Rules Merging Algorithms

During the process of merging two rule sets, the left set *R*1 and the right *R*2, it is necessary to traverse each rule in left set *R*1 to check whether it exists in the rule set *R*2. Since *R*1 and *R*2 are both hash tables, the traversal *R*1 algorithm is $O(n)$ linear complexity, and check rule whether in *R*2 is $O(1)$ constant complexity. It can be seen that the merging cost is mainly determined by the size of the rule set *R*1.

(1) Non-parallel test for rule sets merging algorithm. Performance test is carried out for 10 rounds. Each round of testing uses 30 entity sets, and each entity sets contains 10 to 5000 entities randomly selected from the data set under a certain gradient. Correspondingly, 30 rule sets are extracted from the 30 entity sets. Of the total 300 tests in 10 rounds, the rules number for the left rule sets ranges from 22317 to 867139, and for the right sets it is 12254 to 541369. There are 867,139 rules in the largest left set *R*1, and the corresponding right *R*2 has 541369 rules. In the 10 rounds testing, the average time consuming of merging the two rule sets is 255.5ms. The results of the 10 rounds of testing are shown in Figure 5. It can be found that the merging time-consuming is linear with the scale of left rule set.

(2) Parallel test for rule sets merging algorithm. In parallel testing, for each round of testing, set 1 to 24 parallel threads to merge the 30 rule sets. Finally, count the data for 10 rounds of testing and calculate the average time cost based on the number of threads.

In the case of non-parallel (single-threaded), merging 30 rule sets takes an average of 3802 milliseconds, paralleling two threads takes 2466 milliseconds. A minimum of 1702 milliseconds is obtained when 22 threads are executed in parallel, brings efficiency improvement of 55.23%. Experiments show that the parallel algorithm is effective, and parallelization can significantly improve the merging efficiency. Since this experiment is performed on a single server, limited by hardware limitations and resource coordination between multiple threads, when the number of threads is greater than 10, the performance improvement is no longer obvious. The parallel performance results are shown in Figure 6.

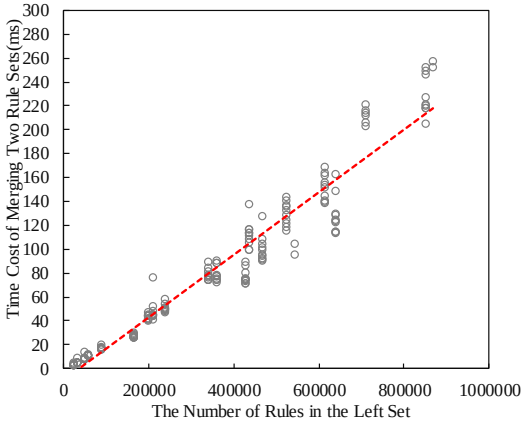


Figure 5. Performance test for merging algorithm.

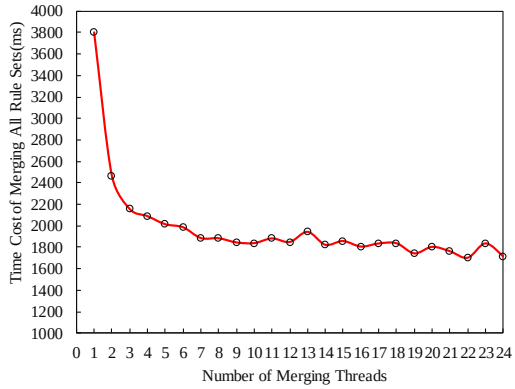


Figure 6. Parallel test for merging algorithm.

5. CONCLUSIONS

Currency rules can be used for both data repairing and data quality evaluation. Based on the current research on data currency, this paper further studied the dynamic updating and parallelization algorithms of currency rules, and proposes several data ageing quality evaluation models. The main research results are as follows:

(1) Extending the basic currency rule. The extended currency rules can be updated incrementally, and the new added path length attribute can provide more effective information for currency quality evaluation.

(2) Proposing parallel extraction and merging algorithms for currency rules. Experimental tests show that the parallel algorithms are effective. Compared with non-parallel algorithms, the extraction performance is improved by 75.20%, merging performance is improved by 55.23%, and the evaluation performance is improved by 85.86%.

In future research, we will build data currency quality evaluation models based on currency rules to evaluate the quality of data currency.

6. ACKNOWLEDGMENTS

This work was supported in part by the National Natural Science Foundation of China under Grant No. 61772352; the Science and Technology Planning Project of Sichuan Province under Grant No. 2019YFG0400, 2018GZDZX0031, 2018GZDZX0004, 2017GZDZX0003, 2018JY0182, 19ZDYF1286.

7. REFERENCES

[1] Ding XO, Wang HZ, Zhang XY, Li JZ, Gao H. 2016. Association relationships study of multi-dimensional data quality. *Ruan Jian Xue Bao/Journal of Software*. 27, 7 (Jul. 2016), 1626-1644. DOI= 10.13328/j.cnki.jos.005040

[2] Eckerson W W. 2002. *Data quality and the bottom line: Achieving business success through a commitment to high quality data*. Washington: The Data Warehouse Institute.

[3] Fan WF, Greets F. 2012. *Foundations of data quality management*. Morgan & Claypool Publishers.

[4] Guo B, Li Q, Duan XL, et. al. 2017. Personal data bank: a new mode of personal big data asset management and value-added services based on bank architecture. *Chineses Journal of Computers*, (Jan. 2017), 126-143. DOI=10.11897/SP.J.1016.2017.00126

[5] Zhang H, Diao Y, Immerman N. 2013. Recognizing patterns in streams with imprecise timestamps. *Information Systems*. 38, 8(Nov. 2013), 1187-1211. DOI=10.1016/j.is.2012.01.002

[6] Fan W, Geerts F, Wijsen J. 2012. Determining the currency of data. *ACM Trans. Database Syst*. 37,4 (Dec. 2012), 1-46. DOI=10.1145/2389241.2389244

[7] Fan W, Geerts F, Tang N, et al. 2014. Conflict Resolution with data currency and consistency. *ACM Journal of Data and Information Quality (JDIQ)*. 5,6 (Sep. 2014), 1-6. DOI=10.1145/2631923

[8] Fan WF, Geerts F., Yu W. et al. 2014. Conflict resolution with data currency and consistency. *Journal of Data & Information Quality*, 5, 6(Sep. 2014). DOI=10.1145/2631923

[9] Li MH, Li JZ. A minimized-rule based approach for improving data currency. 2016. *Journal of Combinatorial Optimization*. 32, 3 (Mar. 2016) 812-841. DOI=10.1007/s10878-015-9904-8

[10] Duan XL, Guo B, Shen YC et al. 2019. Data repair algorithm based on currency rules. *Ruan Jian Xue Bao/Journal of Software*. 30, 3 (Mar. 2019), 589-603. DOI=10.13328/j.cnki.jos.005688

[11] Liang Y, Duan XL, Ding YJ et al. 2019. Data Mining of Students' Course Selection Based on Currency Rules and Decision Tree. In *Proceedings of the 2019 4th International Conference on Big Data and Computing (ICBDC 2019)*. Wuhan, China, 2019. DOI=10.1145/3335484.3335541

A Pair Estimation Technique of Effort Estimation in Mobile App Development for Agile Process: Case Study

Abdullah Altaleb
School of Electronics and Computer Science
University of Southampton, UK
Imam Mohammad Ibn Saud Is. University, Riyadh, KSA
a.altaleb@soton.ac.uk

Muna Altherwi
School of Electronics and Computer Science
The University of Southampton
Southampton, United Kingdom
m.altherwi@soton.ac.uk

Andy Gravell
School of Electronics and Computer Science
The University of Southampton
Southampton, United Kingdom
amg@ecs.soton.ac.uk

ABSTRACT
Effort estimation plays a vital role in the software development process in order to ensure that development tasks are delivered within the planned time. The characteristics of the mobile app environment make it different in terms of development from other traditional software. This paper presents a case study in an IT company, which examined their current estimation techniques, planning poker and expert judgment techniques, and its process in agile, and it provides and has validated a proposed estimation technique in order to enhance the accuracy of the existing technique. Moreover, this study presents the effectiveness of estimation factors/predictors in supporting the development team to manage, estimate and create subtasks for their user stories.

CCS Concepts
• **Software and its engineering→Agile software development.**

Keywords
Effort Estimation; Agile Development Process; Estimation Factors and Predictors; Estimation Techniques; Mobile App.

1. INTRODUCTION
Effort estimation is not crucial for constructing a project's scheduling and planning; however, effort estimation is necessary for the development team members and clients to facilitate and understand the project's functionalities in more detail [1]. Planning Poker is the most frequently used technique in the context of Agile software development [2], [3]. Estimating the effort in mobile app development faces several challenges and special constraints due to the characteristics and specifications of the mobile app environment [4]–[7]. The Planning Poker and Expert Judgment techniques suffer from ad-hoc activity during estimation, and the development team do not rely on a baseline for their estimation. Therefore, the aim of this study is to evaluate the existing estimation technique used in an IT company, and then design a proposed estimation technique in order to enhance the current estimation accuracy and its process.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388212

2. RELATED WORK
An empirical study was conducted to investigate the effort estimation techniques for mobile app development and its accuracy [8]. The study involved 20 practitioners working in different fields of software development from 18 organisations in different countries. The goal of the study was to explore the estimation technique and its process in Agile used in mobile app development. Also, the study provides the accuracy level of the estimation techniques that are used in mobile app development. The results of the study show that Planning Poker and Expert Judgment techniques are the most commonly used in mobile app development, and around 50% of professionals have an error ratio of between 25%-45% in their estimation. Related to this study, an industrial investigation study provided 62 comprehensive effort estimation factors/predictors that effect the accuracy level of the estimation, along with examining its validity in the context of mobile app development [9].

3. RESEARCH METHODOLOGY
The case study method has been used in this research study, and it may be called a "field study" or "observational study", as it involves a particular aspect of the research methodology [10]. This case study began with an empirical investigation of effort estimation techniques in IT companies to understand how the companies estimate the effort of user stories in order to develop a mobile app and verify the influence of estimation factors/predictors on the accuracy of the effort estimation. In addition, the case study will validate the proposed technique and measure its effectiveness. In this research, we have followed the case study guidelines and processes in software engineering according to [10].

3.1 Case Study Objectives
To know what is the objective and goal of the case study, it is useful to state a question and to simplify it to make it clear, and show what is expected to be achieved from the case study. Hence, the objectives of this case study are to:

- Understand the current state of practice for the estimation process and techniques that are used in mobile app development in Agile process.
- Evaluate the accuracy of the current estimation techniques in the organisation.
- Explore the estimation method and factors that affect the inaccuracy of the estimation value.

- Assess the effectiveness of the current estimation techniques, Planning Poker and Expert Judgment, in the context of mobile app development.
- Explore the challenges that effect the estimation accuracy.
- Validate the effectiveness of effort estimation factors/predictors in the accuracy of the effort estimation.
- Analyse the validity and effectiveness of the proposed estimation techniques "pair estimation" and its adoption by the development team.

3.2 Case Study Process

The case study was applied in a medium size IT company that has around 150 employees. The case study was directed and processed as shown in the following steps:

3.2.1 Obtain Historical Data from Previous Projects

At the beginning of the case study, the researcher discussed the following issues with the project manager/product owner:

- Previous estimation models or techniques the company has followed in previous projects.
- Historical data of project and team performance to know the velocity of the development team.
- From the data history, we discussed the accuracy of the estimated effort and actual effort of the project overall, and the user stories, to discover the accuracy level of the estimation model.

3.2.2 Type of Current Estimation Techniques

From the previous data, a focus group meeting was conducted with the product owner and the development team members to discuss how to improve the existing model or technique. Also, during the focus group, the Checklist model [11] was presented, and there was a discussion about whether the model could help them to improve their estimation. In the discussion, the development team were asked about how best to adopt the proposed model in the current estimation model, and how to assess the effectiveness of the estimation factors/predictors to improve estimation accuracy.

3.2.3 Sprint Planning, Review and Retrospective Preparations

In the sprint planning phase, the development team members followed and applied what was discussed and agreed on in the focus group meeting for the estimation process. It was ensured that the proposed estimation process or technique was conducted appropriately. At the end of the sprint, there were some activities flagged up in the sprint review and retrospective event:

- Obtain the actual and estimated effort of the sprint.
- Compare the estimated effort with the actual effort to measure the accuracy level of the estimation of the sprint.
- Compare the accuracy level of this sprint with previous projects conducted in the organisation to measure the improvement level, and find out the impact of the proposed technique/process and the estimation factors/predictors.

At the Sprint Review and Retrospective event, there were two possible scenarios put forward:

- If there is an improvement in the accuracy of the effort estimation, then another focus group meeting would be arranged to discuss any suggested improvements in the model that could provide a higher level of accuracy of the estimation value. Also, in case the accuracy level of the effort estimation in the current sprint is better than previous projects or previous sprints, then it would be necessary to have one more sprint and apply the estimation model to confirm the accuracy of the results and make sure the proposed method works properly.
- If there is no improvement in the accuracy level of the effort estimation, then it will be necessary to have another focus group meeting to diagnose what the problem was from the previous model and obtain suggestions that could improve the estimation level in the next sprint.

4. CASE STUDY RESULTS AND DISCUSSION

The case study has been applied to an existing project in a company that is located in Alkhobar city, Saudi Arabia, and has around 150 employees. The company established in 2009 and specializes in designing and developing a variety of software products. The project is basically about evaluating services provided by the government. The company completed four sprints during this project, and the duration of the sprints was two weeks. The project included five development team members, one product owner and one project manager for the overall project. Table 1 below provides more details of the practitioners' information.

Table 1. Case study participants in the project

Development member name	Years of experience	Member role in the team
T-A	4 years	Mobile app developer
T-B	3 years	Mobile app developer
T-C	8 years	Front-end developer
T-D	6 years	Back-end developer
T-E	4 years	QA
T-F	3 years	Product owner
T-G	9 years	Project manager

4.1 Understand the Current Situation

4.1.1 Meeting with the Project Manager to Understand the Team and Project Performance

To understand the velocity and the progress of the development process, it was important to know the performance of the previous sprints. The project manager "T-G" was happy to share the progress of the development team during the last two sprints, sprint 4 and 5, as shown in the diagrams below in Figure 1 and Figure 2. As can be seen in the diagrams, the development team estimated the user stories and its task at 81-89 story points, and stated that they could deliver these tasks within two weeks. In fact, the development team delivered at the end of the sprint time-boxed in sprint 4 only 10 story points, whereas nothing was delivered in sprint 5. The team worked overtime during the weekend to deliver the rest of the user stories in sprint 4, and in sprint 5 the team took three more days to complete and deliver all the user stories. The estimation technique and reasons for the under estimation were discussed in the focus group interview, as described below.

4.1.2 First Focus Group Discussion with the Development Team to Understand the Current Estimation Process and Its Challenges

A group discussion took place with five members of the development team regarding the estimation techniques and their

accuracy level. The group discussion session was held prior to the sprint planning meeting of Sprint-5. The goal of the group discussion was to understand the estimation techniques that had been used in the previous sprints, and the main reasons that caused the accuracy level of the estimation to be low. There were two group discussions with the development team; the first group discussion was concerned with two main points: 1-understanding the current estimation process of the development team, 2-discussing the main causes of the underestimation. The second group discussion was held later on after the observation was completed by the researcher.

4.1.3 Current Estimation Technique and Process

A question was posed to the development team concerning their estimation process for the last four sprints. The estimation technique that was used during the previous sprints was expert judgment. The expert judgment technique in the company works as follows: At the beginning of the sprint planning, the product owner explains the user story to all development team members. The user story could include front-end tasks for the web developer, mobile app tasks, backend tasks or QA tasks. Then, the team explained what they would do in the user story. It could be that several team members share different responsibilities for one user story. If there are two web developers in the team, the leader of the web-developing team assigns the effort for his part to the user story. Also, the team divided the user story into certain tasks to allow each member of the team to take a task and perform it alone. After assigning the tasks for the user story, the development team have a small discussion to decide whether take on more of the user story or not. The product owner and client usually push the development team to take on more of the user story to achieve the project delivery plan. The development team sometimes take the risk by accepting the pressure from the product owner and the client to take on more of the user story.

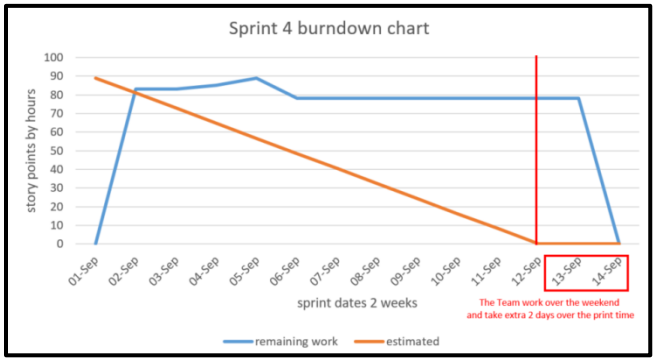


Figure 1. Burndown chart for sprint 4.

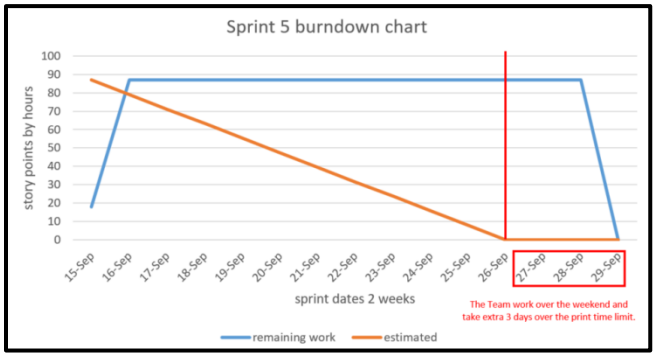


Figure 2. Burndown chart for sprint 5.

4.1.4 Main Causes of the Low Accuracy Estimation in the Previous Sprints

The second part of the group discussion was about the reasons and main causes of the low accuracy of the effort estimation for the last four sprints. There were several reasons that affected the estimation accuracy of the development team, and one of the reasons is that the definition of the user story was not clear to the development team. The product owner did not have a full understanding of the requirement specifications of the user story. The client and product owner discussed the user story during the sprint planning ceremony and gave some suggestions about their needs from the user story. After their discussion, they explained the user story to the development team. The discussion and changes in requirements during the sprint planning caused confusion for the team, and this created some ambiguity around the requirements. The researcher also noted this concern, as discussed in more detail in the researcher observation section. Another concern is that when the team gave their estimation for the user story in the sprint planning, the team asked for more clarification of some points in the user story during the sprint. As a result, the clarification could raise other concerns which need additional time from the developer - more than what they had expected. To avoid this happening again, the development team overestimate their effort estimation for the user stories that are not clear enough for them.

Moreover, the development team suffer from external interference that required the team to take on more tasks. The client agreed with the company to deliver all of the project requirements in 10 months based on their agreement in the project contract. In fact, the company has an issue with their initial estimations for clients for overall project estimations. The project manager gives her estimation to deliver all of the project based on her experience of previous projects, which places the developer under pressure and requires them to work over their capacity.

4.2 Researcher Observation of the Current Estimation Process and Team Performance

The researcher attended the sprint planning meeting for Sprint-5 to observe the development team's behaviour when they had a discussion with the product owner and the client for the user stories. During the sprint planning, several issues were observed by the researcher, as discussed in the following sections, and these issues were raised by the researcher and discussed with the project manager to take action to resolve them.

4.2.1 Lack of Valid Justification Given to the Product Owner and Clients for the Effort Estimation

The development team failed to provide good reasons and justifications to the product owner and customer about their estimation. The development team faced some challenges in persuading and convincing the customer and product owner about their estimation for the selected user story. For example, there was the case of a push notification task, which the mobile developer gave an estimation value of "two days" for, without a clear plan of what they would do in two days. The problem is that the developer seemed unable to explain some of their reasons why this task would take that amount of time. The researcher asked the developer at the end of the sprint planning session about why it was difficult to explain why this task would take that length of time, and the answer was that the developer thought the product owner and client were questioning and arguing about the effort involved. The client was not happy with the developer's justification and stated that the developers are not capable of

completing the task and do not know what they are doing, based on a discussion with the project owner. The development team could not persuade the product owner and customer about their suggested effort by providing good evidence and reasons why this effort takes this amount of time.

4.2.2 Putting the Development Team under Pressure

From the previous point, the customer and product owner of the project put pressure on the development team to force them to take as much as they could of the user stories from the product backlog in the sprint. The project delivery is to deploy, and the customer needed to finish from this project as soon as possible. As shown from the development team's performance in Figure 1, there were 34 story points that were not completed in Sprint 4. The team expected that they could complete these user stories within the sprint period, but in fact they faced some challenges that they did not expect.

4.2.3 Mono Decision Making in Effort Estimation

Each member of the development team provided their effort estimation alone without negotiating with his/her colleagues. The reason they do that is because each member of the team has their own specialty, and they prefer the person who carries out the task to be responsible for assigning the effort value for this task. If the user story consists of backend and front end tasks, usually one of them assigns the effort value for the whole user story alone. In fact, if the user story contains backend tasks, the backend developer assigns the effort for all of the user story because they have about six years' experience and she leads the user story. However, this creates uncertainty for other tasks in the user story and can result in an inaccurate estimation value for frontend tasks, for example.

4.2.4 No Time for taking the decision for Effort Estimation

There is not enough time for the development team to think about what they will do in the task in order to provide a more detailed plan for their task. After the product owner explains the user story, the developer whose role is related to this task gives his/her estimation immediately. The researcher counted the period for three members from the time the product owner finished his explanation of the user story to the time the developer give his estimation value. The first member took five second to give an estimation; the second member took around seven seconds, and the third member took four seconds only. This period is very short for the developer to think about the expected effort required to complete this task.

4.2.5 Some User Stories Related to Unknown or Legacy Systems for the Development Team

One main challenge of the development team is when they are asked to carry out some changes or investigations on a system that they do not know anything about. They cannot make an estimation about something if they do not know what it is. There was a case during the sprint planning in Sprint-5 that the product owner explained a new user story to the development team to carry out some changes and enhancements to an integrated system. The team did not know what was behind the integrated system and they needed time to understand that system before giving their estimation. The client was not happy with the developer when they were reluctant to give an estimation for that user story. There is a type of user story called Spikes [12] for exploration or investigation in order to gain more knowledge about the existing system. The Spike was discussed with the development team to help them estimate and investigate the user story.

4.2.6 The User Stories are not Broken Down into Small Tasks to be Manageable

It is difficult for the development team to estimate all of the user story. Usually, story points should be broken down into small tasks to make it easier to assign an estimation value. Sometimes the development team gives their estimation by day (2-3 days for example), which make the customer and product owner not satisfied with the estimation. Also, this big value of estimation cannot be traceable and manageable by the project manager and developer. Providing an estimation as days instead of hours give the impression to the customer and product owner that the development team are less capable and have a "lack of technical knowledge" concerning this task, or they do not know what this task involves. Therefore, breaking down the user story into small tasks would be helpful for the developer to manage their time and understand the detailed functionality of the user story.

4.2.7 Other Minor Observations

There are other issues that the researcher observed during the sprint planning session. One of them is lack of clarity of the user story during the sprint planning session. This is one of the main issues on the observation from the researcher notice during the sprint planning meeting that the product owner and clients discussed the functionality of the user story during the sprint planning event. For example, concerning the sprint planning event for Sprint-5, the clients discussed the functionality of the "rating feature" of the user story. They took about 20 minutes to discuss between each other what should be included in this user story.

Another concern is the clarity of the "definition of done". There was a misunderstanding between the development team and client concerning the meaning of done for the user story. The developer assumed the user story should be done after they finish doing the "development, testing and QA"; however, the customer claimed that the task should be done after the UAT (user acceptance test) which is supposed to be done on the customer's side.

The Agile maturity level [13] in an organisation is considered as one factor that could effect on the accuracy level of the estimation as mentioned in [9]; however, other effective factors have been observed and discussed in this study.

4.3 Second Focus Group Discussion with the Development Team to Improve the Estimation Process

During Sprint-5, a second group discussion session was held with the development team members and the project manager to improve the estimation accuracy and process of the effort estimation. The second group discussion focused the following topics: 1-explain to the team the main factors that effect on the accuracy of the estimation, and 2-provide suggested solutions to resolve the low accuracy of the effort estimation.

4.3.1 Explain the Estimation Factors to the Development Team

In the group discussion session, the researcher presented all of the 64 effort estimation factors, "comprehensive factors" [9], to the development team and discussed with them the level of impact and influence of these factors on the estimation accuracy. The researcher explained each factor to the development team and asked them how they could use these factors to measure their

effort estimation, and to mention it to the researcher if there are any additional factors they want to add. The team discussed the points together and came up with these statements:

- We can use these factors to let us think more about a new user story in more technical detail. Before, we usually compared the new user story with the one that we did before, but with these factors we can think more in more detail about what we can expect from the user story.
- For example, the transaction journey factor would help us to think about the structure of the data that we need to send to the backend and the result of the data structure from the backend to the frontend. Also, these factors help the backend developer, for example, to discuss with the mobile app developer about the user story, and explain to each other who will do this and split the user story into small tasks for each other.
- The factors overall are comprehensive and we can put them in our mind and concerns before we give an estimation value.
- The effort factors can help the development team to break down the user story into small tasks.
- In order to recall the estimation factors during the estimation, the development team prefer to present the estimation factors through a projector inside a meeting room, while the estimators take their decision regarding the estimation value.
- The 64 factors are comprehensive and we don't have any additional factors.

After explaining the effort estimation factors to the team, the mobile developers, T-A and T-B, added some comments regarding the segmentation of a user story into subtasks. T-A and T-B said: "the estimation factors help us to break down the user story into small tasks". However, both of the mobile developers concluded that one task could be developed into two different platforms "IOS and Android" with different effort estimation values. T-B claimed that the UI design of a task in Android devices sometimes takes more time than in IOS. The reason behind this is the task needs to be tested on multiple Android devices compared with IOS, and the Android emulator is not accurate at reflecting the real UI of Android devices. Also, T-A explained: "the drag and drop feature of designing UI in XCode IDE is more supportive and accurate than Android studio". Regardless of the pros and cons for each of the mobile framework, IDE, tools and platform, this argument is debatable, and the development of professionalism depends on the developer's capability and experience in development skills; these aspect underlie the six technical factors that have been stated in the literature [9].

4.3.2 Provide a Proposed Estimation Technique

In the group discussion session, the development team were asked to discuss and find an appropriate solution to provide a proposed estimation model that could help them to understand the user story and give a highly accurate estimation value. The researcher presented a suggested model to them and asked if this could help with their estimation process.

After a long discussion, the development team came up with a proposed estimation model, which we named the "Pair-estimation technique". The fundamental aspect of the pair-estimation technique is to encourage two of the development team members to talk to each other. An issue explored in the workshop session is presented below, as well as the solutions to this issue. All the solutions are the outcomes from the workshop discussion.

The issue: In the workshop session, the development team claimed that some of the development team members should not give an estimation for something that he or she will not do. For example, the frontend developer "T-C" should not give an estimation for the backend task because he does not know what is behind this task; therefore, the backend developer "T-D" should take the responsibility for assigning the effort for this task.

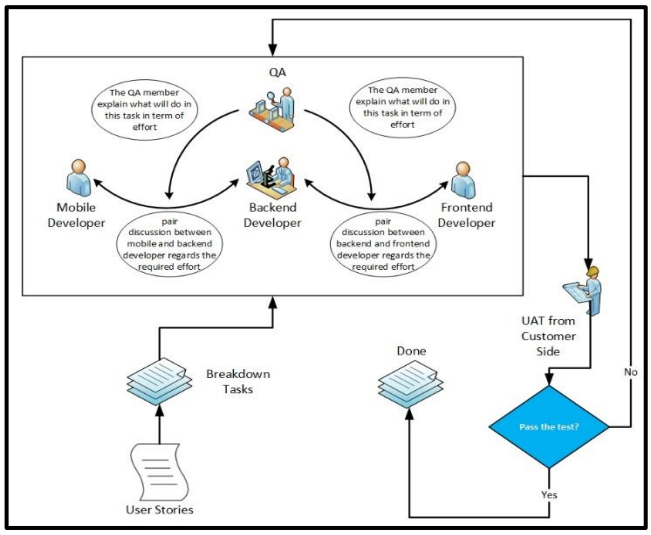


Figure 3. Pair-estimation technique.

The solution: from the group discussion session, the development team agreed that a team member should communicate with his/her pair "at least one person" even if there is no direct impact on his/her task. Figure 3 shows the design of an approach that requires each member to make contact with his/her pair based on their shared interest. For example, the backend developer "T-D" could communicate with the frontend developer "T-C" to ask him about what is the expected response of the data structure from the backend to frontend, and if it will be in a stack or array. Or, how can you store the data and from which database will retrieve you the data, as well as how big will the data be? This form of communication will help in creating a deeper discussion between the two pairs. Also, this approach will help each member of the development team to hear feedback from his/her pair about his/her estimation.

4.3.3 Discussion with the Development Team Regarding the Research Observations

The researcher noted several concerns regarding the effort estimation process and techniques, as discussed in the previous section, and now in the group discussion session the results of the observations were shared with the development team as the basis of a discussion regards them. From our discussion, we concluded, the researcher, development team members and project manager, with certain of actions that need to take during the estimation time, and from the discussion we came up with the following statements:

Break down the task/user-story into subtask that should not exceed 8 hours. If the task reach 8 hours as an estimation, the developer need to break it down into sub-task as shown in Figure 4. The sub-task could include technical subtask that help the developer to measure his effort. The effort estimation should be based on hours not a day.

After we break the user story into small tasks, every member of the team take his task from the user story, and discuss with his/her

peer regards the shared interest, integrated data, APIs,etc as shown in Figure 4.

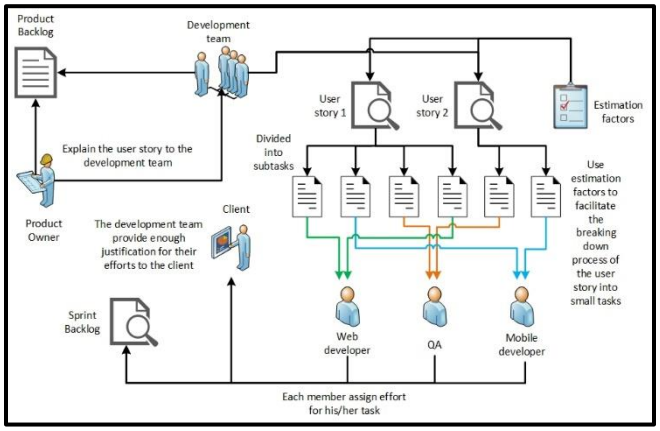


Figure 4. Sub-tasking the user story into independent tasks.

Two hours prior to the sprint planning meeting, the development team met to understand the first 5-6 prioritised user stories and discuss the effort estimation value for each. This allowed the development team to understand the user story and gave them more time to prepare how they would implement the user stories technically. Also, this resolved the issue concerning the T-C member sharing their effort estimation suggestion regarding the user stories or tasks that belong to them.

The development team should provide reasonable factors to the customer and product owner and form a good justification of why they allocate this effort to this user story or task.

It was agreed that the project manager should prevent interference from customers and product owners regarding assigning the effort estimation value to the user stories; however, the development team should provide good justification and reasons to make them satisfied with their estimation values.

It was agreed that the "definition of done" would affect the accuracy of the effort estimation if not stated clearly to all the members of the team; therefore, it was agreed that for each estimation, the development team should be concerned about the workflow of the user stories process and when the user story or task is considered to be done.

The client or product owner should be aware of the consequences of adding or change a user story during the sprint.

The development team agreed that the Planning Poker method would not work properly for them, based on their experience with this technique from earlier projects, because:

- This method will take a long time to hear from each member.
- This method will allow non-specialist members to give their estimation for a task that is not related to them; for example, the backend developer giving their estimation for a mobile app task.

The development team agreed that estimating the effort of "spike" is hard due to uncertainty beyond the investigation and the vagueness of the legacy system; however, it was agreed that assigning a random or arbitrary estimation value would negatively affect the velocity of the development team and turndown chart. Therefore, for the sprint that has a spike, it was agreed that the product owner must assign the spike to a member of the team to conduct the initial investigation of the spike, and reduce the load capacity for that member. The member would continue doing the investigation until he/she feels the investigation will have an effect on his/her delivery of the sprint. At the end of the sprint, either the initial investigation is enough or the member should provide a rough estimation for a more detailed spike in the next sprint.

Moreover, the development team should talk to each other. An issue addressed in the workshop session is presented below, along with a solution to this issue:

- **The issue:** In the workshop session, the development team claimed that some of the development team members should not give an estimation for something that he or she will not do. For example, the frontend developer "T-C" could not give an estimation for the backend task because he does not know what is behind this task; therefore, the backend developer T-D should take the responsibility for assigning the effort to this task.
- **The solution:** the team member should talk with his/her pair "at least one person" even if there is no direct impact for his/her task. An approach was designed that involves each member communicating with his/her peer based on his/her interests. For example, the backend developer, T-D, could communicate with the frontend developer, T-C, to ask about suggestions for the response structure from the backend-to-frontend, and if it should involve the stack or array method. This will help each member of the development team to hear feedback from his/her peers about his/her estimation.

4.4 Result after Applying the Proposed Estimation Technique

After constructing the proposed estimation technique based on the focus group discussion with the development team members and the project manager, the team applied the new estimation technique during the sprint planning meeting in Sprint-6, Sprint-7 and Sprint-8. The development team used the estimation factors to help them obtain a precise estimation. The development team followed the instructions on what they had agreed from the first and second group discussions in order to enhance the estimation accuracy.

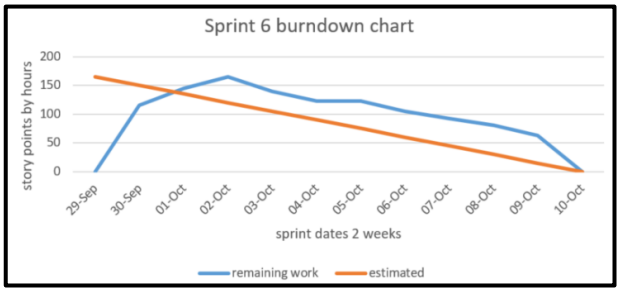


Figure 5. Burndown chart for sprint 6.

In the sprint planning of Sprint-6, the development team took 16 user stories and divided these user stories into 25 subtasks. The team estimated the user stories and subtasks to be around 165 story points. The team delivered all the subtasks by the end of Sprint-6. Compared with the previous sprints (4 and 5), the team delivered the subtasks and user story timely and within the sprint time-box, as shown in Figure 5; whereas for Sprint 4 and 5, the team delivered all the user stories at one time by the end of the sprint time frame. In Sprint-6, the client and product owner were satisfied with the number of task they delivered. The team took 165 user stories in a sprint backlog fin Sprint-6, whereas around

80 user stories were in Sprint-4 and Sprint-5. The proposed estimation process and technique made the task more organised and doable for the team members. Each member knew what he/she should do during the sprint. Moreover, the quality of the development was enhanced as well, as shown in Table 2; 11 and 9 bugs were found in Sprint 6 and 7 respectively from the development, whereas 20 bugs were found in Sprint-4 and 17 bugs in Sprint-5.

Table 2. Overall sprints performance before and after the proposed technique

		Before		After		
Sprint Number		Sprint 4	Sprint 5	Sprint 6	Sprint 7	Sprint 8
Number of user stories		8	7	12	4	6
Number of subtasks		0	1	25	35	32
Number of bugs		20	17	11	9	13
Sprint Estimation (hours)		89	87	165	161	N/A
Deliveries (hours /day)	Mean	9.9	6.7	20.6	16.10	N/A
	Median	0	0	17.5	11	N/A
	Std. Dev	25.8	24.1	18.6	15.8	N/A

4.4.1 Focus Group Discussion after Applying the Proposed Technique

In the review of Sprint-6, the clients were happy and satisfied with the results of the sprint. The team was aware enough to provide a clear plan and estimation for this sprint. The estimation accuracy not only helped the team to provide an accurate estimation, but the estimation also helped the team to organise their work, allowing them to have clear plan, and then to deliver the tasks on time and inform the stakeholder about their actual effort to make them satisfied. In the sprint retrospectively, the team shared their success story with each other about the reasons that made Sprint-6 different from the previous ones. T-C member stated: "in this sprint, we organised our work and simplified the complexity of the user stories by breaking them down into small tasks to allow us to understand the details behind the user story". T-E explained: "The estimation factors are very helpful for us and facilitate the breaking down and categorisation procedure of the user story into small tasks".

In the sprint retrospective session, the researcher asked the development team to provide their feedback on two points: 1-the effectiveness level of the estimation factors that helped them to provide an accurate estimation, and 2- the option of using a checklist form of the factors on a paper sheet instead of presenting them on a projector. The team summarised their answers as following:

First: The comprehensive factors support the team dividing the user story into subtasks. T-B member stated: "the overall factors open my mind to break down the complexity of the user story into small pieces of tasks". T-A explianed: "UI animation, prototype/fidelity design and availability of the API tools are the main factors that help me to think more and deeply about the user story before I give my estimation". T-D claimed: "before, I would compare the new task/user story with similar ones that I have done previously, but now the factors support me in how to facilitate the complex user story and allow me to understand how to collaborate with my colleagues. For example, I was thinking about the transaction journey and what is the structure of the request and response". Furthermore, the researcher recognised from the team work during Sprint-6, that they recalled the explanation of the estimation factors from the projector and broke the user story down into smaller tasks. The factors encouraged the team to evaluate the complexity of the user story and helped them to interpret the complexity involved in the effort value.

Second: The project manager, T-G, extracted the burn-down chart for Sprint-6, as shown in Figure 5, and noticed that the development team continued breaking down the user story during the sprint's development. The concern is that the team figured out additional details concerning the requirement specifications of the user story – more so than they expected. This scenario required additional effort, again, more than they expected at the beginning of the sprint. The project manager claimed this situation happened because it is the first sprint for the team after using the new estimation method.

Third: The pair estimation model encouraged the team to talk to each other. The team experienced some unorganised discussion and that led to a misleading estimation value from an unspecialised person. The proposed method "pair estimation" allows pairs of professionals to exchanges their feelings, experience and understanding about the user story specification to obtain a highly accurate prediction.

The number of bugs reduced in Sprint-6 compared with the previous sprints, as shown in Table 2. As explained earlier, the pair estimation method allows pairs of professionals to spend more time delving into the specification of the user story and interpreting their understanding into a valuable and manageable context. Also, the proposed model allowed the team to spend their time developing without any pressure from taking on more tasks within a short period of time. The breaking down of the user story allowed the QA to design a test case to verify the delivery and achieve its goal.

The researcher observed that there was no opposition or negotiation from the clients about the team estimation during the sprint planning. In fact, the client and product owner were happy and satisfied with the team capacity. The team claimed that they did not add too much work compared with Sprint-5; however, they explained what they would do in more detail and organised their work to make it notable, recognisable and remarkable. In fact, the new method made their work measureable and allowed them to show off their work and make it noticeable. This method also enabled the team to manage their work and make it measurable and understand their capacity.

Moreover, the researcher observed and recorded some examples of how the development team discussed issues with the client representative and product owner to gather more information about the user story and facilitate the user story being broken down into small tasks. One of these examples is: the member T-A and T-B explained the suggested scenario for sending a notification to the apps. T-B stated: "the admin of the app will have the drop down list to select the receiver type for this notification. From this selection, there is a sub role type for this notification: general notification or send notification to a specific people based on their: gender/nationality/location of the user/user age range from X to Y / etc, and also we send scheduled notification to the user about the holidays and events and so on". T-B continued to explain the structure of the push notification form on the apps and the complexity of the form. Also, the client discussed with T-A and T-B and asked: "how will the form style of the notification feature look like?", and the continued to ask for

more details of the UI design of the app form. This kind of communication clarified the user story and made it clear for both sides: the development team members and clients. T-B stated: "during the sprint, we will show you the UI design for this form and ask you for your approval before continuing doing the development". The client representative and team member discussed the workflow of the notification message, and T-F and the client agreed: "A confirmation message must appear to the Admin user before sending the notification".

In Sprint-7, the team followed the same proposed method and focused on avoiding the issues that were mentioned in the sprint review and retrospectively from Sprint-6. The development team estimated 161 story points in Sprint-7 and they delivered all the tasks on time, as shown in Figure 6. Also, the team delivered all the user stories on time with less bugs (9 bugs), and 35 subtasks, as shown in Table 2. For Sprint-8, only partial information has been collected from that sprint.

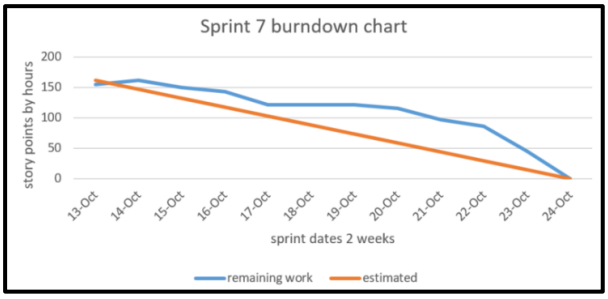


Figure 6. Burndown chart for Sprint 7.

4.4.2 Correlation Test of Estimation Validity

In order to validate the findings and results from the focus group discussions, a statistical Pearson Correlation test has been used to measure the association strength between the estimated effort with the actual effort values during the sprint. As shown below in Table 3, the correlation test was applied in Sprint 4 and 5 to measure the strength of the relationship between the estimated effort values of the user story with the actual effort values. The results from the test show that there is no association between the values, and this indicates that the team did not perform as expected and planned. On the other hand, a correlation test was used for Sprint 6 and 7 after the development team applied the pair-estimation technique in order to enhance the accuracy of the delivery of user stories during the sprint, and the results show that there is a significant relationship. The results indicate that the deliveries of user stories were delivered as planned and expected when the team used the proposed pair-estimation technique.

Table 3. Correlation test for sprint 4, 5, 6 and7

Pearson Correlation	Estimated Effort Sprint 4	Pearson Correlation	Estimated Effort Sprint 5
Actual Effort Sprint 4	0.151	Actual Effort Sprint 5	-0.048
Sig. (2-talied)	0.592	Sig. (2-talied)	0.866
Pearson Correlation	**Estimated Effort Sprint 6**	**Pearson Correlation**	**Estimated Effort Sprint 7**
Actual Effort Sprint 6	0.569*	Actual Effort Sprint 7	0.932**
Sig. (2-talied)	0.027	Sig. (2-talied)	0.0001

* Correlation is significant at the 0.05 level (2-talied)
** Correlation is significant at the 0.01 level (2-talied)

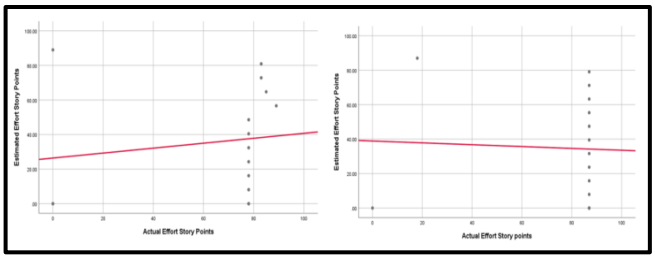


Figure 7. Correlation test for sprint 4 and sprint 5.

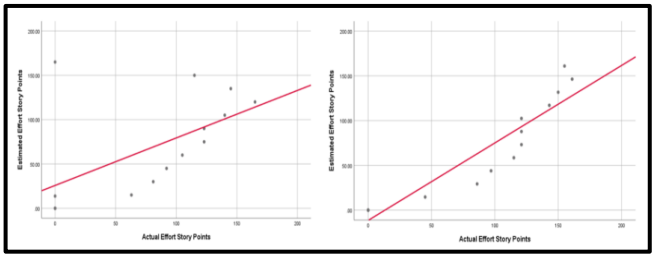


Figure 8. Correlation test for sprint 6 and sprint 7.

5. CONCLUSION AND FUTURE WORK

This study has proposed a pair-estimation technique that provides a more accurate plan than other techniques. The case study has provided an overview of the existing estimation process and its consequences for sprint delivery plans and their quality. The proposed technique is supported by predictors that enable the developer to make their estimation with more confidence. The Planning Poker technique did not work properly with the company due the involvement of non-specialist members in the estimation and the long time of the estimation process.

The proposed technique will be applied in more IT companies, as part of future work, to provide validation and confirmation of the results of the technique. Moreover, the most used estimation techniques in Agile, Planning Poker, need to be examined more in the context of mobile app development in order to validate its suitability in the Agile process for mobile app development. The Agile maturity level [13] has not applied in this case study to measure its relevant and effectiveness to the effort estimation; however, it could be in a future work.

6. REFERENCES

[1] M. Cohn, *Agile Estimating and Planning*, 1st ed. Prentice Hall, 2005.

[2] V. Mahnič and T. Hovelja, "On using planning poker for estimating user stories," *J. Syst. Softw.*, vol. 85, no. 9, pp. 2086–2095, 2012.

[3] M. Usman, J. Börstler, and K. Petersen, "An Effort Estimation Taxonomy for Agile Software Development," *Int. J. Softw. Eng. Knowl. Eng.*, vol. 27, no. 04, pp. 641–674, May 2017.

[4] A. Nitze, A. Schmietendorf, and R. Dumke, "An analogy-based effort estimation approach for mobile application development projects," *Proc. - 2014 Jt. Conf. Int. Work. Softw. Meas. IWSM 2014 Int. Conf. Softw. Process Prod. Meas. Mensura 2014*, pp. 99–103, 2014.

[5] A. Kaur and K. Kaur, "Systematic literature review of mobile application development and testing effort estimation," *J. King Saud Univ. - Comput. Inf. Sci.*, no. November, 2018.

[6] A. R. Altaleb and A. Gravell, “Effort Estimation across Mobile App Platforms using Agile Processes: A Systematic Literature Review,” *J. Softw.*, vol. 13, no. 4, pp. 242–259, Apr. 2018.

[7] G. Catolino, P. Salza, C. Gravino, and F. Ferrucci, “A Set of Metrics for the Effort Estimation of Mobile Apps,” *Proc. - 2017 IEEE/ACM 4th Int. Conf. Mob. Softw. Eng. Syst. MOBILESoft 2017*, pp. 194–198, 2017.

[8] A. Altaleb and A. Gravell, “An Empirical Investigation of Effort Estimation in Mobile Apps Using Agile Development Process,” *J. Softw.*, vol. 14, no. 8, pp. 356–369, 2019.

[9] A. Altaleb, M. Altherwi, and A. Gravell, “An Industrial Investigation into Effort Estimation Predictors for Mobile App Development in Agile Processes,” in *9th IEEE International Conference on Industrial Technology and Management (ICITM 2020)*, 2020.

[10] P. Runeson, M. Höst, A. Rainer, and B. Regnell, *Case Study Research in Software Engineering: Guidelines and Examples*. 2012.

[11] M. Usman, K. Petersen, J. Börstler, and P. Santos Neto, “Developing and using checklists to improve software effort estimation: A multi-case study,” *J. Syst. Softw.*, vol. 146, pp. 286–309, 2018.

[12] D. Leffingwell, *Agile Software Requirements: Lean Requirements Practices for Teams, Programs, and the Enterprise*. 2011.

[13] C. Patel and M. Ramachandran, “Agile Maturity Model (AMM): A software process improvement framework for agile software development practices,” *Int. J. Softw. Eng. IJSE*, 2009.

False Positive Detection in Sender Domain Authentication by DMARC Report Analysis

Kanako Konno
Tokyo University of Agriculture and Technology
2-24-16 Naka-cho, Koganei, Tokyo, 184-8588, Japan
+81 42-388-7683
k_konno@net.cs.tuat.ac.jp

Naoya Kitagawa
Tokyo University of Agriculture and Technology
2-24-16 Naka-cho, Koganei, Tokyo, 184-8588, Japan
+81 42-388-7683
nakit@cc.tuat.ac.jp

Nariyoshi Yamai
Tokyo University of Agriculture and Technology
2-24-16 Naka-cho, Koganei, Tokyo, 184-8588, Japan
+81 42-388-7695
nyamai@cc.tuat.ac.jp

ABSTRACT

The number of spoofed emails is increasing rapidly and become a serious problem, especially in business and e-commerce. Sender domain authentication is an effective countermeasure for spoofed e-mail. Although SPF, DKIM, and DMARC are famous sender domain authentication methods, these methods erroneously determine legitimate e-mails as malicious e-mails, such as forwarded messages. On the other hand, DMARC has a reporting function, which e-mail senders can receive DMARC reports that include SPF and DKIM authentication results, and the sender's domains, and so on. Generally, spam e-mails countermeasures are combined with three approaches: TCP/SMTP session monitoring, sender domain authentication, and contents filtering. Since sender domain authentication is usually processed before contents filtering, the occurrence of many false positives in sender domain authentication is a serious problem. In this paper, we propose a method to detect legitimate IP addresses by adapting X-means clustering to DMARC reports data in order to detect false positive deliveries in sender domain authentications. We apply actual DMARC reports data received from 28th September to 5th October 2019 to our approach. As a result, our method classified 254 to 480 IP addresses per day as legitimate addresses. As an evaluation, we confirmed that 2.8% to 11.1% of e-mails from legitimate IP addresses detected by our method were failed the combination of SPF or DKIM verification, and 36.9% to 62.7% of them were failed to DMARC authentication. From these results, we confirmed the proposed method can detect false positive deliveries caused by conventional sender domain authentication with high accuracy.

CCS Concepts

• Information systems → World Wide Web → Web applications → Internet communications tools → Email • Social and professional topics → Computing/technology policy → Computer crime → Social engineering attacks → Spoofing attacks • Security and privacy → Systems security → Distributed systems security.

Keywords

E-mail; Spoofed e-mail; spam; Sender domain authentication; SPF; DKIM; DMARC; Data clustering;

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388217

1. INTRODUCTION

E-mail is a service widely used around the world to communicate with lots of people or send various information. However, the delivery of spoofed e-mail is increasing rapidly, which is a serious problem, especially in business and e-commerce. Actually, FBI reports that the total financial damage is 26.2 billion US dollars from June 2016 to July 2019 [1].

Sender domain authentication is an effective countermeasure technology against spoofed e-mail. Sender Policy Framework (SPF) [2] and DomainKeys Identified Mail (DKIM) [3] are the most widely used sender domain authentication technologies. SPF verifies that an IP address of the sender's SMTP server is included in the list of authorized IP addresses called SPF record. However, SPF has a problem, which SPF cannot authenticate a forwarded message correctly, because the sender's IP address is changed to the forwarder's IP address that is not included in SPF record.

As another method, DKIM verifies the validity of the digital signature generated from the e-mail body and header in order to confirm whether the e-mail has not been rewritten by spammers. With this mechanism, DKIM can verify the forwarded message correctly. However, DKIM mechanism allows third party's signature, therefore the receiver cannot verify the spoofed e-mail correctly which a spammer utilizes their own malicious DKIM signature domain.

Domain-based Message Authentication, Reporting and Conformance (DMARC) [4] is an effective authentication method, which has reporting and policy controlling framework. DMARC utilizes SPF and DKIM authentication mechanisms. DMARC authentication will be failed when the e-mail fails both SPF and DKIM authentication, and the e-mail receiver deal with the authentication failure e-mail according to the DMARC policy published by the e-mail domain's administrator. Moreover, the e-mail receiver sends the e-mail sender a DMARC report which includes the authentication results, e-mail domains, and so on. In addition, DMARC verifies an alignment of e-mail domains, in other words, DMARC does not allow third party's signature, unlike DKIM. On the other hand, DMARC cannot solve the issue that SPF cannot verify the forwarded messages or mailing list's messages properly. Therefore, a legitimate e-mail will be failed DMARC authentication when the e-mail failed the SPF authentication and its domain is not adapted DKIM or using third party's DKIM signature.

Anti-spam operations are generally combined with several methods, such as TCP/SMTP session monitoring, sender domain authentication, and contents filtering. Sender domain authentication is usually processed before contents filtering, which requires high computational costs. For this reason, although false negatives in sender domain authentication are not a serious problem, it is strongly required to reduce false positives in sender domain authentication.

In this paper, we propose a method to detect false positives in sender authentication by analyzing a large number of DMARC reports. As a result of applying our method to DMARC reports received from 28th September to 5th October 2019, 254 to 480 IP addresses per day were classified as legitimate senders. Additionally, we confirmed that 2.8% to 11.1% of e-mails from legitimate IP addresses detected by our method were failed the combination of SPF and DKIM verification, 36.9% to 62.7% of them were failed to DMARC authentication. From these results, our method can detect false positive deliveries with conventional sender domain authentications with high accuracy.

This paper organized as follows. In section 2, we explain some anti-spam methods and sender domain authentication methods as related works. In section 3, we describe the design of our mechanism. Then we show the dataset that we utilize the experiment in section 4. Section 4 shows the results of our method applying dataset and evaluations of the legitimate IP addresses detection focusing on the false positives in sender domain authentication. Finally, we present the concluding remarks in section 6.

2. RELATED WORK

Many anti-spam methods have been proposed for many years by many researchers. In general, e-mail server operations are generally combined with the following three methods for anti-spam: monitoring of behavior during TCP/SMTP session, sender domain authentication, and contents filtering.

Greylisting [5] checks the retry function for establishing an SMTP session, and Kitagawa et al.'s method [6] inspects the retrying function for establishing a TCP session between the sending host and the receiving host. Although these methods are highly effective against conventional spam transmission, it is expected that the reduction effect for the sophisticated spoofed e-mail that has become a social problem in recent years is not sufficient.

Contents filtering is an effective and the most commonly used technique for anti-spam. For example, Bayesian Filter [7] is a famous contents filtering method utilizing Bayes theorem. In addition, spam detection methods using Natural Language Processing [8], support vector machines [9], and machine learning [10] are widely utilized. In actual operation, because contents filtering is high calculation cost, it is used after reducing the number of e-mails to be inspected by other anti-spam methods in advance.

SpamAssassin [11] scores e-mails based on keyword, public database, and Bayesian Filter, etc. in order to detect spam e-mails. This method utilizes several anti-spam methods, such as Blacklist [12] and sender domain authentication methods when the e-mails are received before Bayesian Filter.

Blacklist detects spammers utilizing a list including attackers' IP addresses and domains. Sender domain authentication methods can verify whether the e-mails are spoofed or not based on the information of e-mail senders.

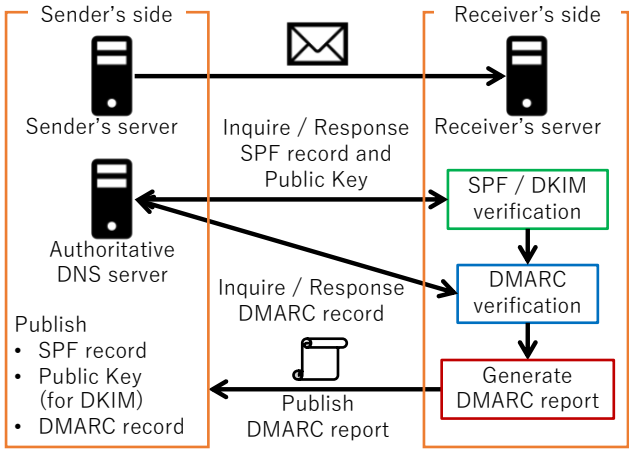


Figure 1. The flow of DMARC verification

SPF, DKIM, and DMARC are the most popular methods among sender domain authentication. We explain these three methods in the following subsections, 2.1 and 2.2.

2.1 SPF and DKIM

SPF checks whether the IP address of the sender's SMTP server is legitimate or not according to the SPF record which indicates a list of IP addresses that the sender may use for e-mail sending. The e-mail sender should publish the SPF record to their own authoritative DNS server. The receiver inquires the SPF record of the Envelope-From domain's authoritative DNS server and checks the IP address of the e-mail sender's SMTP server is included in the SPF record. When the IP address is included in the SPF record, the e-mail passes the SPF authentication. However, SPF has a problem that it cannot verify forwarded messages properly because the e-mail sender's IP address changes from the original SMTP server's IP address to the forwarding server's IP address that is not included in the SPF record.

DKIM checks whether an e-mail has been rewritten by an attacker using a digital signature (hereinafter, this is called "DKIM signature"). In order to install DKIM mechanism, the sender domain's administrator should prepare a pair of the private key and the public key in advance and publish the public key on their authoritative DNS server. When the sender sends an e-mail, the sender domain generates a DKIM signature from the e-mail body and header using the private key and attaches it to the e-mail header. When the receiver receives the e-mail, the receiver inquires the public key to the authoritative DNS server of the sender's domain that is obtained from the "d=" tag in the e-mail header. The receiver compares the hash value obtained from the DKIM signature using the public key with the hash value generated from received e-mail. When these values are the same, the e-mail is passed the DKIM verification. DKIM can verify forwarded messages correctly unlike SPF because DKIM does not depend on e-mail delivery route. However, DKIM allows third party domains to sign e-mails, it has an issue which the spoofed e-mails signed with spammers' own malicious domain will be passed the verification.

2.2 DMARC

DMARC is a reporting and policy controlling framework utilizing SPF and DKIM mechanisms to authenticate e-mails. Figure 1 shows the flow of DMARC authentication and reporting. In order to use DMARC, the sender domain administrator should publish

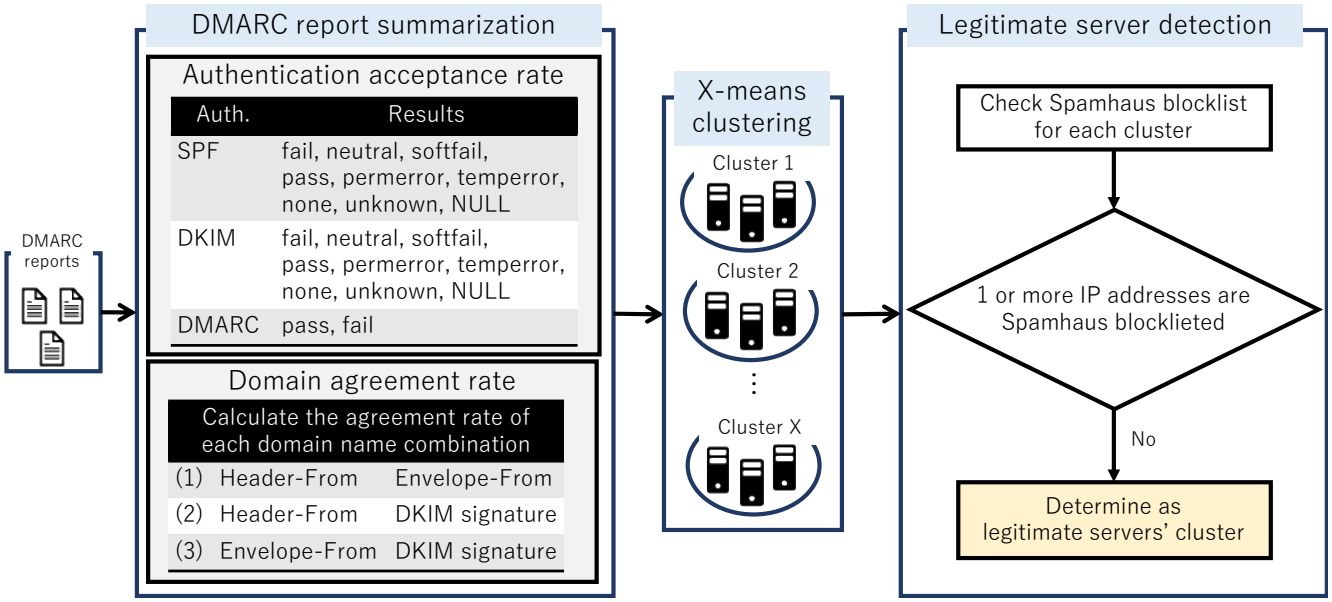


Figure 2. Design of our approach.

SPF record and public key on the authoritative DNS server beforehand to utilize SPF and DKIM authentication. Moreover, the sender domain also needs to publish the DMARC record on the authoritative DNS server. DMARC record indicates the e-mail handling policy how the receiver handles the DMARC failure e-mails, which published by the e-mail sender. This policy has three variations: "none (do not anything even if authentication failure)", "quarantine (quarantine the authentication failure e-mail)", and "reject (reject the authentication failure e-mail)". Additionally, the e-mail address which indicates DMARC reports receiver is also shown in the DMARC record.

DMARC report provides much information, such as e-mail Header-From domain, Envelope-From domain, DKIM signature domain, sender domain authentication results, and effectiveness of DMARC policy, and so on. Thus, the sender domain's administrator can obtain the performance of the authentication from DMARC reports, and they can take stronger measures in order to decrease spoofed e-mails abusing their domain.

With the DMARC alignment, DMARC verification will be failed when the sender's Header-From domain same as the Envelope-From domain or the DKIM signature domain. On the other hand, spammers can fraud the Header-From domain easily. The sender domain administrator can choose from two strictness of alignment, "strict" and "relaxed" in DMARC record. When the sender domain's administrator uses "strict" mode, Header-From address and domain for SPF or DKIM verification need to match completely. On the other hand, when the alignment mode is "relaxed", DMARC verification will success when subdomains of Header-From domain and domain for SPF or DKIM verification match.

3. DESIGN OF OUR METHOD

As described in section 2.2, DMARC cannot verify the legitimate e-mail properly in some cases. In order to overcome this weakness of DMARC, we analyze DMARC report data by adopting X-means clustering analysis.

Our method consists of three phases: DMARC reports summarization, DMARC reports clustering, and false positive detection, as shown in Figure 2. First, we summarize DMARC reports data in order to adapt clustering analysis focusing on the results of sender domain authentication and the e-mail domain names. As summarization of sender domain authentication results, we calculate the acceptance rate of SPF, DKIM, and DMARC for each IP address. These three authentication methods have several authentication results as shown in Figure 2. Our method calculates the percentage of e-mails for each authentication result per IP address. Next, as summarization of the e-mail domain name, we calculate the agreement rate of three combinations of domain names. DMARC mechanism compares the e-mail Header-From with Envelope-From domain ((1) in Figure 2) and the DKIM signature domain ((2) in Figure 2) for the alignment of DMARC. On the other hand, the Envelope-From domain is not compared with the DKIM signature domain ((3) in Figure 2) in the sender domain authentication verification process. However, the combinations (1) and (2) have relationships in SPF, DKIM, and DMARC. Therefore, since we consider that the combination (3) also has a relationship that is not for sender domain authentication, we also utilize domain combination (3) for improving the accuracy of our approach.

Then, our method adapts X-means clustering algorithm to summarized DMARC reports data. K-means is one of the most popular clustering algorithms. In order to utilize K-means, the number of clusters must be provided beforehand. On the other hand, X-means clustering algorithm proposed by D. Pelleg and A. W. Moore [13], determine the number of clusters by iterating K-means and splitting criteria based on Bayesian Information Criterion (BIC). In this clustering flow, our approach classifies the sender's IP address according to their transmission behavior trends, such as similarity of the authentication results consistency between the domain names related to e-mail sending and its authentication.

TABLE 1. Utilized dataset and the results of clustering

Date	*All_IP*	*All_email*	*All_rep*	*Tgt_IP*	*C*	*Leg_C*	*Leg_IP*
9/28	13,805	569,375	104,085	3,639	20	15	474
9/29	12,289	532,407	94,377	3,619	20	14	414
9/30	10,329	437,172	85,082	3,570	20	11	328
10/1	12,542	525,807	93,694	3,604	20	13	405
10/2	14,381	596,734	103,276	3,852	20	14	390
10/3	14,213	637,324	103,964	3,791	20	16	254
10/4	14,083	585,096	101,966	3,724	20	13	453
10/5	14,025	606,372	93,188	3,480	20	14	480

Finally, we check all IP addresses of each cluster whether these are listed in the Spamhaus blocklist [14] that is the most famous IP blacklist in the world. When no IP address in a cluster is included in the Spamhaus blocklist, we determine this cluster as the legitimate server's cluster. Our method does not determine the clusters which at least one IP address of the clusters is listed in the Spamhaus blocklist as a legitimate server's cluster. Although these clusters contain IP addresses which are not listed in the Spamhaus blocklist, these IP addresses may be spammers', because our method classifies these IP addresses into the same cluster with black IP addresses. Thus, in order to detect certainly legitimate IP addresses, our method does not detect a cluster that contains at least one blacklisted address as a legitimate server cluster.

4. DATASET

In this section, we explain the details of the DMARC report as dataset applying to our approach, which we received from 28th September to 5th October 2019. TABLE 1 shows the details of our dataset and the results of applying the dataset to our approach. The abbreviations that we use hereinafter are the following.

- *Date:* Date of DMARC report received
- *All_IP*: The total number of sender's server IP addresses
- *All_email*: The total number of e-mails constructing DMARC reports
- *All_rep*: The total number of DMARC reports
- *Tgt_IP*: The number of IP address for X-means (*They send 90% of all e-mails constructing DMARC reports.)
- C: The number of clusters
- *Leg_C*: The number of legitimate server's cluster
- *Leg_IP*: The number of legitimate IP addresses included legitimate server's cluster

As the *Tgt_IP* column in TABLE 1 shows, we apply the IP addresses which send 90% of all e-mails in DMARC reports. These IP addresses account for 24.8% to 34.6% of *All_IP* and send 90% and more of all e-mails in our DMARC reports. In contrast, the remaining from 65.4% to 75.2% IP addresses send only a few e-mail deliveries. We consider that about 90% IP addresses will be the noise of X-means clustering, thus, we utilize DMARC reports that contain the sender's IP addresses in *Tgt_IP*.

5. RESULTS and EVALUATIONS

In this section, we explain the results of applying the dataset to our method and describe the evaluations. TABLE 1 shows the clustering results and legitimate IP address detection results. As shown in the table, our method divided *Tgt_IP* to 20 clusters for each day, and classified 11 to 16 clusters as *Leg_C*. Additionally, the legitimate servers' clusters consist of 254 to 480 IP addresses (*Leg_IP*).

As described in section 3, we confirmed that all legitimate addresses detected by our method are not on the Spamhaus blocklist. This means that all the legitimate IP addresses our method detected are not spammers' servers.

Then, as an evaluation of the detection results focusing on false positive detections of sender domain authentication, we investigated the number of e-mails that failed in sender domain authentication sent from the legitimate IP addresses detected by our approach.

As mentioned in section 2.2, DMARC mechanism utilizes both SPF and DKIM mechanisms for the authentication. In addition, it is necessary to exclude false positives in forwarded messages or mailing list e-mails caused by using SPF or DKIM independently for authenticating e-mail. Thus, we evaluate the results of DMARC authentication and the combination of SPF and DKIM results.

In order to evaluate SPF and DKIM results, we investigated the number of emails that failed both SPF and DKIM certifications. When the results of SPF and DKIM are *neutral, none, unknown, NULL, fail, softfail, permerror, or temperror*, SPF and DKIM will fail to validate the e-mails correctly and will be false positives.

Next, the variety of DMARC authentication results are only *pass* or *fail*. Therefore, if emails from legitimate IP addresses detected by our method are confirmed as failed by DMARC, their deliveries are false positives.

Figure 3 shows the ratio of false positive deliveries from the legitimate IP addresses in sender domain authentications. As shown in Figure 3, 2.8% to 11.1% of e-mails from the legitimate IP addresses are detected as false positive deliveries in the combination of SPF and DKIM authentications. Moreover, 36.9% to 62.7% of deliveries from the legitimate IP addresses are false positives in DMARC authentication.

From these results of false positive detection, SPF, DKIM, and DMARC determine most e-mails from the legitimate IP addresses detected by our method as spoofed e-mails incorrectly. In contrast, our method can correctly determine all these e-mails as legitimate

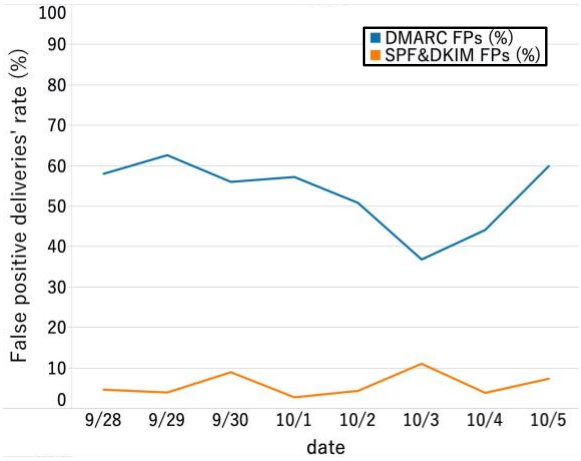


Figure 3. FP deliveries' rate in SPF, DKIM, and DMARC

deliveries.

Therefore, we confirmed that our method can detect deliveries that make false positives in the conventional sender domain authentications with high accuracy without using any computational loaded anti-spam systems.

6. CONCLUSION

In this paper, we proposed a method to detect false positives in sender domain authentication by analyzing DMARC reports.

Our approach summarizes DMARC reports focusing on the results of sender domain authentications and the matching of domain names of the following three combinations: Header-from domain and Envelope-from domain, Header-from domain and DKIM signature domain, and Envelope-from domain and DKIM signature domain. Then, we applied X-means clustering, which is clustering algorithm extended K-means to summarized DMARC reports. Next, we checked whether one or more IP addresses in each cluster are included in Spamhaus blocklist or not. Finally, our method determined the clusters which no IP addresses are included in the Spamhaus blocklist as legitimate sender's server clusters.

As the results of applying the dataset to our method, 254 to 480 IP addresses, which were not listed as spammer's IP addresses in the Spamhaus blocklist were classified as legitimate IP addresses. Additionally, we evaluated these IP addresses by checking the sender domain authentication results. As the evaluation results, 2.8% to 11.1% of the e-mails sent from the legitimate IP addresses detected by our method were false positives in the combinations of SPF and DKIM authentication. In addition, 6.9% to 62.7% of the deliveries from the legitimate IP addresses are false positives in DMARC authentication.

Therefore, we confirmed that our method can detect false positive deliveries in sender domain authentication with high accuracy based on the sender's IP address legitimacy which is provided by our DMARC reports analysis.

7. ACKNOWLEDGMENTS

We would like to thank TwoFive Inc. for supporting this study.

8. REFERENCES

[1] FBI (Federal Bureau of Investigation). *Business Email Compromise The $26 Billion Scam*. [online] Available at: https://www.ic3.gov/media/2019/190910.aspx

[Accessed 8 Jan. 2020].

[2] M. Wong and W. Schlitt. 2006. *Sender Policy Framework (SPF) for authorizing use of domains in e-mail*. RFC4408.

[3] D. Crocker, T. Hansen and M. Kucherawy.2011.

DomainKeys Identified Mail (DKIM) signatures. STD 76.

[4] M. Kucherawy and E. Zwicky. 2015. *Domain-based message authentication, reporting, and conformance (DMARC)*. RFC 7489.

[5] E. Harris. *The Next Step in the Spam Control War: Greylisting*. [online] Available at:

http://projects.puremagic.com/greylisting/whitepaper.html. [Accessed 8 Jan. 2020].

[6] N. Kitagawa, H. Takakura, and T. Suzuki. 2012. An anti-spam method via real-time retransmission detection. In *2012 18th IEEE International Conference on Networks (ICON)*(2012), 382–388. DOI:http://dx.doi.org/10.1109/icon.2012.6506588

[7] I. Androutsopoulos, J. Koutsias, K.V. Chandrinos, and C.D. Spyropoulos. 2000. An experimental comparison of naive Bayesian and keyword-based anti-spam filtering with personal e-mail messages. In *Proceedings of the 23rd annual international ACM SIGIR conference on Research and development in information retrieval - SIGIR 00*(2000), 160–167. DOI:http://dx.doi.org/10.1145/345508.345569

[8] S. Aggarwal, V. Kumar, and S.D. Sudarsan. 2014. Identification and Detection of Phishing Emails Using Natural Language Processing Techniques. In *Proceedings of the 7th International Conference on Security of Information and Networks - SIN 14* (2014), 217–222. DOI:http://dx.doi.org/10.1145/2659651.2659691

[9] W. Feng, J. Sun, L. Zhang, C. Cao, and Q. Yang. 2016. A support vector machine based naive Bayes algorithm for spam filtering. In *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)* (2016), 1–8. DOI:http://dx.doi.org/10.1109/pccc.2016.7820655

[10] M. Crawford, T.M. Khoshgoftaar, J.D. Prusa, A.N. Richter, and H.A. Najada. 2015. Survey of review spam detection using machine learning techniques. *Journal of Big Data*2, 1 (May 2015), 23. DOI:http://dx.doi.org/10.1186/s40537-015-0029-9

[11] The Apache Software Foundation.

The Apache SpamAssassin Project. [online] Available at: http://spamassassin.apache.org/. [Accessed 8 Jan. 2020].

[12] S. Sinha, M. Bailey, and F. Jahanian. 2008. Shades of grey: On the effectiveness of reputation-based "blacklists". In *2008 3rd International Conference on Malicious and Unwanted Software (MALWARE)*(2008), 727–734. DOI:http://dx.doi.org/10.1109/malware.2008.4690858

[13] D. Pelleg and A.W. Moore. 2000. X-means: Extending K-means with Efficient Estimation of the Number of Clusters. In *Proceedings of the Seventeenth International Conference on Machine Learning (ICML 2000)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 727–734.

[14] The Spamhaus Project Ltd. *Spamhaus ZEN*. [online]. Available at: https://www.spamhaus.org/zen/. [Accessed 8 Jan. 2020].

Classification of Medical Data using Character-level CNN

Kazuteru Miyazaki
National Institution for Academic Degrees and Quality Enhancement of Higher Education
1-29-1, Gakuennichimachi, Kodaira, Tokyo, 187-8587 JAPAN
+81-42-307-1834
teru@niad.ac.jp

ABSTRACT
It is necessary to handle an enormous amount of electronic data in medical practice. Therefore, a support system using information technology is desired to analyze the data. In this paper, we propose a preliminary system using character-level convolutional neural networks in order to improve the classification performance of text data on medical practice. The effectiveness of the proposed system is confirmed by the testbed called the NTCIR-13 MedWeb task [15].

CCS Concepts
• **Computing methodologies→Neural networks.**

Keywords
Deep Learning; Medical Data; Character-level CNN; NTCIR-13 MedWeb task.

1. INTRODUCTION
It is necessary to handle an enormous amount of electronic data in medical data. We know recently many results such as diagnosis support [1] using deep learning for enormous amounts of image data. On the other hand, there are many text data along with images in the medical field. In particular, it is expected that a medical diagnosis can be realized from the patient's raw claims obtained through an interview. NTCIR-13 MedWeb (Medical Natural Language Processing for Web Document) task [15] is known as a mock example of such the raw claims, and we will use the data in order to explore the applicability of deep learning to a medical diagnosis using text data.

This paper deals with the classification of text data as electronic data. We know the character-level convolutional neural networks (character level CNN) [18] as a method to classify text data. Though deep learning is particularly effective in image classification, character level CNN is known as an extension of its power to text classification.

We have confirmed the effectiveness of character level CNN in a matching test that were performed for selecting appropriate nomenclature of major fields to be given from an arbitrary diploma policy [11]. Also, we have proposed a method for judging consistency between diploma and curriculum policies using character level CNN [10].

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388191

NTCIR Project
NTCIR-13 MedWeb
Research Purpose Use of Test Collection

[JAPANESE] [NTCIR Home] [NTCIR Data Home]

NTCIR-13 MedWeb (Medical Natural Language Processing for Web Document)

Test Collection

NTCIR-13 MedWeb (Medical Natural Language Processing for Web Document) task requires to perform a multi-label classification that labels for eight diseases/symptoms must be assigned to each tweet. Given pseudo-tweets, the output are Positive:p or Negative:n labels for eight diseases/symptoms. The achievements of this task can almost be directly applied to a fundamental engine for actual applications.

This task provides pseudo-Twitter messages in a cross-language and multi-label corpus, covering three languages (Japanese, English, and Chinese), and annotated with eight labels such as influenza, diarrhea/stomachache, hay fever, cough/sore throat, headache, fever, runny nose, and cold. For more details, please refer to the Task data section and Overview of the NTCIR-13: MedWeb Task [PDF].

References

Shoko Wakamiya, Mizuki Morita, Yoshinobu Kano, Tomoko Ohkuma and Eiji Aramaki: Overview of the NTCIR-13 MedWeb Task, In Proceedings of the 13th NTCIR Conference on Evaluation of Information Access Technologies (NTCIR-13), pp. 40-49, 2017. [PDF]

Task data

NTCIR-13 MedWeb (Medical Natural Language Processing for Web Document) task provides pseudo-Twitter messages (in Japanese, English, and Chinese) with labels for eight diseases/symptoms such as influenza, diarrhea/stomachache, hay fever, cough/sore throat, headache, fever, runny nose, and cold.

Creating Pseudo-Tweets

Owing to the Twitter developer policy on data redistribution, the tweet data crawled using the Twitter API are not publicly available. Therefore, we created Japanese pseudo-tweets by a crowdsourcing service. Then, the Japanese pseudo-tweets were translated into English and Chinese by relevant first-language practitioners. Note that ID corresponds to the corpora of other language (e.g., the tweet of "135en" corresponds to the tweets of "135ja" and "135zh" as shown in Table below).

Symptom Labeling

Two annotators attached Positive:p or Negative:n labels of eight symptoms to tweets, respectively. For more information, please check the annotation guideline [figshare].

Corpus Size

Japanese, English, and Chinese corpora consist of 2,560 tweet texts, respectively. Each corpus is divided into Training data consisting of 1,920 tweet texts (75% of the whole corpus) and test data corpus consisting of 640 tweet texts (25% of the whole corpus).

Table. Examples of pseudo-tweets with labels

ID	Tweet	Influenza	Diarrhea	Hayfever	Cough	Headache	Fever	Runnynose	Cold
135ja	風邪で鼻づまりがやばい。	n	n	n	n	n	n	p	p
135en	I have a cold, which makes my nose stuffy like crazy.	n	n	n	n	n	n	p	p
135zh	感冒引起的鼻塞很烦人。	n	n	n	n	n	n	p	p

To obtain the test collection

The test collection and data are available from NII free of charge.

- **NTCIR-13 MedWeb Test Collection** is downloadable from **NII/IDR** at:
  NII IDR: http://www.nii.ac.jp/dsc/idr/en/ntcir/ntcir.html

(CC BY 4.0)
NTCIR-13 MedWeb Test Collection is licensed under a Creative Commons Attribution 4.0 International License.

Reference

- The terms of use [PDF]
- Task Overview of NTCIR-13 MedWeb Task : Overview of the NTCIR-13: MedWeb Task [PDF]
- NTCIR-13 MedWeb website

Contact us: ntc-secretariat@nii.ac.jp

[JAPANESE] [NTCIR Home] [Top of this page] [NTCIR Data Home]

Updated on : 2018-07-23
ntc-admin@nii.ac.jp

Figure 1. NTCIR-13 MedWeb page [16].

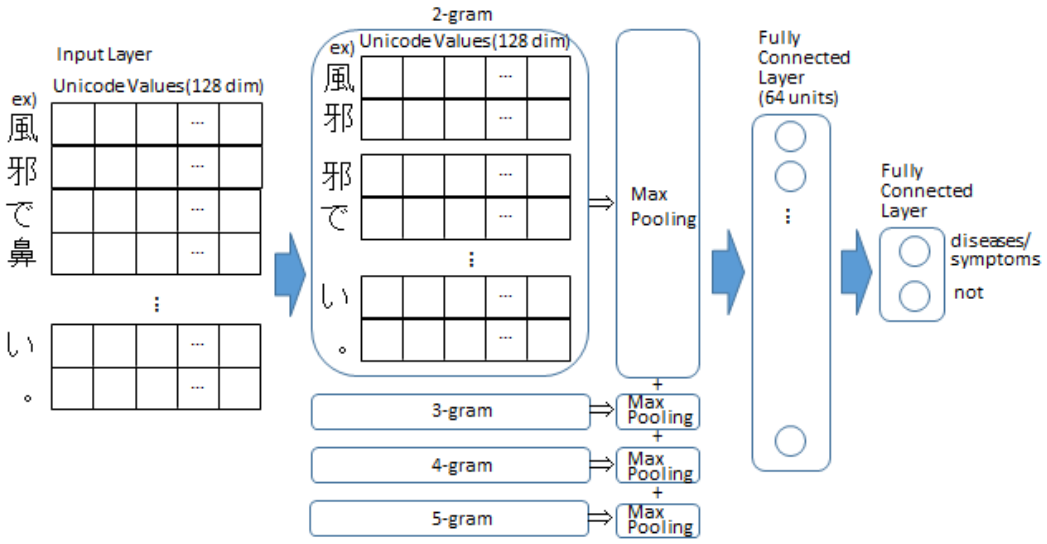


Figure 2. The structure of Character-level CNN used in this paper.

This paper focuses on developing a system for improvement of the classification performance of text data on medical practice. We propose a preliminary system using character level CNN in order to improve the classification performance. The effectiveness of the proposed system is confirmed by the testbed called the NTCIR-13 MedWeb.

2. NTCIR-13 MEDWEB TASK

In the medical field, there are many text data along with images. In particular, it is expected that medical diagnosis can be realized from the patient's raw claims obtained through an interview. NTCIR-13 MedWeb task is known as a mock example of such data.

We explain the NTCIR-13 MedWeb task by citing the content of the web page [16] as shown in Figure 1. NTCIR-13 MedWeb task requires to perform a multi-label classification that labels for eight diseases/symptoms must be assigned to each tweet. Given pseudo-tweets, the output are Positive:p or Negative:n labels for eight diseases/symptoms. The achievements of this task can almost be directly applied to a fundamental engine for actual applications.

This task provides pseudo-Twitter messages in a cross language and multi-label corpus, covering three languages (Japanese, English, and Chinese), and annotated with eight labels such as influenza, diarrhea/stomachache, hay fever, cough/sore throat, headache, fever, runny nose, and cold. Two annotators attached Positive:p or Negative:n labels of eight symptoms to tweets, respectively. Japanese, English, and Chinese corpora consist of 2,560 tweet texts, respectively. Each corpus is divided into Training data consisting of 1,920 tweet texts (75% of the whole corpus) and test data corpus consisting of 640 tweet texts (25% of the whole corpus). We can get more details in the paper [15].

3. CLASSIFICATION OF NTCIR-13 MEDWEB TASK USING CHARACTER-LEVEL CNN

3.1 Basic Data

This paper deals with the text classification problem on the NTCIR-13 MedWeb task. Text classification can be regarded as a problem that categorizes text data based on its contents. Several methods for solving text classification problems, such as support vector machine, have been proposed. Traditionally, approaches using natural language processing techniques such as morphological analysis and syntactic analysis have been mainstream. Such the pre-processing often becomes an obstacle to application to actual problems since processing steps increase.

On the other hand, in recent years, the approach using a neural network represented by deep learning is attracting attention because of its high versatility. We therefore attempt to solve the text classification problem using deep learning. Deep learning has been successful in image analysis [5] and computer game programming [9, 12, 13], herein training is usually performed using convolutional neural networks (CNN). For example, by repeating CNN and applying any image and the meaning of the respective image (correct answer) as a teaching signal, classification can be performed on unknown images. However, when targeting the NTCIR-13 MedWeb task, it is mainly necessary to handle natural language processing instead of images.

If we apply deep learning to natural language processing, the method to configure input to the network is very important. It is generally necessary to replace the document with a numerical value when inputting text data into a neural network. For this purpose, methods using bug-of-words [3] and distributed word representations [1, 6, 14] are well-known. In particular, word2vec [6] and GliVe [14] are often used.

Table 1. Validation Results.TP:True Positive, FN:False Negative, FP:False Positive, TN:True Negative

TV	Evaluation	influenza	diarrhea/stomachache	hay fever	cough/sore throat	headache	fever	runny nose	cold
0.0	TP	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
	FN	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	FP	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
	TN	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.1	TP	1.00	1.00	0.98	1.00	1.00	0.95	0.99	0.98
	FN	0.00	0.00	0.02	0.00	0.00	0.05	0.01	0.02
	FP	0.10	0.04	0.02	0.01	0.01	0.06	0.05	0.03
	TN	0.90	0.96	0.98	0.99	0.99	0.94	0.95	0.97
0.3	TP	1.00	1.00	0.98	1.00	1.00	0.95	0.99	0.98
	FN	0.00	0.00	0.02	0.00	0.00	0.05	0.01	0.02
	FP	0.10	0.04	0.02	0.01	0.01	0.05	0.05	0.03
	TN	0.90	0.96	0.98	0.99	0.99	0.95	0.95	0.97
0.5	TP	1.00	1.00	0.98	1.00	1.00	0.95	0.99	0.97
	FN	0.00	0.00	0.02	0.00	0.00	0.05	0.01	0.03
	FP	0.10	0.04	0.02	0.01	0.01	0.04	0.04	0.03
	TN	0.90	0.96	0.98	0.99	0.99	0.96	0.96	0.97
0.7	TP	1.00	1.00	0.98	1.00	1.00	0.92	0.98	0.97
	FN	0.00	0.00	0.02	0.00	0.00	0.08	0.02	0.03
	FP	0.10	0.04	0.02	0.01	0.01	0.04	0.04	0.03
	TN	0.90	0.96	0.98	0.99	0.99	0.96	0.96	0.97
0.9	TP	1.00	1.00	0.96	0.99	1.00	0.91	0.96	0.97
	FN	0.00	0.00	0.04	0.01	0.00	0.09	0.04	0.03
	FP	0.10	0.04	0.02	0.01	0.01	0.04	0.04	0.02
	TN	0.90	0.96	0.98	0.99	0.99	0.96	0.96	0.98

A sentence is usually broken down into word units, and word2vec output values are used as input to the network (e.g. [4). On the other hand, we know the character-level Convolutional Neural Network [18] (Character-level CNN) as a more versatile technology.

3.2 Character-level CNN

We explain the Character-level CNN used in this paper according to Figure 2. After breaking a sentence down into character units, each unit is converted into a corresponding character code (e.g., Unicode values) and input into the network in character-level CNN. Thus, sentences can be treated as images. Character-level CNN is used by the Web service Retty [19] to search for places serving delicious food based on online reviews. We also know its use in education [10, 11].

Here, we used unicode values when inputting each character into the network. The convolutions involved executing multiple kernel sizes for the same input. The horizontal size was the dimension size of 1 character horizontally; for the vertical size, we used four sizes of 2, 3, 4, and 5 characters. In this way, the convolutions would obtain n-grams. For example, “風邪で鼻づまりがやばい。” is inputted to the network, {風邪, 邪で, で鼻, 鼻づ, づま, まり, りが, がや, やば, ばい, い。} is obtained as 2-gram and {風邪で, 邪で鼻, で鼻づ, 鼻づま, づまり, まりが, りがや, がやば, やばい, ばい。} is obtained as 3-gram.

With multiple kernels, after sending the result of the convolutions to the respective pooling layers, it is placed on a fully connected layer. Finally, an output of the necessary number of dimensions is obtained. In this paper, we build a network for each diseases/symptoms and obtain a two-dimensional output of there is a diseases/symptoms or not. We expressed one character in 128 dimensions. Convolution was performed 64 times for each n-gram. These values were determined by preliminary experiments. The maximum length of input is 140 words in Japanese.

3.3 Combination with Reinforcement Learning

Furthermore, as a proposed method, we have considered that the result of the learned network of character-level CNN is corrected using the reinforcement learning method. Specifically, the reproducibility test is performed on the learned network, and if classification is successful, a reward is given, and if it fails, a penalty is given. This reward and penalty are distributed by Profit Sharing (PS) [7, 8] in the Appendix, and the result of learning is used as a correction value.

4. VALIDATION OF THE PROPOSED METHOD

4.1 Validation Method

We have applied character-level CNN to the NTCIR-13 MedWeb task in Japanese.

For each of the eight diseases/symptoms, learning is performed using the network shown in Figure 2. As an example, the flow of processing when learning disease/symptoms A is shown below.

- Convert each word in a tweet data for learning into unicode values that are represented by 128 dimensions.
- Input the value obtained in step1 into the network in Figure2.
- If the inputted tweet data is for disease A, update the network parameters so that the values of "disease/symptoms" is 1.0 and "not" is 0.0. Otherwise, update the network parameters so that the values of "disease" is 0.0 and "not" is 1.0.

When verifying the result, tweet data for verification is input to each learned network. For example, when tweet data of disease A is input to a network that has learned about disease A, if the values of "diseases/symptoms" is close to 1.0 and "not" is close to 0.0, the learning is regarded as successful. Otherwise, it is determined that the learning has failed.

4.2 Validation Results

The effectiveness of the proposed system is confirmed by the testbed called the NTCIR-13 MedWeb task. The results shown in Table 1. TP, FN, FP and TN means that true positive, false negative, false positive and true negative, respectively. From TV=0.0 to 0.9 are threshold value where the network value exceeds the value, the output value is determined to be 1.0, i.e., there is the disease/symptoms. Note that the results in Table 1 are mean values for each disease/symptoms.

When the threshold value is 0.1 or more, we can confirm that TP and TN are close to 1.0 and FN and FN are close to 0.0. We can therefore confirm that the effectiveness of our proposed method using character-level CNN.

In order to confirm the stability of the experimental results, as an example, Table 2 shows five results in the case of diarrhea/stomachache. The values other than No. 4 are the same as the values shown in Table 1, and the results of No. 4 are not significantly different from the values in Table 1. Therefore, it can be confirmed that there is no problem in stability.

Furthermore, we have confirmed the effectiveness of combination with reinforcement learning. When the first 80 learning data were input to the learned network for each item, only the diarrhea/stomachache result had a poor recall result. Therefore, we distributed a penalty with PS only to the output of the diarrhea/stomachache result, and lowered the value of the output. As a result, the performance of the diarrhea/stomachache result was improved. It means that character-level CNN with reinforcement learning is effective in the text classification.

5. CONCLUSION

In this paper, we have proposed a preliminary system using character-level convolutional neural networks in order to improve the classification performance for medical practice. The effectiveness of the proposed system has been confirmed by the testbed called the NTCIR-13 MedWeb task.

In this task, each data is independent and it is unsuitable confirm an effect corresponding to the delay reward of reinforcement learning method. Therefore, in the future, we plan to apply the proposed method to analysis of timelines and/or biological signals.

In particular, we are currently collecting my three-point electrooculography sensors, the accelerometer and gyroscope sensors by the eye sensing glasses called JiNS MEME™ [20]. Also these sensor's values are combined with the blood pressure measured by a smart watch to help prevent drowsiness of the driver. In this case, we should use a deep Q-network [12, 13] and DQNwithPS [9] instead of QL and PS as a reinforcement learning method, since it is necessary to handle continuous value input.

APPENDIX A: PROFIT SHARING

A.1 The Domain

Consider an agent in an unknown environment. After perceiving sensory input from the environment, the agent selects and executes an action. Time is discretized by one input-action cycle. Action selects one from among the discrete types. The discrete types of action is called the number of actions and denoted M.

The pair consisting of the state and an action selected in a state is called a rule. Rewards and penalties based on a series of actions are provided from the environment, and a reward is given to a state or an action causing transition to a state in which our purpose is achieved, whereas a penalty given to a state or corresponding

Table 2. Five results of diarrhea/stomachache

TV	Evaluation	No.1	No.2	No.3	No.4	No.5
0.0	TP	1.00	1.00	1.00	1.00	1.00
	FN	0.00	0.00	0.00	0.00	0.00
	FP	1.00	1.00	1.00	1.00	1.00
	TN	0.00	0.00	0.00	0.00	0.00
0.1	TP	1.00	1.00	1.00	0.97	1.00
	FN	0.00	0.00	0.00	0.03	0.00
	FP	0.04	0.04	0.04	0.03	0.04
	TN	0.96	0.96	0.96	0.97	0.96
0.3	TP	1.00	1.00	1.00	0.97	1.00
	FN	0.00	0.00	0.00	0.03	0.00
	FP	0.04	0.04	0.04	0.02	0.04
	TN	0.96	0.96	0.96	0.98	0.96
0.5	TP	1.00	1.00	1.00	0.97	1.00
	FN	0.00	0.00	0.00	0.03	0.00
	FP	0.04	0.04	0.04	0.02	0.04
	TN	0.96	0.96	0.96	0.98	0.96
0.7	TP	1.00	1.00	1.00	0.97	1.00
	FN	0.00	0.00	0.00	0.03	0.00
	FP	0.04	0.04	0.04	0.02	0.04
	TN	0.96	0.96	0.96	0.98	0.96
0.9	TP	1.00	1.00	1.00	0.97	1.00
	FN	0.00	0.00	0.00	0.03	0.00
	FP	0.04	0.04	0.04	0.02	0.04
	TN	0.96	0.96	0.96	0.98	0.96

action in which our purpose is not achieved. A rule series that begins from a reward/penalty state or an initial state and ends with the next reward/penalty state is called an episode. A rule always existing on a detour is called an ineffective rule, and otherwise called an effective rule.

A.2 Profit Sharing Algorithm

PS learns a rational policy by propagating a reward backward in an episode when a reward is given. Assume that a reward R is given at time $n + 1$ and the corresponding episode is $\{(S_1, a_1), (S_2, a_2), \cdots, (S_t, a_t), \cdots, (S_n, a_n)\}$, then the amount of rewards (the evaluation value) of the rule (S_t, a_t), $Q(S_t, a_t)$, is updated as follows:

$$Q(S_t, a_t) \leftarrow Q(S_t, a_t) + f(n-t), t = n, n-1, \ldots, 1, \quad (1)$$

where $f(0) = R$. The function f (k) to propagate a reward is known as a reinforcement function. In this paper, we use a geometrically descending function:

$$f(i) = \lambda^i R, \quad (2)$$

where λ ($0 < \lambda < 1$) is the discount rate.

A.3 The Rationality Theorem of Profit Sharing

If the reinforcement function satisfies the following condition, ineffective rules will not be enhanced over effective rules.

$$L\sum_{j=i}^{W} f(j) < f(i-1), \forall i = 1,2,\ldots,W \quad (3)$$

where W is the maximum episode length and L is the maximum number of effective rules in the state [8, 10]. A geometric decreasing function satisfies the condition is as follows.

$$f(i) = \lambda f(i-1), \forall i = 1,2,\ldots,W, where\ \lambda \leq 1/(L+1). \quad (4)$$

The value of L cannot be known in advance, but it is sufficient to set the maximum number of rules available in each state minus 1. The simplest and representative geometric decreasing function is $\lambda = M$ in the equation (2).

6. REFERENCES

[1] Bengio, Y., Ducharme, R., Vincent, P. and Jauvin, C. 2003. A neural probabilistic language model, Journal of machine learning research, Vol.3, pp.1137-1155.

[2] Geert, L., Thijs, K., Babak, E. B., Arnaud, A. A. S., Francesco, C., Mohsen, G., Jeroen, A. W. M. L., Bram, G. and Clara, I. S. 2017. A Survey on Deep Learning in Medicine Image Analysis, Medicine Image Analysis, Vol.42.

[3] Johnson, R. and Zhang, T. 2014. Effective use of word order for text categorization with convolutional neural networks, arXiv preprint arXiv:1412.1058.

[4] Kim, Y.2014. Convolutional Neural Networks for Sentence Classification, Proc. of the 2014 Conference on Empirical Methods in Natural Language Processing, pp. 1746-1751.

[5] Le, Q. V., Ranzato, M., Monga, R., Devin, M., Chen, K. Corrado, G. S., Dean, J. and Ng, A. Y. 2012. Building Highlevel Features Using Large Scale Unsupervised Learning, Proc. of the 29th International Conference on Machine Learning, pp.507-514.

[6] Mikolov, T., Chen, K., Corrado, G. and Dean, J. 2013. Efficient Estimation of Word Representations in Vector Space, arXiv:1301.3781.

[7] Miyazaki, K. and Yamamura, M. and Kobayashi, S.1994. A Theory of Profit Sharing in Reinforcement Learning, Transactions of the Japanese Society for Artificial Intelligence, Vol.9, No.4, pp.580-587 (in Japanese).

[8] Miyazaki, K. 2010. Exploitation-Oriented Learning XoL : A New Approach to Machine Learning Based on Trial-and-Error Searches, Multi-Agent Applications with Evolutionary Computational and Biologically Inspired Technologies : Intelligent Techniques for Ubiquity and Optimization, IGI Globel, pp.267-293.

[9] Miyazaki, K. 2017. Exploitation-Oriented Learning with Deep Learning - Introducing Profit Sharing to a Deep Q-Network - , Journal of advanced computational intelligence and intelligent informatics, Vol.21, No.5, pp.849-855.

[10] Miyazaki, K. and Ida, M. 2018. Consistency Assessment between Diploma Policy and Curriculum Policy using Character-level CNN, Proc. of Joint 10th International Conference on Soft Computing and Intelligent Systems and 19th International Symposium on Advanced Intelligent Systems (SCIS&ISIS2018).

[11] Miyazaki, K., Takahashi, N. and Mori, R. 2019. Research on Consistency between Diploma Policies and Nomenclature of Major Disciplines: Deep Learning Approach, Proc. of 2019 7th International Conference on Information and Education Technology (ICIET2019).

[12] Mnih, V., Kavukcuoglu, K., Silver, D., Graves, A., Antonoglou, I., Wierstra, D., and Riedmiller, M. 2013. Playing Atari with Deep Reinforcement Learning, NIPS Deep Learning Workshop 2013.

[13] Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., Graves, A., Riedmiller, M., Fidjeland, A. K., Ostrovski, G., Petersen, S., Beattie, C., Sadik, A., Antonoglou, I., King, H., Kumaran, D., Wierstra, D., Legg S., and Hassabis D. 2015. Human-level control through deep reinforcement learning, Nature, Vol.518, pp.529-533.

[14] Pennington, J., Socher, R. and Manning, C. 2014. GloVe: Global vectors for word representation, Proc. of the 2014 conference on EMNLP, pp.1532-1543

[15] Wakamiya, S., Morita, M., Kano, Y., Ohkuma, T. and Aramaki, E. 2017. Overview of the NTCIR-13 MedWeb Task, In Proceedings of the 13th NTCIR Conference on Evaluation of Information Access Technologies (NTCIR-13), pp. 40-49.

[16] http://research.nii.ac.jp/ntcir/permission/ntcir-13/perm-en-MedWeb.html [accessed: 2019-11-08].

[17] Watkins, C. J. H. and Dayan, P. 1992. Technical note: Qlearning, Machine Learning, Vol.8, pp.55-68.

[18] Zhang, X., Zhao, J. and LeCun, Y. 2015. Characterlevel Convolutional Networks for Text Classification, arXiv:1509.01626.

[19] https://retty.me [accessed: 2019-11-08]

[20] https://jins-meme.com/en/products/es/[accessed: 2019-11-08]

Chapter 2

Image Intelligent Recognition and Analysis Method

Food Image Classification with Improved MobileNet Architecture and Data Augmentation

Sirawan Phiphiphatphaisit
PhD Student, Department of Information Technology
Faculty of Informatics, Mahasarakham University
Maha Sarakham, Thailand
61011261005@msu.ac.th

Olarik Surinta
Multi-agent Intelligent Simulation Laboratory (MISL)
Faculty of Informatics, Mahasarakham University
Maha Sarakham, Thailand
olarik.s@msu.ac.th

ABSTRACT
The real-world food image is a challenging problem for food image classification, because food images can be captured from different perspective and patterns. Also, many objects can appear in the image, not just foods. To recognize food images, in this paper, we propose a modified MobileNet architecture that is applies the global average pooling layers to avoid overfitting the food images, batch normalization, rectified linear unit, dropout layers, and the last layer is softmax. The state-of-the-art and the proposed MobileNet architectures are trained according to the fine-tuned model. The experimental results show that the proposed version of the MobileNet architecture achieves significantly higher accuracies than the original MobileNet architecture. The proposed MobileNet architecture significantly outperforms other architectures when the data augmentation techniques are combined.

CCS Concepts
• **Computing methodologies → Object recognition**
• **Computing methodologies → Neural networks.**

Keywords
Food Image classification; Convolutional Neural Network; MobileNet Architecture; Data Augmentation.

1. INTRODUCTION
Nowadays, people are becoming obese and overweight due to the imbalance between calorific intake and use. This increases the risk of other diseases such as diabetes, sleep apnea, acid reflux, and heart disease [12]. Nutritionists advise obese and overweight people to exercise and to monitor their daily consumption of calories [4]. Due to the assessment of calorie intakes into the body, Ege and Yani [3] proposed a multi-task convolutional neural network (CNN) method that allows the CNN architecture to learn from food calories, categories, ingredients, and cooking directions data. Furthermore, Myers et al. [13] presented a system that recognizes the contents of food from a single image, and then predict calories using the CNN based classifier. Then, people can estimate calories from food images.

In recent years, most research in food image classification has focused on hand-crafted features that consist of a color histogram [10,21], local binary pattern (LBP) [10,15], scale invariant feature transform (SIFT) [10], histogram of oriented gradients (HOG) [10,21], and speeded up robust feature (SURF) [2]. These hand-crafted methods are combined with machine learning algorithms to classify food images.

Due to the large-scale of food image datasets, researchers proposed to use deep learning algorithms to learn from the large-scale food image dataset such as the ETH Food-101 dataset which contains 101,000 images from 101 food categories; Food-256 dataset, a data set of 256 food categories with approximately 32,000 food images [2,5,7]. Yanai and Kawano [21] used a pre-trained model of AlexNet architecture for the feature extraction method. This method extracts 6,144 features from the image. In [5], the data augmentation techniques consist of brightness, contrast, saturation, and hue and are applied to food images before feeding to the Inception V3 network. Ming et al. [11] proposed the DietLens, which is a prototype of tracking dietary intake system for Singapore hawker food. The core architecture of the DietLens is the ResNet-50, which contains 50 convolutional layers and one fully connected layer and experiments on 87,470 images. The FoodNet [17], which is an ensemble deep neural network, is proposed to classify the Food-101 dataset. This network combined three well-known networks (AlexNet, GoogLeNet, and ResNet) as the ensemble network. The output of three networks and concatenate are passed to a fully connected layer to classify food images.

(A) (B)

Figure 1. Example of ETH Food-101 dataset. a) The apple pie category and b) the similarity shape between two categories of apple pie (first row) and Baklava (second row).

The challenge of food image classification is that food images from the same category are captured with different patterns, shapes, and perspective, accordingly to the people who take the image. For example, there are many objects such as forks and spoons, glasses, and bottles that appear in the image. For example of ETH Food-101 dataset, has many different apple pie images (that include other objects, patterns, shapes, and scenes) that

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388179

appear in the apple pie category, as shown in Figure 1a). Even the similarity shape and pattern between the two categories of apple pie and Baklava, as shown in Figure 1b). These kinds of images can decrease the performance of the food image classification.

Related work: Hand-crafted feature extraction methods [14] are used in many image classification applications. In [15], two feature extraction methods consisting of a non-redundant local binary pattern (NRLBP) and the shape context descriptor of the interest points, called structure information are used to describe the local appearance information of food images. The achieved accuracy shows that the combination of the two features can improve classification performance. In [21], the first step uses, the color patches and RootHOG patches, (which is a square root of the L1 normalized HOG) to extract the data from the images. In the second step, the information from the first step is sent to a Fisher vector to encoding and used as the feature vector. This method achieved an accuracy of 65.3% on the UEC Food-100 dataset. In addition, Martinel et al. [10] presented the supervised extreme learning committee approach (ELM) to learning attributes of color, shape, texture, and local features. Then, the output of the ELMs is fed into the structured support vector machine (SVM) to classify food images. The performance achieved by this method is 55.89% and 84.34% on ETH Food-101 and UEC Food-100, respectively.

Nowadays, convolutional neural networks (CNNs), which are the most successful, and widely used for image classification problems [19]. Although, many CNN architectures can compute due to the large-scale images [19] and obtain very high accuracy [9,17]. In the area of food image classification, state-of-the-art CNN architectures such as AlexNet, GoogLeNet, and ResNet are proposed [17], although, the experimental results obtained with tem did not obtain high accuracy. Pandey et al. [17] invented a CNN-based ensemble network, called FoodNet architecture. This architecture consists of a fine-tuned model of AlexNet, GoogLeNet, and ResNet. The networks compute feature vectors and then concatenate all of the feature vectors, and a rectified linear unit (ReLU) used as a non-linear activation. Then, data is passed to a fully connected layer and the softmax function used to predict the output of the food image. The experiments showed that the FoodNet architecture obtained the Top-1 accuracy of 72.12% on ETH Food-101 and 73.50% on Indian food database. Also, the result was not good when the feature vector from the FoodNet architecture was fed into the SVM classifier.

As for the pre-trained model, In [21], the fine-tuning of the deep CNN pre-trained model based on AlexNet network, called DCNN was proposed to examine three food image datasets. The results showed that the fine-tuned DCNN achieved the Top-1 accuracy of 78.77%, 67.57%, and 70.40% on UEC Food-100, UEC Food-256, and ETH Food-101 datasets, respectively. The Inception networks [5,8] are proposed to address the food image classification. Lin et al. [8] presented the DeepFood network to recognize the food image for computer-aided dietary assessment. The DeepFood network, which is applied to an Inception module by adding 1x1 convolutional layers and then connected with two inception modules via an additional max-pooling layer. The best Top-1 accuracy results on UEC Food-256, UEC Food-100, and ETH Food-101 were 54.7%, 76.3%, and 77.4%, respectively. Hassannejad et al. [5] invented a deep network with 54 layers based on Inception V3 to classify three well-known food image datasets and achieved 88.28% on ETH Food-101, 81.45% on UEC Food-100, and 76.17% on UEC Food-256 datasets as top-1 accuracy.

Additionally, data augmentation is proposed to address the problem of insufficient data and to increase the performance of the image classification [1,22]. The data augmentation is also widely used in plant [18] and animal [16], and food [22] image recognition.

Contributions: In this paper, our main contribution is the use of the state-of-the-art deep convolutional neural network, called MobileNet architecture and our proposed MobileNet architecture is applied to recognize a challenging ETH food image dataset that contains 101 food categories.

In our proposed version, we reduce the number of parameters in the model by replacing the average pooling with the global average pooling (GAP) layers; then the overfitting is decreased. Subsequently, the batch normalization (BN), rectified linear unit (ReLU), and dropout layers, are utilized instead of the fully connected layers. Finally, the softmax layer is calculated. The results show that our proposed MobileNet architecture outperforms when compared to the original MobileNet architecture.

Moreover, we evaluate most effective data augmentation techniques to random creating images in the ETH food-101 dataset. We compared data augmentations and combined with the cropping image before passing to train the model. Also, the accuracy increased by approximately 5%. Finally, our proposed MobileNet architecture when combined with the data augmentation techniques outperforms the other methods.

***Paper outline*:** The paper is organized as follows: In Section 2, the MobileNet and the proposed MobileNet architectures are explained. In Section 3, the data augmentation techniques are presented. Experimental results are reported in Section 4. The last section is the conclusion and future work.

2. MOBILENET ARCHITECTURE

We used MobileNet architecture presented by Howard et al. [6] that is designed and based on depthwise separable convolutions to build a lightweight deep CNN that makes a model too small and reduces the computation time. The diagram in Figure 1a) illustrates the MobileNet architecture. Consequently, MobileNet can be implemented for several recognition problems such as object detection, face attributes, fine-grain classification, and landmark recognition.

2.1 Proposed MobileNet Architecture

Our proposed MobileNet architecture was as follows. First, we used the pre-trained model of MobileNet architecture. We decided to remove three layers, including the average pooling, fully connected, and softmax layers from the original network. Second, three extra layers; the global average pooling (GAP) layers, the batch normalization (BN), and softmax layers are attached. The main objective of our proposed MobileNet architecture is helping the network to train faster and achieving higher accuracy. Then, the dropout method is proposed to prevent overfitting. Also, the batch normalization layer helps the network to train faster. The activation function called the rectified linear unit (ReLU) is computed between the batch normalization layer and the dropout layer. After we applied the GAP layers instead of the average pooling, it shows that the parameters in the model are decreased, and impact directly on the size of the model. Finally, for training the proposed network, we used the fine-tuned MobileNet to train the network on the ETH Food-101 dataset. The proposed MobileNet architecture as shown in Figure 2b).

2.2 Depthwise Separable Convolutions Layer

The MobileNet architecture is computed based on depthwise separable convolutions (DS). The concept of decomposition of convolution called factorization is considered to factorize a standard convolution into a depthwise convolution.

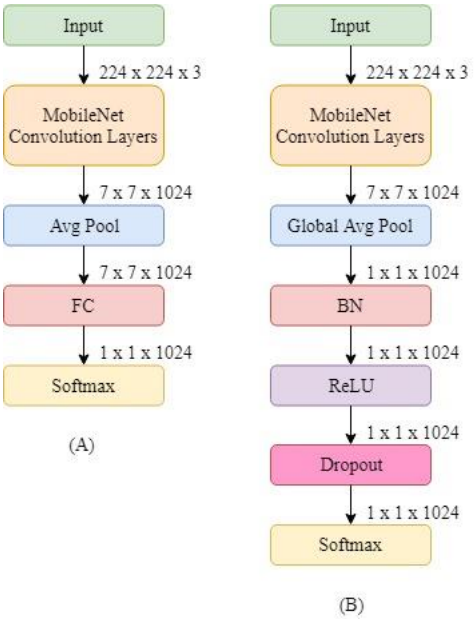


Figure 2. The architectures of the MobileNet. (A) the original MobileNet and, (B) the proposed MobileNet architectures.

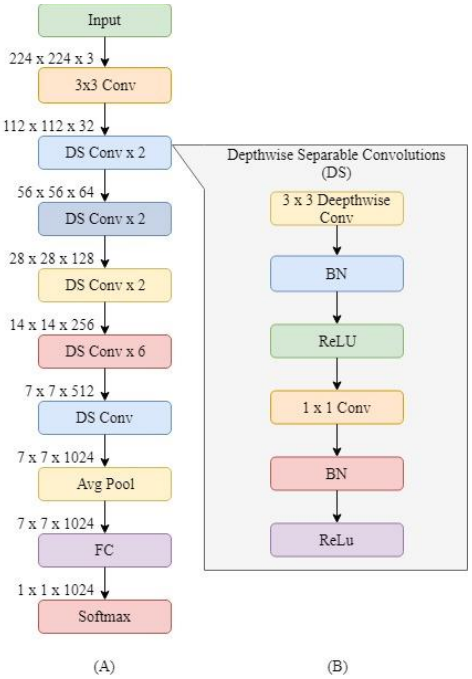


Figure 3. Illustration of the MobileNet architecture. (A) The overall MobileNet architecture and (B) an in-depth explanation of the DS layer.

After that, all depthwise convolution layers are computed with 1x1 convolution called a pointwise convolution, and then combined as the outputs to the next layer. The diagram in Figure 3a) shows the detail of the MobileNet that includes convolutional, depthwise separable convolutions (DS), average pooling, fully connected (FC), and softmax layers.

Figure 3b) shows an in-depth explanation of the DS layer consisting of depthwise convolution, batch normalization (BN), and rectified linear unit (ReLU), respectively.

3. DATA AUGMENTATION TECHNIQUES

Data augmentation is a technique to generate new training image data that relate to the same image. Many data augmentation techniques such as rotation, horizontal, vertical, flip, width shift, height shift techniques are applied to the image recognition problems and the accuracy performance is improved [22]. Samples of image augmentation are shown in figure 4. In this paper, the data augmentation techniques applied to our experiments consists of rescaling, rotation, width shift, height shift, horizontal flip, shear, and zoom.

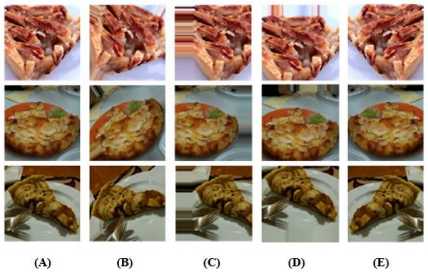


Figure 4. Example of the data augmentation images: (A) original, (B) rotation, (C) width shift, (D) height shift, and (E) horizontal flip images.

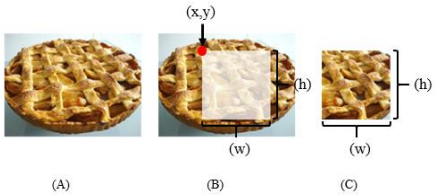


Figure 5. Illustration of the random cropping method. (A) Original food image, (B) random points (x,y) and crop sizes of the cropped image (w, h), and (C) the random cropping image used in training process.

Additionally, the image randomly changes to generate a new image in each training epoch, according to the range of the parameters.

Furthermore, random cropping is applied [20]. In this method, the position of points (x,y) are random, then it automatically crops and resizes to the target size, as shown in Figure 5. In this experiment, the size of the image is 224x224 pixel dimension.

4. EXPERIMENTAL SETUP AND RESULTS

4.1 ETH Food-101 Dataset

In this paper, we evaluate the deep CNN architectures on the benchmark food image dataset. The real-world food images were collected by downloading from foodspotting.com website. The food images are a mix of eastern and western meals such as apple pie, Hamburger, Sashimi, Ramen, Peking duck. The challenging dataset consists of 101,000 food images from 101 food categories,

called the ETH food-101 dataset [2]. Examples of the food images are shown in Figure 6.

Figure 6. Sample real-world food images from the ETH Food-101 dataset.

4.2 Experimental Setup

Due to the large number of images in the dataset, we divided it into four subsets (Set I, Set II, Set III, and Set IV) sizes of 10,100 (randomly selected 100 images from each category), 20,200, 30,300, and 40,400 images to perform all of the experiments. Images in each subset were divided into training, validation, and testing sets of 70%, 10%, and 20%, respectively. For the training of the deep CNN architectures, we used the transfer learning with the following parameter settings: stochastic gradient descent (SGD) solver, batch size of 16, learning rate at 0.0001. We note that entire experiments were carried out using the TensorFlow platform running on Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz, 8GB RAM.

In the experiments, *firstly*, we used the original food images from the ETH Food-101 dataset to experimented with the MobileNet architectures in order to find the appropriate training epoch. *Secondly*, the first data augmentation called random cropping was employed. The program randomly cropped from a part of a food image and resize to the target size, which was 224x224 pixel dimension. *Thirdly*, the data augmentation techniques consisted of rescaling, rotation, width shift, height shift, horizontal flip, shear, and zoom applied according to the random parameters. Suddenly, the food images randomly change in each training epoch. *Finally*, the random cropping image and the data augmentation techniques are combined.

4.3 Experimental Results

We used 5-fold cross-validation in the training and testing phases. The accuracy and standard deviation are used to evaluate the performance of the deep CNN architectures on ETH food-101 dataset.

From the first experiment, it is essential to indicate that a huge number of food images can increase recognition performance. We set up the number of training to 50 epochs, which is similar to previous reports [1,17,23]. The accuracy of Set I with 10,100 images and Set IV with 40,400 images were significantly different. The accuracy results improved from around 42% to 57% when testted on the original MobileNet architecture. Moreover, the results improve from 46% to 67% when performed on the proposed MobileNet architecture, when accuracy increased by more than 10%, as shown in Figure 7. This clearly indicates that recognition performance is increased when using more food images.

We show the obtained results of second to fourth experiments using the proposed MobileNet architecture on four subsets of the ETH Food-101 dataset in Table 1. The table shows that the combination of the data augmentation and random cropping was the best approach in our experiments. This approach outperformed other methods with an increase of around 3-5% accuracy.

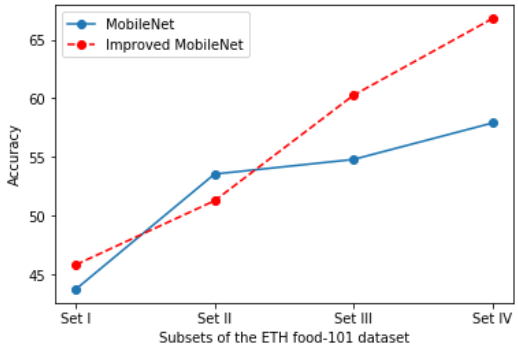


Figure 7. The performance of the MobileNet and proposed MobileNet architectures versus the different number of training samples (Set I - Set IV) on the ETH food-101 dataset.

Table 1. The performance results of food image recognition on four subsets on ETH Food-101 dataset using the approach MobileNet architecture

Methods	Subsets of the EHT Food-101 dataset			
	I	II	III	IV
Without data augmentation	45.84	51.29	60.26	66.78
Random cropping	45.79	55.82	59.52	67.44
With data augmentation	48.71	56.71	62.49	69.86
With data augmentation + random cropping	51.39	59.68	65.97	**72.59**

Table 2. Performances of the five different techniques on ETH Food-101 dataset

Method	The number of image per class	Accuracy (%)
Random Forest Discriminative Components [2]	1,000	50.76
Supervised Extreme Learning Committee [10]	1,000	55.89
Data Augmentation + MobileNet	400	57.90
Data Augmentation + Inception V3 [21]	1,000	70.41
FoodNet: Ensemble Net [17]	1,000	72.10
DeepFood [9]	1,000	**77.00**
Our proposed (Data Augmentation + MobileNet)	400	72.59

From the results in Table 2, the DeepFood architecture obtains the best performances on the ETH Food-101 dataset with an accuracy rate of 77%. Due to the computer used in the experiments, we decided to use the food image only 400 images per class to examine our proposed architecture. However, our proposed MobileNet architecture reached an accuracy of 72.59%. It is only 4.41% less than DeepFood architecture. As a result, our proposed MobileNet architecture outperforms the Random Forest

Discriminative Components [2], Supervised Extreme Learning Committee [10] and three deep CNN architectures; MobileNet, Inception V3 [21] and FoodNet [17].

In addition, the proposed MobileNet created a model size of 22.4MB, which less than the MobileNet architecture 10MB.

5. CONCLUSION

In this paper, we used the state-of-the-art MobileNet architecture on the food image dataset. We also described a MobileNet architecture, which was designed to address the overfitting problem. In this proposed MobileNet architecture, the number of parameters is decreased by applying the global average pooling (GAP) layers. Moreover, the batch normalization (BN), rectified linear unit (ReLU), and dropout layers are combined. Also, the last layer is the softmax. In addition, the data augmentation techniques are computed before transferring to the training process.

From the experimental results, to the best of our knowledge, we trained the MobileNet architecture according to the fine-tuned model. The proposed MobileNet architecture is competitive when compared to the original MobileNet architecture on the ETH food-101 dataset. We also demonstrated the impact of the data augmentation techniques; rotation, shift, flip, shear, zoom, and crop when implemented before assigning to the proposed MobileNet architecture to process. The best performance achieved when the combination of the various data augmentation techniques and the proposed MobileNet architecture.

In future work, we plan to construct the deep ensemble convolutional neural network (CNN) architectures, which are a combination of the state-of-the-art deep CNN architectures. We are interested in extracting the feature vector from the convolutional layers which may work better than individual deep CNN architecture.

6. REFERENCES

[1] Attokaren, D., Fernandes, I., Sriram, A., Murthy, Y. , and Koolagudi, S. 2017. Food classification from images using convolutional neural networks. *TENCON 2017 - 2017 IEEE Region 10 Conference*, 2801–2806.

[2] Bossard, L., Guillaumin, M, and Gool, L. 2014. Food-101 -- Mining Discriminative Components with Random Forests. In *Fleet D., Pajdla T., Schiele B., Tuytelaars T. (eds) Computer Vision – ECCV 2014. ECCV 2014. Lecture Notes in Computer Science, Springer, Cham*. 8694, 446–461.

[3] Ege, T. and Yanai, K. 2017. Image-Based Food Calorie Estimation Using Knowledge on Food Categories, Ingredients and Cooking Directions. In *Proceedings of the on Thematic Workshops of ACM Multimedia 2017* (Thematic Workshops '17), 367–375.

[4] Fatehah, A., Poh, B., Shanita, S., and Wong, J. 2018. Feasibility of Reviewing Digital Food Images for Dietary Assessment among Nutrition Professionals. *Nutrients* 10, ,8 (July 2018), 1–12.

[5] Hassannejad, H., Matrella, G., Ciampolini, P., Munari, I., Mordonini, M., and Cagnoni, S. 2016. Food Image Recognition Using Very Deep Convolutional Networks. In *Proceedings of the 2nd International Workshop on Multimedia Assisted Dietary Management - MADiMa '16*, 41–49.

[6] Howard, A., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Andreetto, M., and Adam H. 2017. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. *ArXiv, abs/1704.04861*, 1–9.

[7] Kawano, Y. and Yanai, K. 2014. FoodCam-256: A Large-scale Real-time Mobile Food RecognitionSystem employing High-Dimensional Features and Compression of Classifier Weights. In *Proceedings of the 22nd ACM international conference on Multimedia (MM '14)*, 761–762.

[8] Liu, C., Cao, Y., Luo, Y., Chen, G., Vokkarane, V., and Ma, Y. 2016. Deepfood: Deep learning-based food image recognition for computer-aided dietary assessment. In *ICOST 2016. Lecture Notes in Computer Science, Springer, Cham*. 9677, 37–48.

[9] Liu, C., Cao, Y., Luo, Y., Chen, G., Vokkarane, V., Ma, Y., Chen, S., and Hou, P. 2018. A New Deep Learning-Based Food Recognition System for Dietary Assessment on An Edge Computing Service Infrastructure. *IEEE Transactions on Services Computing*. 11, 249–261.

[10] Martinel, N., Piciarelli, C., and Micheloni, C. 2016. A supervised extreme learning committee for food recognition. *Computer Vision and Image Understanding.* 148, 67–86.

[11] Ming, Z., Chen, J., Cao, Y., Forde, C., Ngo, C., and Chua, T. 2018. Food Photo Recognition for Dietary Tracking: System and Experiment. In *MultiMedia Modeling*, 129–141.

[12] Must, A., Spadano, J., Coakley, E., Field, A., Colditz, G. and Dietz, W. 1999. The Disease Burden Associated With Overweight and Obesity. *JAMA* 282, 16 (October 1999), 1523–1529.

[13] Myers, A., Johnston, N., Rathod, V., Korattikara, A., Gorban, A., Silberman, N., Guadarrama, S., Papandreou, G., Huang, J., and Murphy, K. 2015. Im2Calories: Towards an Automated Mobile Vision Food Diary. In *2015 IEEE International Conference on Computer Vision (ICCV)*, 1233–1241.

[14] Nanni, L., Ghidoni, S., and Brahnam, S. 2017. Handcrafted vs. non-handcrafted features for computer vision classification. *Pattern Recognition.* 71, 158–172.

[15] Nguyen, D., Zong, Z., Ogunbona, P., Probst, Y., and Li, W. 2014. Food image classification using local appearance and global structural information. *Neurocomputing.* 140, 242–251.

[16] Okafor, E., Schomaker, L., and Wiering, M. 2018. An analysis of rotation matrix and colour constancy data augmentation in classifying images of animals. *J. Information Telecommunication.* 2, 465–491.

[17] Pandey, P., Deepthi, A., Mandal, B., and Puhan, N. B. 2017. FoodNet: Recognizing Foods Using Ensemble of Deep Networks. *IEEE Signal Processing Letters.* 24, 1758–1762.

[18] Pawara, P., Okafor, E., Schomaker, L., and Wiering, M. 2017. Data Augmentation for Plant Classification. In *ACIVS, Springer, Cham*, 615–626

[19] Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., Huang, Z., Karpathy, A., Khosla, A., Bernstein, M., Berg, A., and Fei-Fei, L. 2015. ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision.* 115, 211–252.

[20] Takahashi, R., Matsubara, T., and Uehara, K. 2018. Data Augmentation using Random Image Cropping and Patching for Deep CNNs. *ArXiv, abs/1811.09030*, 1–16.

[21] Yanai, K. and Kawano, Y. 2015. Food Image Recognition using Deep Convolutional Network with Pre-training and Fine-Tuning. In *2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*, 1–6.

[22] Yunus, R., Arif, O., Afzal, H., Amjad, M., Abbas, H., Bokhari, H., Haider, S., Zafar, N., and Nawaz, R. 2019. A Framework to Estimate the Nutritional Value of Food in Real Time Using Deep Learning Techniques. *IEEE Access.* 7, 2643–2652.

[23] Zheng, J., Zou, L., and Wang, Z. 2018. Mid-level deep Food Part mining for food image recognition. *IET Computer Vision.* 12, 298–304.

Deep Learning for Pixel-based Edge Models Classification of Tertiary Dentine Images

Slamet Riyadi
Dept. of Information Technology, Universitas Muhamammadiyah Yogyakarta
Jl. Brawijaya, Tamantirto, Kasihan, Bantul, Yogyakarta 55183 Indonesia
Telp. 62-274387656
riyadi@umy.ac.id

Siti Mayanti
Dept. of Information Technology, Universitas Muhamammadiyah Yogyakarta
Jl. Brawijaya, Tamantirto, Kasihan, Bantul, Yogyakarta 55183 Indonesia
Telp. 62-274387656
mayanti.96@gmail.com

Cahya Damarjati
Dept. of Information Technology, Universitas Muhamammadiyah Yogyakarta
Jl. Brawijaya, Tamantirto, Kasihan, Bantul, Yogyakarta 55183 Indonesia
Telp. 62-274387656
cahya.damarjati@umy.ac.id

Sartika Puspita
Dept. of Dentistry, Universitas Muhammadiyah Yogyakarta
Jl. Brawijaya., Tamantirto, Kasihan, Bantul, Yogyakarta 55183 Indonesia
Telp. 62-274387656
sartika.puspita@umy.ac.id

ABSTRACT
Prevalence of dental caries remains significant clinical problems. The dental caries disease is treated by doing pulp capping. The treatment is evaluated by visually observing the tertiary dentine on x-ray images. This conventional evaluation is not accurate and subjective among the doctors. In order to assist doctor, this research proposed implementation of deep learning method to classify pixel-based edge images of tertiary dentine. The method involves x-ray image data collection, edge modelling, edge training and testing. Eleven pixel-based edge models were defined which consist of eight edge models and three non-edge models. A total number of 660 edge images were extracted from tertiary dentine images and used Convolutional Neural Network deep learning for training and testing. The overall classification of edge images was validated using cross validation method and performed 91% of classification accuracy.

CCS Concepts
• **Computing methodologies→Neural networks.**

Keywords
Deep learning; convolutional neural network; tertiary dentine; edge detection, image processing.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

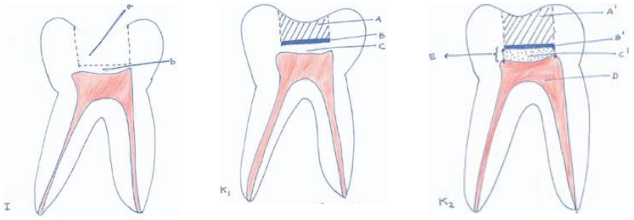
ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388197

1. INTRODUCTION
Indonesia has high prevalence of dental caries both for children and adults. According to Research Report on Basic Health by Ministry of Health 2018, caries was experienced by 88.8% of Indonesia's population and 92.6% of children under five years old [1]. For teeth with caries that can still be treated in the oral cavity, one of the most popular endodontic conservation treatments is pulp capping treatment. Pulp capping is performed by adding protective or treatment material to the exposed pulp and stimulate the growth of tertiary dentin. Evaluation of this treatment is done by observing the results of periapical dental x-rays so that doctor can obtain the condition of density, the presence or absence of edge leakage of tertiary dentin thickness.

The use of x-rays or also called radiographic photographs in the observation and evaluation of dental care has been commonly used in various hospitals and clinics. Radiographic images are obtained from X-ray radiation that penetrates the body structure with different levels depending on the density of organs to produce a different level of gray image and finally produce an X-ray image.

To observe the thickness of tertiary dentin, currently doctor make qualitatively comparison between the results of X-ray images before and after pulp treatment. The comparison resulted information whether the tertiary dentin after treatment is thicker or not. The thicker tertiary dentin after the treatment compare to the before shows an indication of the success of the treatment. Figure 1 (a), (b) and (c) are illustrations of teeth with caries, after temporary lift treatment and after composite treatment, respectively. Tertiary dentin thickness observations were made by comparing thickness after treatment (Figure 1 (b) and (c)) with before treatment (Figure 1 (a)).

In addition to qualitative information, quantitative information on the actual thickness of the dentin is also very much needed as information to support subsequent treatments. Digital image processing technology has an opportunity to process the X-ray image and extract the quantitative information of tertiary dentine thickness.



A. Caries (dx Pulpitis Reversible)

B. Remaining Dentin Thickness

A. Temporary Filling

B. Capping and Linning

C. Tertiary Dentin

A'. Composite Filling

B'. Capping and Linning

C. Tertiary Dentin

D. Pulp Chamber

E. Tertiary Dentin Thickness

(a) (b) (c)

Figure 1. Illustration a tooth (a) with caries; (b) after treatment of temporary filling; and (c) after treatment of composite filling.

Segmentation between dental parts received a lot of attention from researchers. Methods that have been proposed by researchers include phase congruency based on the local structure of imagery [2]. This method is quite strong and is not affected by changes in image size, rotation, translation, changes in light and noise. Other researchers make supervised learning techniques with Bayesian classifier with training-testing input are moments and some statistical characteristics [3]. Another method based on texture feature extraction using the gray level co-occurrence matrix is also proposed to separate each tooth in an x-ray [4].

In terms of edge detection and segmentation, many digital image processing methods have been developed by researchers as shown in Table 1 [5][6][7]. In addition to the methods listed in the table, methods based on training and testing using the deep learning method have been studied for edge detection the last five years [8][9]. These methods were reported to be able to detect the edges of various objects accurately.

From the literature review, no research has been found on the use of image processing technology to estimate tertiary dentin thickness. This is an opportunity to contribute in the application of image processing technology. Therefore, the objective of this research is to implement deep learning method for edge detection of tertiary dentine images.

2. METHODOLOGY

The research involves steps which are summarized as x-ray image collection, edge modelling, edge training and testing. The details are discussed in the following paragraphs.

2.1 X-ray Image Collection

The material used in this study were x-ray photographs of patient teeth which were treated with pulp capping at Oral and Dental Hospital Universitas Muhammadiyah Yogyakarta. In this study, x-ray photographs had been standardized by the hospital. Each patient has three x-rays namely Indication, Control 1, and Control 2. Indication image is the first photo taken by the patient before the pulp capping treatment, Control 1 image is a patient photo when the teeth were treated, and Control 2 is a photograph of patient a couple months after pulp capping treatment. Example of these images are shown in Figure 2.

(a) (b) (c)

Figure 2. (a) Indication image, (b) Control 1, and (c) Control 2.

Table 1. Comparison of previous methods for edge detection [5, 6, 7]

Method	Decsription	Positive	Negative
Thresholding-based			
Gray level fixed thresholding	Detection based on histogram of intensity grey level	Simple, easy to implement, appropriate for bimodal image	Difficult to apply to low contrast images or not bi-modal histograms; Threshold is fixed so that it could not been applied to all image types
Otsu method	Threshold value follows histogram	Compared to fixed thresholding, it is more stable for various types of images	False maxima occurred on small classes
Region-based			
Region growing	Separate areas based on homogeneous pixels	Easy if homogeneous criteria are easily defined	Requires a lot of time and memory
Edge-based			
Prewitt	Based on discontinuity between intensities	Simple, easy to implement	Noise sensitive
Laplacian of gaussian	Apply a combination of laplace and gaussian	Successfully reduced sensitivity to noise	Error often occurs when the intensity varies

2.2 Edge Modelling

In this research, edge models from El-Sayed [1] were used. The model consists of eight categories for edge and three categories for non-edge as shown in Figure 3. Edge categories are numbered from 1 to 8 whether non-edge categories from 9 to 11. These pixel-based edge models were used as models to create training and testing data for tertiary dentine images.

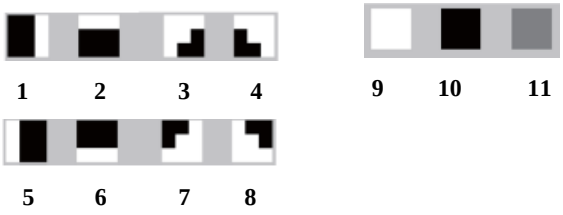


Figure 3. Edge model (a) Edge and (b) non-edge category and number [10].

To create training and testing data from the x-ray images, the image was cropped manually only on the tertiary dentine to ease observation on the edge as shown by red square in Figure 4(a). Small square image of 150x150 pixel were then manually cropped along the edge of tertiary dentine and categorized to a certain model as shown in Figure 5. This edge cropping process resulted 60 cropped images for each category.

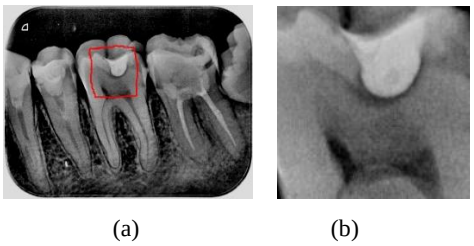


Figure 4. Crop area of tertiary dentine: (a) original images and (b) cropped area.

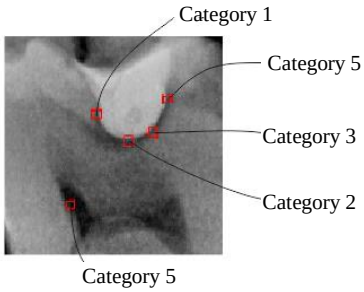


Figure 5. Cropping process on edge and categorization into model number.

2.3 Edge Training and Testing

Training and testing were done using Convolutional Neural Network (CNN) deep learning. CNN is a special type of neural network for processing data that has a mesh topology or grid-like topology. The name of a convolutional neural network indicates that the network uses mathematical operations called convolution. Convolution itself is a linear operation. So, a convolutional neural network is a neural network that uses minimal convolution at one of its layers [11]. CNN is one of the popular algorithms of deep learning that provides regularization of fully connected multi-layer perceptron. It uses the hierarchical patterns to effectively overfitting data and combine local receptive fields, weight and temporal sub-sampling. The common structure of CNN is shown in Figure 6.

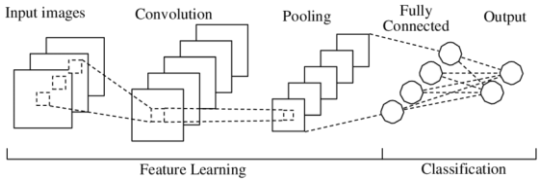


Figure 6. Structure of CNN [12].

Convolutional layer is the first layer that receives input images directly on the architecture. The operation at this layer is the same as the convolution operation, which is doing linear combination filter operation on the local area. Filters are representations of receptive fields of neurons that are connected to the local area of the input image. Convolutional layer performs convolution operations at the output of the previous layer. This layer is the main process that underlies a CNN. The purpose of convolution in image data is to extract features from the input image. This research used several parameters i.e. filter width and number 10 for the convolution, epoch 50, pooling layer 2 and stride 2. Validation of the result was done using 10-fold cross validation using 660 images provided.

3. RESULT AND DISCUSSION

A number of 237 x-ray images from 79 patients have been collected. However, due to incomplete, noisy and low-quality images, only 20 cropped edge images per category or total of 660 images were used. Figure 7 shows example of images of edge model which were cropped from tertiary dentin.

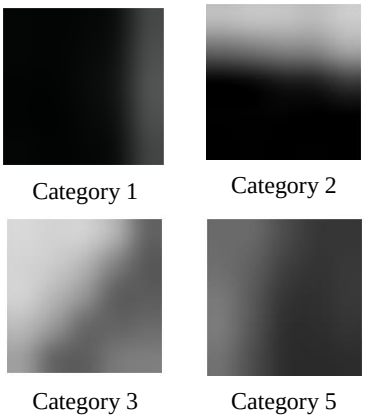


Figure 7. Images of edge model from cropping process in Figure 5.

The training of CNN reached stable condition of 100% accuracy at epoch 32 although it reached down to 80% at epoch 37 as shown in Figure 8. Higher number of epoch should be perform in the next research to obtain more accurate training performance.

Classification results of edge image were obtained by testing the CNN model to edge images. Figure 9 shows the edge image category 1 and the classification result. It can be seen in this figure that three edge images were classified as wrong category due to their similarity to other edge model categories, such as category 4, 7 and 11 (marked with red). The testing resulted overall 91% of accuracy for classification of edge image category.

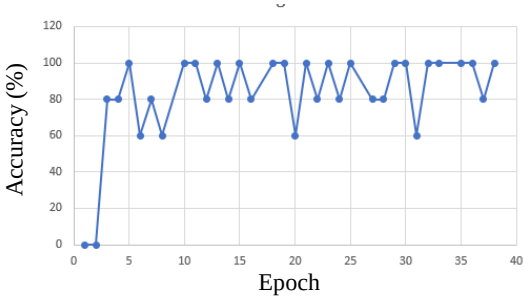


Figure 8. Accuracy of CNN training.

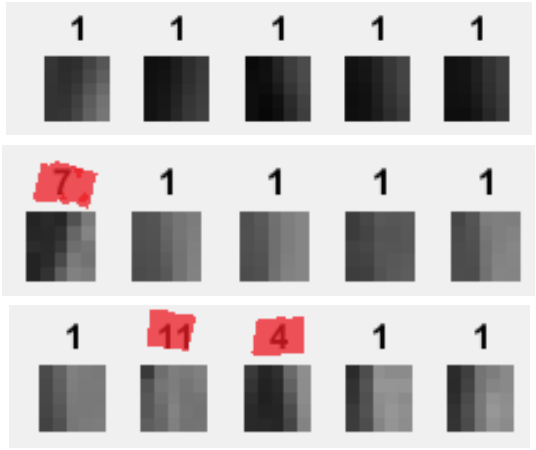


Figure 9. Edge images of category 1 and classification result on the above each image.

4. CONCLUSION

According to previous discussion, deep learning using CNN could be implemented to classify edge images of tertiary dentin image. Using 11 category of edge images, the CNN preliminary testing performed 91% of classification accuracy. The wrong classification occurred due to the similarity of the edge image to another category. Further research should increase the number of epoch and adjusting CNNN parameters. Since the edge images were cropped manually in this research, automatic edge detection using CNN will be an advanced contribution to this area.

5. ACKNOWLEDGMENTS

Authors would like to thank the Universitas Muhammadiyah Yogyakarta for the Multidisciplinary Research Grant 2018 as well as the Oral and Dental Hospital Universitas Muhammadiyah Yogyakarta for providing the x-ray images.

6. REFERENCES

[1] Ministry of Health Republic of Indonesia. 2018. Research Report on Basics' Health.

[2] Sattar, Farook and Karray, Fakhri. 2012. Dental X-Ray Image Segmentation and Object Detection Based on Phase Congruenc', In *Proceedings of the 9th international Conference on Image Analysis and Recognition.*

[3] Lira, Pedro Henrique Marques, et al. 2014. Dental R-Ray Image Segmentation Using Texture Recognition. *IEEE Latin America Transactions* 12 (4), 694-98.

[4] Rad, Abdolvahab Ehsani, et al. 2013. Digital Dental X-Ray Image Segmentation and Feature Extraction. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, 11 (6), 3109-14.

[5] Kaur, Dilpreet and Kaur, Yadwinder. 2014. Various image segmentation techniques: A review. *International Journal of Computer Science and Mobile Computing* 3(5), 809-814.

[6] Kumar, M Jogendra, Kumar, Raj, Reddy, Vijay Kumar. 2014. Review on image segmentation techniques. *International Journal of Scientific Research Engineering and Technology* 3(6), 992-997.

[7] Lee, Lay Khoon, Liew, Siau Chuin. 2015. A review of image segmentation: Methodologies in medical imaging. *Lecture Notes in Electrical Engineering* November 2015.

[8] Shen, W., Wang, X., Wang, Y., Bai, X., Zhang, Z. 2015. DeepContour: A deep convolutional feature learned by positive-sharing loss for contour detection. *Computer Vision and Pattern Recognition* 2015, 3982-3991.

[9] Wang, Rohui. 2016. Edge detection using convolutional neural network. Lecture Notes of Computer Science 9719, 12-20.

[10] El-Sayed, MA, Estaitia, YA, Khafagy, MA. 2013. Automated edge detection using convolutional neural network. *International Journal of Advance Computer Science and Application* 4(10), 11-17.

[11] LeCun, Y., Bengio, Y., & Hinton, G. 2015. *Deep Learning. Nature*, 521 (7533), 436-444.

[12] Zhongyu Li, Xiaofan Zhang, Henning Muller, Shaoting Zhang. Large-scale retrieval for medical image analysis: A comprehensive review. *Medical Image Analysis* 43 (October 2018)

Instance Segmentation of Water Body from Aerial Image using Mask Region-based Convolutional Neural Network

Sangdaow Noppitak
PhD Student, Multi-agent Intelligent Simulation Laboratory, Department of Information Technology, Faculty of Informatics, Mahasarakham University, Thailand
61011261007@msu.ac.th

Sarayut Gonwirat
PhD Student, Multi-agent Intelligent Simulation Laboratory, Department of Information Technology, Faculty of Informatics, Mahasarakham University, Thailand
61011262003@msu.ac.th

Olarik Surinta
Multi-agent Intelligent Simulation Laboratory, Department of Information Technology, Faculty of Informatics, Mahasarakham University, Thailand
Olarik.s@msu.ac.th

ABSTRACT

Land use is constantly changing, and water plays a critical role in the process. If changes are noticed quickly or are predictable, land use planning and policies can be devised to mitigate almost any problem. Accordingly, researchers present a mask region-based convolutional neural network (Mask R-CNN) for water body segmentation from aerial images. The system's Aerial image water resources dataset (AIWR) was tested. The AIWR areas were agricultural and lowland areas that require rainwater for farming. Many wells were spotted throughout the agricultural areas. The AIWR dataset presents two types of data: natural water bodies and artificial water bodies. The two different areas appear as aerial area images that are different in color, shape, size, and similarity. A pre-trained model of Mask R-CNN was used to reduce network learning time. ResNet-101 was used as backbone architecture. The information gathered in the learning process is limited, and only 720 pictures were produced, Researchers used data augmentation to increase the amount of information for training by using affine image transformation, including scale, translation, rotation, and shear. The experiment found that mask R-CNN architecture can specify the position of the water surface. Measuring method in this case is mAP value. The mAP value is at 0.30 without data augmentation. However, if using the R-CNN mask with data augmentation, the mAP value increased to 0.59.

CCS Concepts

• **Computing methodologies → Image segmentation**
• **Computing methodologies → Neural networks.**

Keywords

Instance Segmentation; Water Body; Aerial Image; Mask R-CNN; Transfer Learning.

1. INTRODUCTION

The two terms "land cover" and "land use" are typically used together [12]. Over the past ten years the difference between land cover and land use has attracted many researchers [2] prompted by a change in land cover to accommodate changes in land use. As such, if land use data are accurate and up-to-date, we can apply that information to many objectives, such as city planning, environmental audit or evaluation, and national policy [14].

Elagouz et al. [3] tracked land use in the Nile River, Egypt with RS technology to determine the impact of land changes in urban areas during and after the year 2011. The land changed because of the unplanned expansion of a nearby city. Jazouli et al. [7] said that soil erosion was the most important cause of land degradation throughout the world. Jazouli et al. has predicted the impact of land use changes, which affect soil erosion, in the Oum Er Rbia basin, Morocco. They studied the mountainous areas with steep, slopes, and clay soil where places are higher risk for soil erosion. Soil erosion is sometimes caused by human activities and local weather. Further research would be beneficial for generating land use prediction maps, detecting land use changes, and creating yearly mapping for soil erosion.

Nowadays, deep learning research is very popular, For example, land cover analysis research [13]. The research used deep neural networks for analysis of Landsat 5/7 satellite images to show land cover maps for agriculture, including agriculture areas, water, grass, mixed wood, and border. Kussul et al. [8], used convolutional neural network (CNN), which is the method for classification of recorded images, in remote sensing work. The CNN classified recorded images in category of optical and synthetic aperture radar (SAR) derived from Landsat-8 and Sentinel-1A using CNN type one-dimensional (1-D) and 2-D. The results from CNN were compared with the random forest method and the ensemble neural networks technique. 2D-CNN got the highest score with a 94.6% accuracy rate. However, 2D-CNN still has some problems distinguishing small objects. Spatial resolution of the satellite images is 30 meters, which is low resolution.

Miao et al. [9] presented water body segmentation using restricted receptive field deconvolution network (RRF DeconvNet) for extraction of water body from high-resolution spectrum images. This method did not require infrared spectrum images, and this method also decreased blurring boundaries problem by using a new loss function called edges weighting loss (EWLoss). The researchers tested with the dataset collected from Google Earth. The images from Google earth were in the visible spectrum at 50 meters spatial resolution of the rural area at Suzhou and Wuhan, China. The experiments showed that RRF DeconvNet method using EWLoss had 96.9% accuracy rate.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388184

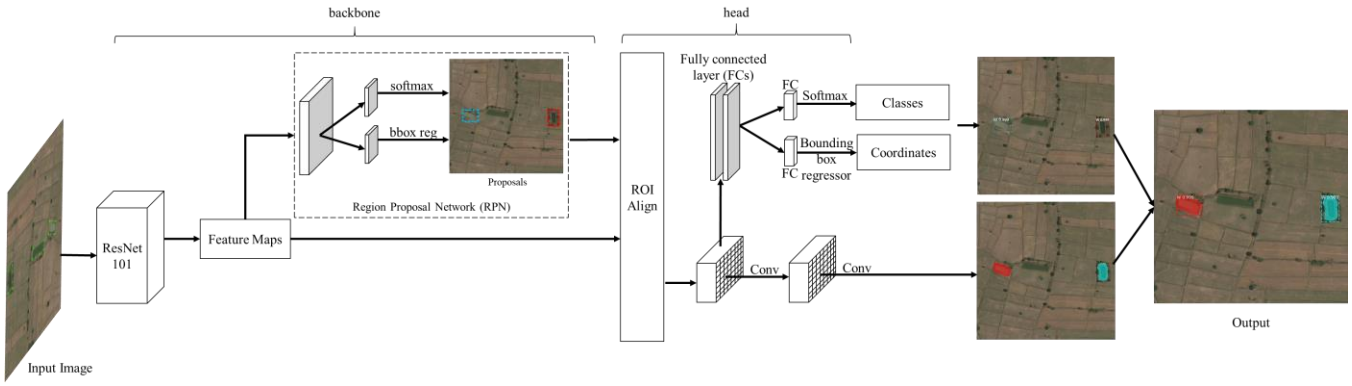


Figure 1. Mask R-CNN Framework.

Wen et al. [15] used Mask R-CNN to segment the building area and the background from Google Earth images. They created a new dataset with 2,000 aerial images in Fujian province, China. The sizes of images used in the experiment range from 1,000x1,000 to 10,000x10,000 pixel. All aerial images were tagged with a label. In the experiment, researcher used pre-trained model of ResNet architecture. All images were resized to 500x500 pixel. The result showed Instance Segmentation using Mask R-CNN resulted in mean Average Precision (mAP) value at 0.9063.

Contribution: this article presents mask region-based convolutional neural network (Mask R-CNN) for water body segmentation from aerial images. This method has been called instance segmentation. ResNet-101 was used as backbone architecture. Mask R-CNN architecture was tested with aerial image water resources dataset (AIWR). The AIWR is the images of agricultural areas in the northeast region of Thailand; these are fertile agricultural areas where people grow rice. The areas require rainwater for farming and many wells can be spotted throughout the agricultural area. Water body data were collected from 2 types, natural water bodies (W1) and artificial water bodies (W2). The aerial images of water bodies were different in color, shape, size, and similarity. This dataset includes 800 images, so AIWR dataset challenges the instance segmentation process.

This research also attempted to add data augmentation in the category of affine image composed of 4 different methods: scale, translation, rotation, and shear. Augmentation processes were used only in the training process. Data augmentation would be a random parameter value. The images, which trained in each epoch using mask in the R-CNN process, were different. The experiments found that data augmentation had improved the performance of Mask R-CNN in the instance segmentation process when used with AIWR Dataset. The result showed better performance for specifying water bodies. The mAP value increases from 0.30 to 0.59 when researcher used data augmentation.

Paper outline: Section 2 explains the Mask R-CNN architecture used for making instance segmentation. Section 3 explains the data collection process of the aerial image water resources (AIWR) Dataset. Experimental results are explained in Section 4. The final section is the conclusion and future work.

a) b)

Figure 2. Result from a) Faster R-CNN method and b) Mask R-CNN.

2. MASK R-CNN ARCHITECTURE

Mask R-CNN was presented by He et al. [6] in 2017 for improving instance segmentation performance. Mask R-CNN was developed from Faster R-CNN, which was presented by Ren et al. [11] in 2015

Faster R-CNN were designed to use a convolutional network (ConvNet) for feature map extraction of Images. ConvNet can use VGGNet and ZFNet architectures. After that, the region proposal network (RPN) was used for inspecting the object areas. RPN operates location inspection for each object. The reason for running RPN was to create a bounding box of each object, which is called ROI pooling layer. In the ROI pooling layer, ROI in each section would be sent to fully connected layers (FCs) for ROI feature vector calculation before sending the value to the softmax function for consideration of ROI as an object. After that, the function will predict the object type in ROI as shown in Figure 1.

According to the introduction, faster R-CNN [11] is an object detector, so this function can't specify an object in pixel-to-pixel, or we would call it instance segmentation as shown in Figure 2a. Mask R-CNN has been designed to help instance segmentation by using the capabilities of RPN to specify ROI. The next step is to segment the ROI areas to specify the edge of an object as shown in Figure 2b.

2.1 Backbone Architecture

Backbone architecture consists of 2 main networks|; ConvNet and RPN. ConvNet used in this research is ResNet-101 architecture, using a pre-trained model derived from learning of COCO dataset. This architecture can reduce network learning time. The main function of ResNet architecture is to extract feature maps from

aerial images, then use the region proposal network (RPN) to find the location of an object using ResNet-101 architecture.

2.2 Head Architecture

An advantage of Mask R-CNN is that it can perform instance segmentation by using the location of any object, derived from RPN, which is another name for the region of interest (ROI). The ROI will be considered whether it is an object or not. If the ROI area is an object, then types of an object would be considered in the next step. This step is similar to Faster R-CNN. After that, areas will be calculated for intersection over union (IoU). Shown in Equation a) The IoU values are assigned to be greater or equal to 0.5.

Any area with an IoU value greater or equal too 0.5 is required to find the perimeter of an image. Sometimes, this method is also known as a segmentation mask. This process is an additional process from Faster R-CNN. In each ROI area, there is only one class. Then, the semantic segmentation model is created. It is as same as binary classification to distinguish an object from background.

3. AERIAL IMAGE WATER RESOURCES DATASET

According to the standard of land use code by fundamental geographic data set: FGDS), Thailand [5] land use classification requires an analysis and transformation of satellite images data together with field survey data. In this article, researchers studied only land use in water bodies. The water bodies in this research can be divided into 2 levels: natural body of water (W1) artificial body of (W2) water.

The deep learning method was used in this research for aerial image data analysis. The aerial images were derived from Bing map by collecting only data in the northeastern region of Thailand. The northeast of Thailand is lowland area mainly used for growing rice, There are also agricultural areas that rely on rainwater for agriculture. As such, there are many ponds in and around the agricultural areas.

The experiments in the study used the Mask R-CNN algorithm which is a suitable method for performing instance segmentation. The model in this experiment can be further developed and applied to water management tasks. Farmers in the northeastern region of Thailand can also create water management plans.

The aerial image data used in this research was 1:50 meters. Every aerial image had 650x650 pixels. Those images included water bodies type W1 and W2 as shown in Figure 3a. Ground truth of all aerial images was set for before sending it to be analyzed and interpreted by remote sensing experts. This assured that the water bodies groupings were correct. An example of ground truth, which has been checked by experts as shown in Figure 3b. Ground truth has been used in learning the algorithm in deep learning mode and also used in further evaluation.

The aerial images used in this experiment consists of water body: types W1 (see, Figure 3, Column 1, 2, and 3) and W2 (see, Figure 3 Column 4). Aerial image water resources dataset, AIWR has 800 images. Data were chosen at random and divided into 3 sections: training, validation, and test set with ratio 8:1:1. Therefore, 640 aerial images were used for learning and creating the model, 80 images were used for validation, and the remaining 80 images were used for test.

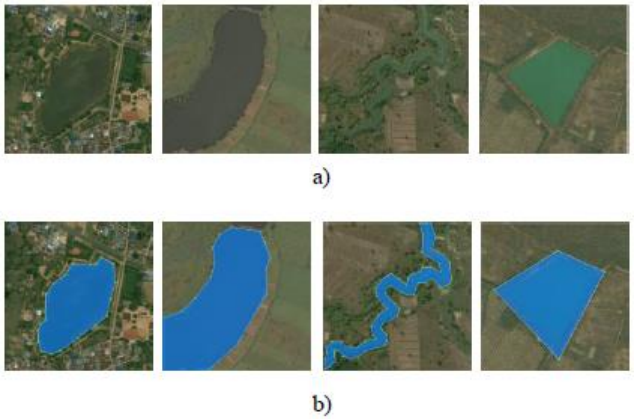


Figure 3. Example of aerial images. a) Water bodies W1 and W2 b) ground truth of water resources.

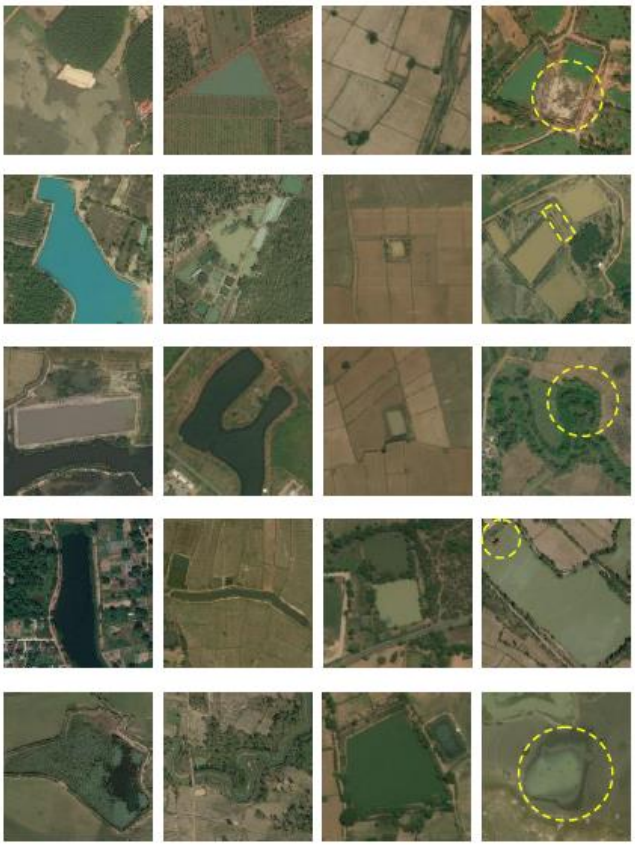
This dataset challenges for instance segmentation process because the water body are W1 and W2 types. There are 4 challenging objectives: color, shape, size, and similarity as follows:

- **Color**: Figure 4a shows that water bodies have different color, for example white, blue, gray and black. Some areas are covered by unwanted flora, so the images are seen as dark green and black.
- **Shape**: The shape of the areas have different characteristics such as triangles, squares, curves, U-shaped and zigzag as shown Figure 4b.
- **Size**: the water body sizes are different. Size measurement in Bing maps found that the water bodies sizes range from 10, 20, 30, 60 and 120 meters as shown in Figure 4c. When researchers observe 10 meter wide water sources, only a small point can be seen.
- **Similarity**: Aerial images of some water bodies are similar to other types of land use, for example flooded areas, water areas that are obscured by trees, or buildings on water areas etc. Figure 4d uses the dotted lines to show areas that have the characteristics as mentioned above

4. EXPERIMENT AND DISCUSSION

A deep learning algorithm was used in this research for instance segmentation. This method can identify the areas in pixel-to-pixel by using Mask R-CNN architecture. The method is suitable for water body segmentation because it can analyze both natural water bodies and artificial water bodies. The data were collected from aerial image data from agricultural areas in the northeastern region of Thailand There was a total of 800 aerial image data. Those images were divided by the 10-fold cross-validation method. There were 720 images for training, and 80 images were used for test. All aerial images were resized to 512x512 pixel.

In this research, TensorFlow platform was used for training and testing the Mask R-CNN algorithm which runs on GPU GeForce GTX 1070 Ti, Intel(R) Core-i5, 7400CPU @ 3.00GHz, 8GB RAM, Linux Operating system. ResNet architecture is backbone architecture for learning aerial imagery learning. This research used transfer learning [1] to reduce learning time of ResNet architecture. Pre-trained model of ResNet-101 architecture, which derived from the learning process of COCO dataset, was also used. Then, researchers used the mentioned model to perform Fine-Tune for adjusting the parameters in order to make it become suitable for the AIWR dataset.



a) b) c) d)

Figure 4. Challenges of instance segmentation of collected data are a) color, b) shape, c) size, and d) similarity.

The parameters used for Fine-tune consist of NUM_CLASSES=2, BATCH_SIZE=4, FPN_CLASSIF_FC_LAYERS_SIZE=512, IMAGES_PER_GPU = 1, IMAGE_MIN_DIM = 512, IMAGE_MAX_DIM = 512, IMAGE_SHAPE=[512, 512, 3], RPN_ANCHOR_SCALES=(8, 16, 32, 64, 128), STEPS_PER_EPOCH=100, TRAIN_ROIS_PER_IMAGE=32, VALIDATION_STEPS=5, and LEARNING_RATE=0.0001

One of the deep learning problems is the amount of training data is too small. A common way to solve the problem is to perform data augmentation, which can be divided into 2 groups including the traditional, white-box method or black-box method. Two common methods for image augmentation in traditional transformations are affine image transformations and color modification [10]

This research used data augmentation, affine image transformations series, which includes scale={"x": (0.8, 1.2), "y": (0.8, 1.2)}, translate_percent={"x": (-0.2, 0.2), "y": (-0.2, 0.2)}, rotate=(-25, 25), and shear=(-8, 8). An example of aerial images obtained after data augmentation are shown in Figure 5.

4.1 Model Evaluation

To Evaluation Mask R-CNN algorithm, researchers used mean average precision (mAP) [4] ,which is a method for evaluating the effectiveness of image retrieval by an intersection over union (IoU) calculation from the following equation.

Figure 5. Examples of data augmentation.

$$IoU = \frac{area(B_p \cap B_{gt})}{area(B_p \cup B_{gt})} \quad (1)$$

where $B_p \cap B_{gt}$ are the areas of intersection between the predicted area. Ground truth (gt) is bounding boxes and $B_p \cup B_{gt}$ is the area of union, determined by the value of $IoU \geq 0.5$

After that, true positive (TP), a correct detection, and false positive (FP) (A wrong detection) were calculated. The detection were performed by $values \geq 0.5$, false negative (FN) (A ground truth not detected) and true negative (TN) (corrected misdetection). The TP, FP, FN, TN value are taken to calculate precision (P) and Recall (R) value.

AP value was considered by average of maximum precision at a set of 11-spaced recall levels . The equation is as follows:

$$AP = \frac{1}{11} \sum_{r \in \{0, 0.1, .., 1\}} P_{inter\,p}(r) \quad (2)$$

with $P_{inter\,p}(r) = \max_{\tilde{r}.\tilde{r} \geq r} p(\tilde{r})$

where $p(\tilde{r})$ is the measured precision at recall $\tilde{r}$
After that, mAP value are calculated as the following equation.

$$m\text{AP} = \frac{1}{N} \sum_{i=1}^{N} \text{AP}_\text{i} \quad (3)$$

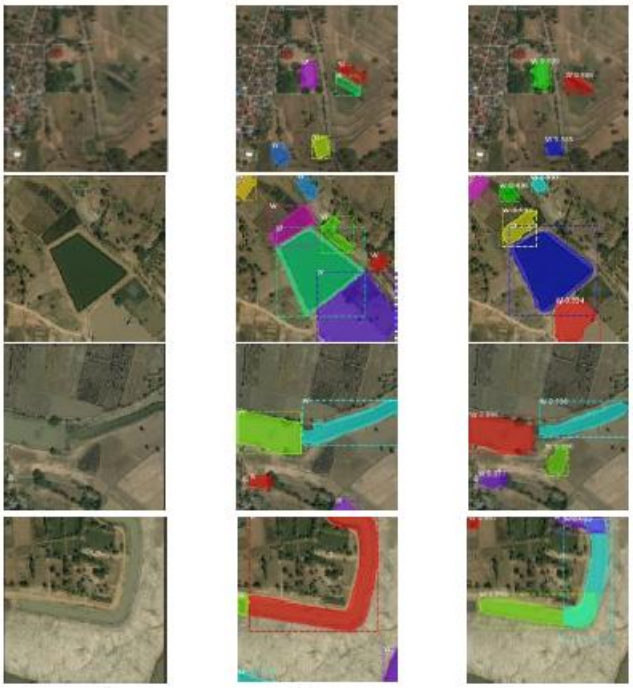
where N is number of query

4.2 Result of Instance Segmentation of Water Body

Table 1 is the result of the experiment of mask R-CNN architecture to segment water bodies from the AIWR dataset. Augmentation data experiments of AIWR dataset were performed by affine image transformations method, including scale, translation, rotation, and shear. The result shows that the loss error value from training processes was up to 1.08. That result in the mAP was as low as 0.30, but when researchers tested again using data augmentation, the loss errors were reduced to only 0.41 and the mAP increased to 0.59, which is almost 2 times higher. However, the data augmentation process takes 12 day and 9 hours to learn.

Table 1. The result of the experiment using mask R-CNN with the AIWR Dataset

Augment	Validation loss	mAP	Training Time	Test Time /img
False	1.08	0.30	11d 15h 16min 27s	3 µs
True	0.41	0.59	12d 9h 48min 25s	4 µs



a) b) c)

Figure 6. Result of instance segmentation using mask R-CNN with data augmentation. a) Aerial images b) images with ground truth, and c) instance segmentation.

a) b) c)

Figure 7. Error results in segmentation. a) Aerial images b) images with ground truth and c) error of instance segmentation.

Figure 6 included the data augmentation method in data training in order to create a model. The result shows that data augmentation in data training leads to a better result of segmentation. Figure 7 demonstrates errors from instance segmentation. It is because Figure 7c (Row 1) cannot segment the river areas covered with trees, and Figure 7c (Row 2) is the area covered by unwanted flora.

5. CONCLUSION

In this paper evaluated the accuracy of instance segmentation by Mask R-CNN together with data augmentation. The mAP values were used as the measuring method. This research tested with aerial images of water resources dataset (AIWR). The areas are the lowlands which require rainwater for farming. The challenges of AIWR dataset the collection of 2 types of water bodies: natural water bodies and artificial water bodies. The two types of data are different in color, shape, size, and similarity. This paper used a pre-trained model to reduce learning time of the Mask R-CNN. This research has shown that the mask R-CNN architecture combined with data augmentation can identify the water surface using the mAP value for measurement. The value was up to 0.59. It is almost two times greater than not using data augmentation method.

In future work, because the data tested is aerial photography obtained from Bing map, only RGB colors can be evaluated. If other research can use data from satellites, such as Landsat, which has a band specifically for water analysis, the result of an analysis of water bodies with different color might give higher accuracy. Any new architecture suitable for water body analysis might be used to expect an even higher accuracy rate.

6. REFERENCES

[1] Bunrit, S., Nittaya, K. and Kerdprasop, K. 2019. Evaluating on the Transfer Learning of CNN Architectures to a Construction Material Image Classification Task. *International Journal of Machine Learning and Computing*. 9, 2 (2019), 201–207.

[2] Caldas, M.M., Goodin, D., Sherwood, S., Campos Krauer, J.M. and Wisely, S.M. 2015. Land-cover change in the Paraguayan Chaco: 2000–2011. *Journal of Land Use Science*. 10, 1 (Jan. 2015), 1–18.

[3] Elagouz, M.H., Abou-Shleel, S.M., Belal, A.A. and El-Mohandes, M.A.O. 2019. Detection of land use/cover change in Egyptian Nile Delta using remote sensing. *Egyptian Journal of Remote Sensing and Space Science*. (Jan. 2019), 0–5.

[4] Everingham, M., Gool, L. Van, Williams, C.K.I., Winn, J. and Zisserman, A. 2010. The Pascal Visual Object Classes (VOC) Challenge. International Journal of Computer Vision. 88, 2 (2010), 303–338.

[5] GISTDA 2013. *Fundamental Geographic Data Set (FGDS)*.

[6] He, K., Gkioxari, G., Dollár, P. and Girshick, R. 2017. Mask R-CNN. In *Proceedings of the 2017 IEEE International Conference on Computer Vision (ICCV)* (Venice, Italy, Oct 22-29, 2017), 2961–2969.

[7] Jazouli, A. El, Barakat, A., Khellouk, R., Rais, J. and Baghdadi, M. El 2019. Remote sensing and GIS techniques for prediction of land use land cover change effects on soil erosion in the high basin of the Oum Er Rbia River (Morocco). *Remote Sensing Applications: Society and Environment*. 13, (Jan. 2019), 361–374.

[8] Kussul, N., Lavreniuk, M., Skakun, S. and Shelestov, A. 2017. Deep Learning Classification of Land Cover and Crop Types Using Remote Sensing Data. *IEEE Geoscience and Remote Sensing Letters*. 14, 5 (May 2017), 778–782.

[9] Miao, Z., Fu, K., Sun, H., Sun, X. and Yan, M. 2018. Automatic Water-Body Segmentation from High-Resolution Satellite Images via Deep Networks. *IEEE Geoscience and Remote Sensing Letters*. 15, 4 (2018), 602–606.

[10] Mikołajczyk, A. and Grochowski, M. 2018. Data augmentation for improving deep learning in image classification problem. In *Proceedings of the International Interdisciplinary PhD Workshop (IIPhDW)* (swinoujście, Poland, May 09 - 12, 2018), 117–122.

[11] Ren, S., He, K., Girshick, R. and Sun, J. 2017. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal

Networks. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 39, 6 (2017), 1137–1149.

[12] Rujoiu-Mare, M.-R. and Mihai, B.-A. 2016. Mapping Land Cover Using Remote Sensing Data and GIS Techniques: A Case Study of Prahova Subcarpathians. *Procedia Environmental Sciences*. 32, (2016), 244–255.

[13] Storie, C.D. and Henry, C.J. 2018. Deep learning neural networks for land use land cover mapping. In *Proceedings of the International Geoscience and Remote Sensing Symposium (IGARSS)* (Valencia, Spain, July 22-27, 2018), 3445–3448.

[14] Treitz, P. and Rogan, J. 2004. Remote sensing for mapping and monitoring land-cover and land-use change-an introduction. *Progress in Planning*. 61, 4 (2004), 269–279.

[15] Wen, Q., Jiang, K., Wang, W., Liu, Q., Guo, Q., Li, L. and Wang, P. 2019. Automatic Building Extraction from Google Earth Images under Complex Backgrounds Based on Deep Instance Segmentation Network. *Sensors*. 19, 2 (Jan. 2019), 333.

Road Detection for Reinforcement Learning Based Autonomous Car

Martin Holen
Centre for Artificial Intelligence Research, University of Agder
4604 Kristiansand, Norway
+4737233182
Martin.holen@uia.no

Rupsa Saha
Centre for Artificial Intelligence Research, University of Agder
4604 Kristiansand, Norway
Rupsa.saha@uia.no

Morten Goodwin
Centre for Artificial Intelligence Research, University of Agder
4604 Kristiansand, Norway
Morten.goodwin@uia.no

Christian W. Omlin
Centre for Artificial Intelligence Research, University of Agder
4604 Kristiansand, Norway
Christian.omlin@uia.no

Knut Eivind Sandsmark
Sopra Steria
Biskop Gunnerus' gate 14A
0185 Oslo, Norway
knut@sandsmark.net

ABSTRACT

Human mistakes in traffic often have terrible consequences. The long-awaited introduction of self-driving vehicles may solve many of the problems with traffic, but much research is still needed before cars are fully autonomous.

In this paper, we propose a new Road Detection algorithm using online supervised learning based on a Neural Network architecture. This algorithm is designed to support a Reinforcement Learning algorithm (for example, the standard Proximal Policy Optimization or PPO) by detecting when the car is in an adverse condition. Specifically, the PPO gets a penalty whenever the virtual automobile gets stuck or drives off the road with any of its four wheels.

Initial experiments show significantly improved results for PPO when using our Road Detection algorithm, as compared to not using any form of Road Detection.

In fact, without this detection algorithm, the vehicle often gets into non-terminating loops (for example, driving into the dividers, getting stuck, or driving into a pit).

CCS Concepts

•Computing methodologies→Supervised learning •Computing methodologies→Reinforcement learning •Computing methodologies→Continuous simulation •Computing methodologies→Distributed simulation.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388199

Keywords

Reinforcement learning; neural networks; road detection; simulation.

1. INTRODUCTION

Every year nearly 1.25 million people die in traffic, much of it caused by human error. A potential solution to this high death rate is self-driving vehicles, as computers do not suffer from the same drawbacks as human drivers, for example, causing fatal mistakes when tired [22].

Self-driving algorithms are, to some extent, part of modern cars, and data from companies such as Tesla show examples of self-driving cars are already safer than human drivers [18].

These self-driving vehicles are mostly trained using human drivers' data. A notable limitation of this approach is the repetition of human mistakes. One way of counteracting the weakness is through Reinforcement Learning.

Reinforcement Learning (RL) in self-driving cars do not learn using data previously collected from human drivers. Instead, RL algorithms explore and reinforce correct actions and penalize wrong ones (for example, driving off the road).

Much research is still needed. In fact, seemingly straight forward problems, such as proper lane detection, is not in place. Further, there is no common understanding of which learning functions to use in any given environment — in conclusion, enabling self-driving in cars if far from a resolved research problem.

Partly autonomous cars, which is a step towards self-driving vehicles, are already an industry standard and affordable for many people. Such cars are available for approximately 45,000 USD which makes them affordable for a relatively large group of people. And given that auto companies now offer vehicles that can perform multiple complex actions such as lane changing to overtake another car, adaptive cruise control, collision avoidance, collision detection, and more, improvements on these systems are even more important [17].

A predefined rule-based system or machine learning-based classification is the basis for most autonomous driving available in the literature. Machine learning-based driving is challenging for

companies that do not have hundreds of thousands of cars collecting data. Further, since privacy concerns have become more and more critical in recent years, there is an added difficulty in data collection. Moreover, data of human driving is imperfect as many collisions happen due to human error [22].

Reinforcement Learning (RL) is a machine learning sub-field that has received a lot of focus recently. Perhaps the most notable examples are AlphaGo beating the world's best Go player, and AlphaZero beating the best chess AI's [15] [1]. The basic principle of this approach is to arrive at a set of appropriate actions via rewards or penalties associated with learned actions.

RL is also used for self-driving cars. Here, instead of training on data from human drivers, the RL algorithm typically learns to drive in a simulated environment. In simulations, wrong actions have little consequence. Once the learning is proficient, transfer learning is used to train in a physical environment. The combination of simulation and transfer learning speeds up the training process compared to training only in a physical environment [2].

This paper focuses on a small but crucial sub-problem in the RL self-driving scenario -- namely lane detection. We introduce a Road Detection algorithm to support an RL-based self-driving algorithm (for example, the Proximal Policy Optimization or PPO), by informing the RL algorithm when the car is going off the road in multiple different environments.

2. BACKGROUND

In recent years, autonomous vehicles have been the object of a lot of research across industry and academia.

One common approach is to have an RL based self-driving car that uses human interaction as part of the reward function [2]. The setup is so that whenever the vehicle drives off the road, a human trainer stops the car, which the reward function interprets as a penalty. This penalty is, in turn, used to correct the vehicle's actions in the algorithm. Not surprisingly, the training process becomes quite expensive and time-consuming -- a human always has to be in the car. Another challenge is that human drivers become tired, which could lead to slow corrections, thereby affecting the efficacy of the reward and penalty system. As a consequence, the system could learn incorrect or unsafe actions that may cause accidents and injuries.

Before the rise of deep learning, most methods for creating self-driving cars were based on using sensor data and manually creating rulesets for driving behavior. These systems employed various strategies, such as k-means clustering, Dijkstra, perspective transformation. The general actions performed here were mapping, planning, and control, and getting the data from sensors and estimating the state of the car. Many of these methods used computer vision. Cameras or LIDARs were used to get an image of the surrounding area so that the system was able to map it. The process depended mainly on the task which the researchers focused on, such as Road Detection in different lighting conditions using vanishing point detection or Road Detection for rural areas. Such systems, not surprisingly, worked well in those specific conditions but could struggle in a more generalized environment [15] [1] [12].

In recent years, there has been a broader focus on creating supervised image recognition models whose objective was to imitate the driving of humans. Resulting in not only larger more accurate models, but also computationally effective ones [1]. These supervised models, learn by getting an input predicting an output. This output is checked versus a label, resulting in a difference between the prediction and the label. The model then optimizes to get closer to the labels for any input it is given. The models created to do so have become extremely good at these tasks, even surpassing humans in some of them [6] [16].

Supervised systems work quite well in general, but vital issues remain. Mainly, it is challenging to gather a large enough amount of training data collected by experts. A mitigating is the approach carried out by Tesla: every time the driver takes control, it is assumed that the cars' prediction was incorrect. The drawback to this, again, is if the drivers' actions are less than ideal, the vehicle will be trained to drive in that specific manner. Nvidia has also created a simple yet effective imitation based model, based on the earliest Neural Network autonomous vehicle implementation (ALVINN) [5]. The Nvidia self-driving car worked reasonably well, though the model needs to be shown many different scenarios to be able to perform the correct actions, which does not scale well [20] [14].

Reinforcement Learning takes an input (s), performs an action (a), and gets a reward (r). A common environment for RL is a Markov decision process (MDP). An MDP contains a state s, and action a, a probability transition p, and gives a reward r for the action which leads to the state s+1. Given the MDP, the RL algorithm can predict the best action to take.

A common approach is to estimate the reward of each action is Deep-Q networks (DQN). Of which notable examples are [3] [19]. For Fayje et. al. the task was to create an autonomous robot which learned to navigate using a Deep-Q network (DQN), whose inputs were a camera and a LIDAR [3]. While Okuyama, Gonsalves et. al. focused on creating a simulation in which the task was to avoid obstacles, this task was solved using a DQN [19]. The estimation of a reward is essential to a DQN along with the verification of the discounted reward, which is collected after performing any action. The discounted reward is a way of saying that all the actions which lead up to a reward were important, ensuring that the network rewards the action completing a goal (for example, a lap in a racing game) but also the other action [21].

Another RL method, also used for self-driving cars, is that of policy gradients, in which the policy predicts which action is the best through an actor. The policy is then later updated based on how good that action was, which is determined by a critic. Promising examples of policy gradients include Proximal Policy Optimization (PPO) and Trust Region Policy Optimization (TRPO), of which PPO is said to be "much simpler to implement, more general, and have better sample complexity (empirically)." [13] [9] [4].

The way all of these methods work is by performing what are random actions at the beginning, then updating the reward for the set of actions the RL algorithm performed. Eventually, the system will learn which actions are beneficial, and in turn, become more and more confident in its operations, making the activities less and less random.

3. APPROACH

A notable drawback of the previously discussed methods is the difficulty in scaling up such systems. The apparent consequence of this is that cars would likely get damaged often in the beginning, and it would be unsafe for humans to stay near the car. Hence, there is a need for a reliable method to detect whether the vehicle is on the road. Through RL, any off-road vehicle should

yield a penalty. This would result in a so-called Road Detection algorithm. An algorithm that detects when the car is off the road, other parts of the system can perform actions to get it back onto the road.

There is also the issue of time, as a car is only able to perform up to 10's of actions every second. An improvement of the training speed could be achieved by training in simulations until the car has become proficient enough to be transferred into a real-world scenario. We use transfer learning to move knowledge from one environment into another one.

In our approach, the Road Detection algorithm will be running alongside the Reinforcement learning algorithm (see Figure 3. A challenge with this approach is the size and computational complexity of the Road Detection algorithm. An algorithm that slows down the RL algorithm would impact how quickly the car can react. It is, therefore, necessary for the Road Detection algorithm to be efficient in terms of both memory and computational power [11]. Referring to Cui et al. the choice of the Road Detection algorithm is between algorithms made for mobile devices, the quickest of these is MobileNet [1]. MobileNet which was introduced by Howard et. al. in 2017, is a Neural Network made to be faster and is usable for mobile devices such as phones. MobileNet uses depth-wise separable convolutions, which reduces the number of variables in the convolutions, as well as the size. It also has two hyperparameters, which have trade-offs between latency and accuracy. These hyperparameters are a width multiplier, which can make the model thinner or thicker as well as a resolution multiplier, which can reduce the representation. The balance of these can be used to create either a faster algorithm or a more accurate (but slower) model. The hyperparameter choice is vital as a loss in accuracy could impact the usefulness of the Road Detection algorithm [1].

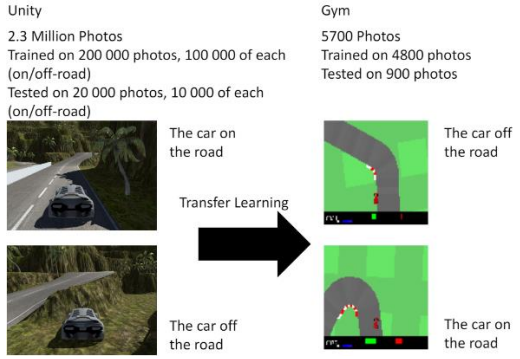


Figure 1. Information about the different environments, and how they are trained. With the Unity photos shown, being a screenshot instead of the image sent to the agent.

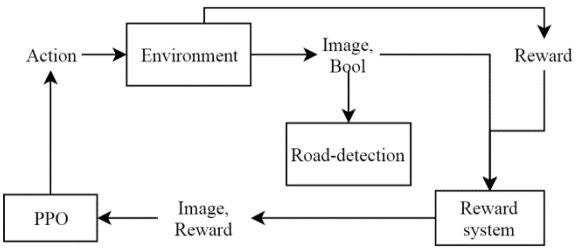


Figure 2. An overview of how the system works during training given the Unity environment.

For training and experimenting with our proposed Road Detection algorithm, we use an RL-based self-driving car in simulated environments. Using Proximal Policy Optimization (PPO) for driving avoids extensive policy updates. The PPO predicts where the vehicle should drive.

Secondly, the Road Detection algorithm is MobileNet, a convolutional neural network that gives feedback to the PPO whenever the car is off the road. MobileNet is quite fast, with only a small impact on the accuracy [1].

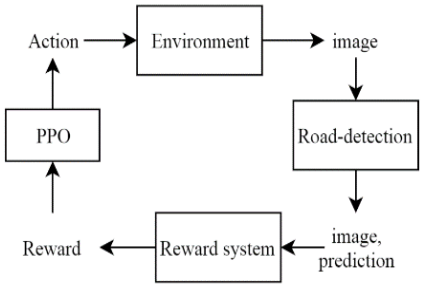


Figure 3. An overview of how the testing system works when the Road Detection algorithm is trained, and used to train the PPO.

4. ENVIRONMENTS

Training and testing of the Road Detection algorithm was done with two separate environments: A Unity environment created by Udacity, as well as carracing-v0 from OpenAI's gym. Using different environments means that there is a need to be able to use the same setup for each environment. We achieve this by calculating the reward outside of the Unity environment.

The Udacity environment is a 3D racing game with twists and turns, as well as hills and bridges. When one acts in the environment it feeds both the image and a Boolean value indicating if the car is off the road. The boolean is sent to a reward function, which in turn sends the image and the reward function onward to the PPO and the Road Detection algorithms. This duality enables training of both algorithms simultaneously, which can be seen in figure 3. The images given from the unity environment is not in the standard RGB format, resulting in the images it sends looking a bit different than the gym images, for reference look at figure 1. Both of the images from figure 1, are photos given by the environment and saved to png format directly.

Figure 4. Shows the images given from each environment, during the training and testing phase.

The Gym environment is a 2D racing game, with some turns. When interacting with this environment it gives the state in the form of an image, along with a reward, and a boolean which says whether the episode is done or not. The RL algorithm interacts with the environment simply by saying environment step(action), which applies the action to the environment and sends back the aforementioned variables.

During the testing of the algorithm, a similar process is carried out. The environment also sends the image to the Road Detection algorithm, which again is forwarded to the reward function along with the Boolean on-or-off road value. All of this is delivered to the PPO, which uses the information to collect a reward for its driving.

Overall these environments are quite different, as the Udacity environment is a rather complex 3D racing game, while the Gym environment is a rather simple 2D racing game. For reference refer to figure below. The images from figure below were captured using screenshots, resulting in the Unity images colors looking normal compared to figure 1.

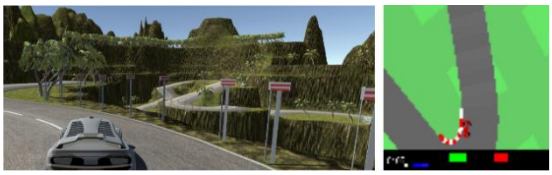


Figure 5. Shows the complexity of each simulation.

5. RESULTS

The Road Detection algorithm needed to be tested for two different goals, to verify that its accuracy was high enough to be used in the reward system, as well as verifying how much it improved the self-driving algorithm.

For both the test of the accuracy and the improvement in the PPO's actions, there were two environments; namely Udacities Unity environment, as well as OpenAIs gym environment carracing-v0. This provided evidence that the Road Detection algorithm was suitable for multiple different environments of various complexities.

Table 1. The testing accuracies for the two different environments (Unity and Gym), RD is the Road Detection algorithm, and the arrow represents transfer learning (from x ➔ y). The K-means was both trained and tested in the environment corresponding to that column

Train\Test	Unity	Gym
RD Unity	98.26	51.48
RD Gym	43.05	96.70
RD Unity ➔ Gym	49.69	97.98
RD Gym ➔ Unity	99.41	54.09
K-Means	93.15	57.05

Table 1 presents the accuracy for applying the method in the Unity and Gym environment. The accuracies listed in table 1, lists the testing accuracy where the row shows where the algorithm was trained, while the columns show the environment the algorithm was tested in. The K-means algorithm was trained and tested on the same environment, as a baseline test. The table shows, not surprisingly, that training in one environment (for example, Unity) and validating in another (for example, Gym) yields a lower accuracy than training and testing in the same environment. Further, by using transfer learning by training in one environment, and continue training in another, this gives even better results. When we train and validate in Gym alone the model gives an accuracy of 96.70, but transfer learning from Unity to Gym increases the accuracy to 97.98. This is likely due to the weights from training in the Unity environment being a better starting point than the initial weights given by simply initiating the model.

When looking at the accuracy for the Unity environment given that the model is trained in the gym environment, the accuracy is rather low at 43.05% accuracy. This is likely due to the color scheme from the Unity environment being quite different from the standard RGB format given in the Gym environment, resulting in the model not functioning correctly, as the weights will only be tuned for the one environment. To see how the Unity environments images look, refer to figure 1.

If the PPO algorithm does better when it uses the Road Detection algorithm, this means that the Road Detection improves training. The validity was verified in the modified Unity environment, which had checkpoints in it, these checkpoints represented how far the car drove.

Table 2. The performance of the PPO in the Unity simulation, with and without the use of the Road Detection algorithm during training

PPO with Road Detection	4.8 Checkpoints
PPO without Road Detection	3.6 Checkpoints

Table 2 shows the average number of checkpoints the PPO was able to drive past, with and without the Road Detection algorithm when training. This shows how the PPO is able to drive further when using a Road Detection algorithm, than when not using one. Showing that the Road Detection is an improvement to the PPO during training. The checkpoints have a distance of approximately 5 units each, meaning that 5 checkpoints is approximately 25 distance units. This means that an increase in the number of checkpoints, means an increase in the distance travelled by the autonomous car.

6. CONCLUSION

In this paper we create a novel system which gives an automatic feedback, using a state of the art Road Detection algorithm. This feedback system automates the penalty for driving off the road, for a Reinforcement Learning algorithm which can be used in different environments. Allowing for the training of autonomous vehicles in different environments without the need to modify the environments. In turn resulting in less work when training the RL algorithms, while speeding up the training process.

7. REFERENCES

[1] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto and H. Adam, "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications," CoRR, vol. abs/1704.04861, 2017.

[2] A. Kendall, J. Hawke, D. Janz, P. Mazur, D. Reda, J.-M. Allen, V.-D. Lam, A. Bewley and A. Shah, "Learning to Drive in a Day," CoRR, vol. abs/1807.00412, 2018.

[3] A. R. Fayjie, S. Hossain, D. Oualid and D. Lee, "Driverless Car: Autonomous Driving Using Deep Reinforcement Learning in Urban Environment," in 2018 15th International Conference on Ubiquitous Robots (UR), 2018.

[4] D. A. Lazar, E. Bıyık, D. Sadigh and R. Pedarsani, Learning How to Dynamically Route Autonomous Vehicles on Shared Roads, 2019.

[5] D. A. Pomerleau, "ALVINN: An Autonomous Land Vehicle in a Neural Network," in Advances in Neural Information

Processing Systems 1, D. S. Touretzky, Ed., Morgan-Kaufmann, 1989, pp. 305-313.

[6] D. C. Ciresan, U. Meier and J. Schmidhuber, "Multi-column Deep Neural Networks for Image Classification," CoRR, vol. abs/1202.2745, 2012.

[7] D. Silver, T. Hubert, J. Schrittwieser, I. Antonoglou, M. Lai, A. Guez, M. Lanctot, L. Sifre, D. Kumaran, T. Graepel, T. Lillicrap, K. Simonyan and D. Hassabis, "A general reinforcement learning algorithm that masters chess, shogi, and Go through self-play," Science, vol. 362, pp. 1140-1144, 2018.

[8] D. Silver, T. Hubert, J. Schrittwieser, I. Antonoglou, M. Lai, A. Guez, M. Lanctot, L. Sifre, D. Kumaran, T. Graepel, T. P. Lillicrap, K. Simonyan and D. Hassabis, "Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm," CoRR, vol. abs/1712.01815, 2017.

[9] E. Vinitsky, A. Kreidieh, L. L. Flem, N. Kheterpal, K. Jang, C. Wu, F. Wu, R. Liaw, E. Liang and A. M. Bayen, "Benchmarks for reinforcement learning in mixed-autonomy traffic," in Proceedings of The 2nd Conference on Robot Learning, 2018.

[10] H. Dahlkamp, A. Kaehler, D. Stavens, S. Thrun and G. R. Bradski, "Self-supervised monocular road detection in desert terrain.," in Robotics: science and systems, 2006.

[11] J. Cui, P. Chen, R. Li, S. Liu, X. Shen and J. Jia, "Fast and Practical Neural Architecture Search," in The IEEE International Conference on Computer Vision (ICCV), 2019.

[12] J. M. Álvarez, T. Gevers and A. M. López, "Road Detection by One-Class Color Classification: Dataset and Experiments," CoRR, vol. abs/1412.3506, 2014.

[13] J. Schulman, F. Wolski, P. Dhariwal, A. Radford and O. Klimov, "Proximal Policy Optimization Algorithms," CoRR, vol. abs/1707.06347, 2017.

[14] M. Bojarski, D. D. Testa, D. Dworakowski, B. Firner, B. Flepp, P. Goyal, L. D. Jackel, M. Monfort, U. Muller, J. Zhang, X. Zhang, J. Zhao and K. Zieba, "End to End Learning for Self-Driving Cars," CoRR, vol. abs/1604.07316, 2016.

[15] O. Miksik, "Rapid vanishing point estimation for general road detection," in 2012 IEEE International Conference on Robotics and Automation, 2012.

[16] T. Ho-Phuoc, "CIFAR10 to Compare Visual Recognition Performance between Deep Neural Networks and Humans," CoRR, vol. abs/1811.07270, 2018.

[17] T. Inc, "Introducing navigate on autopilot," 2018. [Online]. Available: https://www.tesla.com/no_NO/blog/introducing-navigate-autopilot?redirect=no.

[18] T. Inc, "Tesla Vehicle Safety Report," 2019. [Online]. Available: https://www.tesla.com/no_NO/VehicleSafetyReport?redirect=no.

[19] T. Okuyama, T. Gonsalves and J. Upadhay, "Autonomous Driving System based on Deep Q Learnig," in 2018 International Conference on Intelligent Autonomous Systems (ICoIAS), 2018.

[20] T. Xiao, T. Xia, Y. Yang, C. Huang and X. Wang, "Learning From Massive Noisy Labeled Data for Image Classification," in The IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015.

[21] V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra and M. A. Riedmiller, "Playing Atari with Deep Reinforcement Learning," CoRR, vol. abs/1312.5602, 2013.

[22] W. H. Organization, "Global status report on road safety 2018," 2018. [Online]. Available: https://www.who.int/violence_injury_prevention/road_safety_status/2018/en/.

Plant Leaf Image Recognition using Multiple-grid Based Local Descriptor and Dimensionality Reduction Approach

Thipwimon Chompookham
PhD Student, Department of Information Technology
Faculty of Informatics,
Mahasarakham University, Thailand
61011261002@msu.ac.th

Sarayuth Gonwirat
PhD Student, Department of Information Technology
Faculty of Informatics,
Mahasarakham University, Thailand
61011261003@msu.ac.th

Siriwiwat Lata
PhD Student, Department of Information Technology
Faculty of Informatics,
Mahasarakham University, Thailand
61011261004@msu.ac.th

Sirawan Phiphiphatphaisit
PhD Student, Department of Information Technology,
Faculty of Informatics, Mahasarakham University,
Thailand
61011261005@msu.ac.th

Olarik Surinta
Multi-agent Intelligent Simulation Laboratory (MISL),
Faculty of Informatics, Mahasarakham University
Maha Sarakham, Thailand
olarik.s@msu.ac.th

ABSTRACT

The identification process of plant species is one of the significant and challenging problems. In this research area, many researchers have focused on identifying the plant leaf images because the leaves of a plant are found almost all year round. The achieve method of the plant leaf image recognition is based on unique extraction features from the plant leaf and using the well-known machine learnings as a classification method. As a result, recognition accuracy was often not very high. In order to improve recognition accuracy, we proposed a multiple grids technique based on the local descriptors and dimensionality reduction. Firstly, we divided the plant leaf image according to grid size and calculated the local descriptors from each grid. Secondly, the dimensionality reduction is proposed to transform and decrease the correlated variables of the feature vector. Finally, the feature vector with a relatively low-dimensional is transferred to the machine learning techniques, which are the support vector machine and multi-layer perceptron algorithms. We have evaluated and compared the proposed algorithm with the bag of visual words method and the deep convolutional neural network (including AlexNet and GoogLeNet architectures) on the Folio leaf image dataset. The experiments show that the proposed algorithm has improved and obtained very high accuracy on plant leaf image recognition.

CCS Concepts

• Computing methodologies→Object recognition • Computing methodologies→Support vector machines • Computing methodologies→Neural networks.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388180

Keywords

Plant leaf recognition; Multiple grids approach; Local descriptor; Dimensionality reduction; Support vector machine; Multi-layer perceptron.

1. INTRODUCTION

Plants are living things that relate directly to humans in that they are used as a food and medicine. Botanists have collected and studied various plant species which can be of some benefit for humans. However, while the physical characteristics of some plants are similar, they have different benefits and toxins. As such, the ability to distinguish the types of plants requires an advanced knowledge of botany. A typical plant classification problem is the diversity of plants and their botanical characteristics. Researchers find that classification of plant species is a challenging problem. Nowadays, computer vision and machine learning are used as instruments for recognition and classification.

This research aims to use image processing and machine learning for plant classification by classifying plant leaf photos taken from the laboratory.

Wäldchen and Mäder [1] said that over the past 10 years, researchers have tried to bring various parts of the plant including leaves, plant blossom and fruits [2, 3, 4] to study plant classification. Most researchers are interested in the leaves because the plant leaves have specific shape, surface shape, color, and leaf structure [5, 6]. The images of plant leaves used in this research are divided into two forms including 1) Plant leaf taken in an outside environment [7] and 2) Plant leaf taken in a laboratory on a white background [8-10].

In [11], used curvature-scale space for recognizing margin shape (Margin shape recognition) and Leaf identification from the characteristics of plant leaves by Semi-supervised fuzzy C means (FCM) for training the margin shape with 12 terms. Then, it learns with the Pl@ntLeaves database, which is divided into three subsets including Scan, Pseudoscan, and Photograph by using Top-K in the test. The result found that the given K=10 in dataset Scan, Pseudosca, and Photograph, accuracy rates were estimated as 95%, 92%, and 80%, respectively.

Image data of plant leaves taken in the laboratory is presented by Munisami et al. [8] The Folio dataset is a dataset which contains 32 species of plant images. The research suggested the methods to find feature extraction technique including plant shape and color histogram, then used it to classify the plant leaves. The result was an accuracy rate of 87.3%

In [10], have tested the Folio dataset by using deep convolutional neural networks (CNNs) which includes architecture types AlexNet architecture and GoogleNet architecture. Another method was classical local descriptors which include a histogram of oriented gradients (HOG) and bags of visual words (BOW). The support vector machine (SVM), multi-layer perceptron (MLP), and K-nearest neighbor (KNN) were used as instruments for classification of plant leaves images. In the experiments, databases were divided into two parts: 80% dataset for training and 20% of dataset for testing. The result showed that AlexNet Architecture type fine-tuned was the most accurate method, with a 97.67% accuracy rate. Moreover, in the research [9] they used 6 methods of data augmentation. The methods were rotation, blur, contrast, scaling, illumination, and projective transformation. These methods can add up to 25 times the number of datasets for training. Researchers increased the number of images to 11,125 images and tested by using AlexNet architecture. The result could be summarized as increasing dataset contrast methods, which can increase the accuracy rate to 99.04%. When tested with the GoogleNet architecture, it was found that the illumination method had the highest accuracy rate at 99.42%.

Another set of plant leaves images taken in the laboratory was the Flavia dataset presented by [12]. There are 32 species of plant images. The characteristics of the shape feature of the plant leaves were studied before being classified by the SVM method. The accuracy rate was 85%. At the same time, the research [13] developed an automatic leaf classification system by using feature extraction types colored SIFT in cooperation with SVM. In [14] used geometrical and shape feature in cooperation with SVM. The accuracy rates from the test were 98% and 97.69% respectively. In the case of leaf classification by MLP, the research [15] used feature extraction types texture-based with constraint. MLP method must have an input layer, hidden layer, and output layer as 44, 30, and 31 nodes respectively. The accuracy rate of the test was 87.1%.

Contributions: The research focuses on the importance of plant leaf recognition by experiment with (Folio dataset) which collects 32 different species of plants. This research presents multiple grids and dimensionality reduction based descriptors approach, which is simple but effective. The multiple grids divide plant leaves into sub-regions, then it brings the sub-region to calculate the special features using various feature extraction techniques that pull out the distinctive characteristics of the plant leaves. The methods are a histogram of oriented gradients (HOG), local binary pattern (LBP), and color histogram. Finally, the feature will be fed to the dimensionality reduction method by using principal component analysis (PCA) in order to reduce the feature vector size of each method. The size reductions have direct effect on training time and increase the recognition efficiency as well. In this paper, the feature vector was used in training and recognition by a support vector machine (SVM) and Multi-layer perceptron (MLP). This method obtained a very high recognition rate when compared to the deep learning method.

Paper Outline: This paper has been organized as follows. In Section 2, the method for plant leaf recognition is explained. Section 3, the dataset and pre-processing with plant leaf images, which are used in our experiments are described. Section 4, experimental results is presented. The last section discusses the significant findings from this study and describes future work.

2. PROPOSED PLANT LEAF RECOGNITION METHOD

In this study, we use multiple grids and dimensionality reduction based on three feature extraction techniques. Figure 1 shows the process of this research. The input images were forwarded to the multi-grid based process to divide the images into (Sub-regions), then a sub-region was calculated by using three techniques of feature extraction. Each technique was calculated by principal component analysis (PCA) method in order to decrease the amount of feature vector. Finally, researchers put all FE+PCA in concatenate to use it as a feature vector ($f_1, f_2, \dots, f_n$) then forwarded it to the classification process.

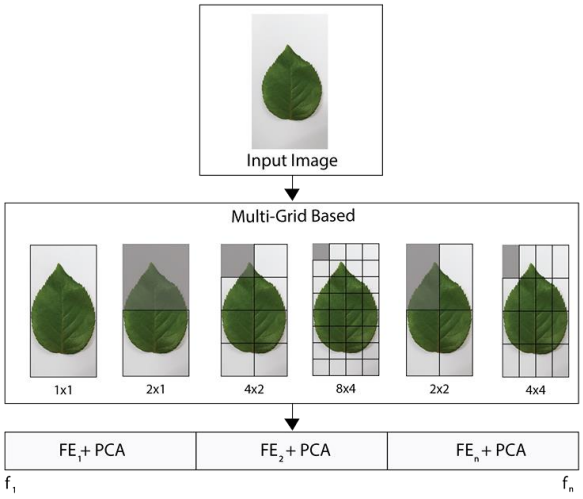


Figure 1. Proposed plant leaf recognition method.

2.1 Multiple Grid-based Technique

The working process of multiple grid-based technique is to divide the picture of the leaves (Input image) into sub-regions by using a grid in the determination of the sub-regions. In these experiments, the Grids were determined at 6 different types, including Grid size of 1x1, 2x1, 4x2, 8x4, 2x2, and 4x4. After that, each sub-area was calculated to find the feature vector by using HOG, LBP, and color histogram.

2.2 Feature Extraction Techniques

2.2.1 Histogram of Oriented Gradients (HOG)

HOG introduced by Dalal and Triggs [16], a method that extracts the characteristics of the image by calculating the oriented gradients from gradient Image by finding gradient in (Horizontal) (G_x) and (Vertical) (G_y) which is calculated from pixel intensities ($I(x, y)$) at (x, y) as the following equation:

$$G_x = I(x+1, y) - I(x-1, y) \quad (1)$$

$$G_y = I(x, y+1) - I(x, y-1) \quad (2)$$

After that, the magnitude (M) and gradient orientation (θ) are calculated as the following equation:

$$M(x, y) = \sqrt{G_x^2 + G_y^2} \quad (3)$$

$$\theta_{x,y} = tan^{-1}\frac{G_y}{G_x} \quad (4)$$

where$M(x,y)$is magnitude of gradients, $\theta_{x,y}$is gradient orientation at x,y. Then, gradient orientation values will be taken to the weighted vote process and will be kept in the orientation bins (β) [17].

Finally, gradient orientation values, which are kept in each orientation bin will be taken to do the Normalization by L2-norm method.

2.2.2 Local Binary Patterns (LBP)

LBP was proposed in [18] for invariant texture classification. LBP is designed for extracting characteristics of pixel points from Neighborhood pixels which are calculated from gray values as the following equation:

$$\mathrm{LBP_{P,R}} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p \quad (5)$$

where

g_c is the gray value of the central pixel.
g_p is the gray value of its neighbor pixels.
P is the total number of involved neighbors.
R is the radius of the neighborhood.

Then, the central pixel will be used as Threshold value (T) to compare with Neighborhood pixels values, $s(x) = \begin{cases} 1, x \geq T \\ 0, x < T \end{cases}$ The next step is to bring the value 1 and 0 from Neighborhood pixels to come together as concatenate. Then, it was converted to decimal. Finally, researchers bring the values into the specified bins.

2.2.3 Color Histogram

This research used two types of color models. There are RGB and HSV color models, while HSV used only hue (H) values because hue values show the true color. Therefore, colors values used for histogram creation consist of red (R), green (G), blue (B), and hue. While, histogram of color RGB values consist of 256 color values, H consist of 360 color values.

2.3 Dimensionality Reduction

From the Multiple-grid based method, a lot of sub-region will be created, which is used for calculation of unique features. This causes high dimensionality of the feature vector and results in computational complexity. Therefore, dimensionality reduction is one of the best ways to minimize the feature vector. This research uses PCA [19] in feature vector reduction. Feature vector from each technique has been reduced to only 80 Features. These techniques improved the accuracy rate as well.

2.4 Classification Algorithms

This research used two types of classification algorithm, including support vector machine (SVM) [20] and multi-layer perceptron (MLP) [21]. The SVM used RBF kernel and MLP by determining the hidden layer as two layers. The dropout method was selected for prevention of an overfitting situation.

3. PLANT LEAF DATASET

The plant leaves images used in the experiment were taken in the laboratory. Thus, most images have a white background. The background makes the leaves prominent and clearly separates them from the background.

3.1 Folio Dataset

The leaves data used in the experiment was the Folio dataset, presented in 2015 [8]. The data represents 32 species of leaves plant images (see Figure 2). All images were taken in the laboratory with a white background. All images were saved in the JPEG format. Size of images is 2322x4128 and 2448x3264 pixel resolution. The plants were in the University of Mauritius farm. Twenty images of each plant species were collected except for mulberry with 19 images and eggplant with 18 images. The dataset contains 637 images.

Some plant leaves are shown twice; they are the same type, but they have different shapes (For example, papaya, chrysanthemum, and ketembilla). Image differentiation of each species are shown in Figure 3. Some plant leaves still have similar shape, e.g., star apple and pomme jacquot (See Figure 4). The factors mentioned above have directly affected the accuracy of recognition.

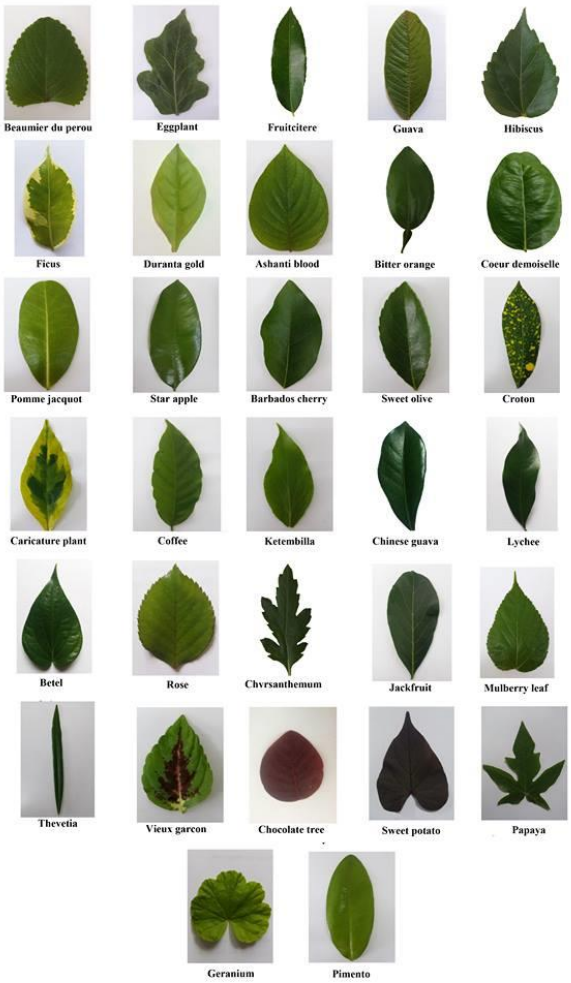
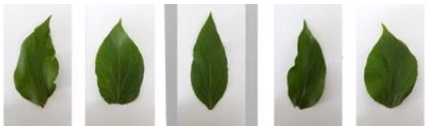


Figure 2. Examples of 32 plant leaves of the Folio dataset.

a)

b)



c)

Figure 3. Some variety examples of plant leaves, a) papaya, b) chrysanthemum, and c) ketembilla leaf images of the Folio dataset.

a) b)

Figure 4. Similarities shape between different plant leaves. a) The images of star apple and b) pomme jacquot leaves.

3.2 Dataset Pre-processing

The process of preparing the image of the plant leaves from the Folio dataset is very simple. The process starts by converting all the images to black and white in order to find the plant leaves area (Region of interest: ROI), Then, crop to get ROI. The next step is to check the image of the leaf in the horizontal position and then rotate the image to vertical shape (See Figure 2). After that, the image resizes are resize to 400 pixels. The width of each picture will have different sizes because some plant leaves, e.g., thevetia, lychee, and fruit citere are slender. Therefore, if we assign the size as 400x200 pixel, the plant leaves images will be distorted. Finally, when ROI was identified and resized, the color image for feature extraction process was used.

4. EXPERIMENTAL RESULTS

We compared the feature extraction techniques (i.e., color histogram, local binary pattern (LBP), a histogram of oriented gradients (HOG), and principal component analysis (PCA)) and HOG-bag of word (HOG-BOW) to deep learning techniques (AlexNet and GoogleNet).

In these experiments, we used 5-fold cross-validation to evaluate the results of the plant leaf recognition methods. We used the recognition rate (accuracy) and standard deviation to measure the performance of each feature extraction technique. For the experiments using the support vector machine (SVM) algorithm, the grid-search technique was used to search the best parameters. The best C and gamma (γ) parameters of the SVM with the RBF kernel are 100 and 0.1, respectively. For the multi-layer perceptron (MLP), two hidden layers are used where the size of each layer is 512 and 512 hidden units, respectively. The dropout regularization is used to prevent neural networks from overfitting. The dropout rates of 0.5 for all hidden units are selected. As for the output layer, the softmax function is used. Table 1 and Table 2 show the results (average test accuracy and standard deviation).

The results in Table 1 show the recognition performances obtained from the combination of multiple grid approaches with feature extraction techniques, the result of the HOG-BOW method, and the training time on the Folio dataset. We can see 15 different results. Here, the HOG-BOW method obtains an inferior performance compared to the other feature extraction techniques. On the other hand, the Color-Histogram-LBP-HOG-PCA, when combined with the SVM with the RBF kernel algorithm, significantly outperforms the other techniques and provides a high accuracy of 99.06%. Subsequently, the plant leaf recognition obtains a high accuracy of 98.75% when combined with the Color-Histogram-LBP-HOG-PCA and MLP algorithm.

Table 1. Plant leaf recognition results of the 15 different techniques on the Folio dataset

Multiple Grid Methods	Training Time (Sec)		Accuracy (%)	
	SVM	MLP	SVM	MLP
Color-Histogram	221.86	232.42	96.25±1.87	95.94±1.94
LBP	278.80	284.80	94.45±1.06	91.87±2.22
HOG	201.27	206.83	94.14±2.45	94.14±2.34
Color-Histogram-PCA	182.88	189.49	97.73±1.30	97.11±1.28
LBP-PCA	278.15	285.29	94.14±1.06	94.14±1.74
HOG-PCA	202.12	209.53	93.83±2.62	93.91±1.83
Color-Histogram-LBP	496.61	511.65	97.81±1.15	96.09±1.65
Color-Histogram-HOG	419.10	435.47	98.13±1.39	96.64±1.38
LBP-HOG	481.14	489.10	97.50±1.46	96.87±1.98
Color-Histogram-LBP-HOG	697.46	716.77	98.67±0.91	97.42±1.48
Color-Histogram-LBP-PCA	460.96	469.78	98.67±1.11	98.28±1.51
Color-Histogram-HOG-PCA	384.91	393.20	98.59±1.46	98.28±1.32
LBP-HOG-PCA	480.19	488.94	97.50±1.46	97.58±1.01
Color-Histogram-LBP-HOG-PCA	663.01	672.19	**99.06±0.89**	**98.75±0.92**
HOG-BOW [9]	-	-	92.78±2.17	92.37±1.78

Table 2. Comparing results between proposed method and fine-tuned deep learning methods on the Folio dataset

Method	Accuracy (%)
AlexNet [10]	97.67±1.60
GoogleNet [10]	97.63±1.84
AlexNet data augmentation (Contrast) [9]	99.04±0.38
GoogleNet data augmentation (Illumination) [9]	**99.42±0.38**
Proposed Method (Color-Histogram-LBP-HOG-PCA)	99.06±0.89

We also compared our proposed method with the find-tuned deep convolutional neural networks (CNNs), which are AlexNet and GoogleNet architectures [9]. Furthermore, the data augmentation techniques consisting of contrast and illumination [10] techniques were compared as well. The accuracy results between our proposed method and fine-tuned deep CNNs are shown in Table 2.

The performance of our proposed multiple grids and dimensionality reduction based descriptors approach reaches 99%. Our proposed method performs better than the deep CNN architectures. However, the fine-tuned deep CNNs with the combined data augmentation technique, (contrast and illumination), slightly outperform our proposed method. This is because, the fine-tune deep CNNs were trained from millions of images, and the training data increased 4,005 images from the data augmentation technique our proposed method train and create the plant leaf recognition model from only 510 plant leaf images.

5. CONCLUSION

In this paper, we have investigated many different plant leaf recognition techniques on a Folio dataset. From the experimental results, we conclude that the performance of multiple grids and dimensionality reduction based descriptors, which is our proposed method, is much better than the histogram of oriented gradients combined with bag-of-words technique and fine-tuned deep CNN architectures which are AlexNet and GoogleNet architectures as well. We also have shown that the principal component analysis (PCA), which is the dimensionality reduction technique, increased the accuracy performance and decreased the number of the feature vector of the plant leaf recognition system. Nevertheless, the data augmentation technique can increase the accuracy performance of the plant leaf recognition system. This technique added more than 4,000 illumination images to the training set. Subsequently, we used only 510 images to train the plant leaf recognition system. As a result, the accuracy result of our proposed method is slightly decreased than the fine-tuned deep CNNs with the combined data augmentation technique.

According to the high accuracy of the deep CNNs, in future work, we would like to study the effect of parallel CNN architecture and use this architecture to train the plant leaf images. This technique maybe necessary to improve training times and accuracy performance.

6. REFERENCES

[1] Wäldchen, J. and Mäder, P. 2018. Plant species identification using computer vision techniques: a systematic literature review. In *Archives of Computational Methods in Engineering*. 25, 2 (2018), 507–543.

[2] Caballero, C. and Aranda, M. C. 2010. Plant species identification using leaf image retrieval. In *ACM International Conference on Image and Video Retrieval (CIVR)*, 327–334.

[3] Cerutti, G., Tougne, L., Mille, J., Vacavant, A. and Coquin, D. 2013. Understanding leaves in natural images - A model-based approach for tree species identification. In *Computer Vision and Image Understanding*. 117, 10 (2013), 1482–1501.

[4] Cho, S. Y. 2012. Content-based structural recognition for flower image classification. In *7th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 541–546.

[5] Caglayan, A., Guclu, O. and Can, A.B. 2013. A plant recognition approach using shape and color features in leaf images.In *Image Analysis and Processing (ICIA)*, 161–170.

[6] Hossain, J. and Amin, M. A. 2010. Leaf shape identification based plant biometrics. In *13th International Conference on Computer and Information Technology (ICCIT)*, 458–463.

[7] Wang, X. F., Huang, D. S., Du, J. X., Xu, H. and Heutte, L. 2008. Classification of plant leaf images with complicated background. In *Applied Mathematics and Computation.* 205, 2 (2008), 916–926.

[8] Munisami, T., Ramsurn, M., Kishnah, S. and Pudaruth, S. 2015. Plant leaf recognition using shape features and colour histogram with k-nearest neighbour classifiers.In *Procedia Computer Science*. 58, (2015), 740–747.

[9] Pawara, P., Okafor, E. and Schomaker, L. 2017. Data augmentation for plant classification. In *Advanced Concepts for Intelligent Vision Systems. (ACIVS)*, 615-626.

[10] Pawara, P., Okafor, E., Surinta, O., Schomaker, L. and Wiering, M. 2017. Comparing local descriptors and bags of visual words to deep convolutional neural networks for plant recognition. In *the 6th International Conference on Pattern Recognition Applications and Methods (ICPRAM)*, 479–486.

[11] Cerutti, G., Tougne, L., Coquin, D. and Vacavant, A. 2013. Curvature-scale-based contour understanding for leaf margin shape recognition and species identification. In *the International Conference on Computer Vision Theory and Applications (VISAPP)*, 227-284.

[12] Salman, A., Semwal, A., Bhatt, U. and Thakkar, V. M. 2017. Leaf classification and identification using Canny edge detector and SVM classifier. In *International Conference on Inventive Systems and Control (ICISC)*, 1–4.

[13] Arafat, S. Y., Saghir, M. I., Ishtiaq, M. and Bashir, U. 2016. Comparison of techniques for leaf classification. In *Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, 136–141.

[14] Khmag, A., Al-Haddad, S. A. R. and Kamarudin , N. 2017. Recognition system for leaf images based on its leaf contour and centroid. In *IEEE 15th Student Conference on Research and Development (SCOReD)*,467-472.

[15] Chaki, J., Parekh, R. and Bhattacharya, S. 2015. Plant leaf recognition using texture and shape features with neural classifiers. In *Pattern Recognition Letters.* 58, (2015), 61–68.

[16] Dalal, N. and Triggs, B. 2005. Histograms of oriented gradients for human detection. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 886–893.

[17] Karaaba, M., Surinta, O., Schomaker, L. and Wiering, M. 2015. Robust face recognition by computing distances from multiple histograms of oriented gradients.In *IEEE Symposium Series on Computational Intelligence (SSCI)*, 203-209.

[18] Ojala, T., Pietikainen, M. and Maenpaa, T. 2002. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. In *IEEE Transactions on Pattern Analysis and Machine Intelligence.* 24, 7 (2002), 971–987.

[19] Cootes, T. F., Taylor, C. J., Cooper, D. H. and Graham, J. 1995. Active shape models – their training and application. In *Computer Vision and Image Understanding*. 61, 1 (1995), 38–59.

[20] Vapnik, V. N. 1998. *Statistical Learning Theory*. Wiley.

[21] Haykin, S. 2008. *Neural Networks and Learning Machines: A Comprehensive Foundation*.

Adaptive Height Table and Chair System Based On Face Recognition

Zhifeng He
Internet of Things Engineering
Zhengzhou University
China
+86 17638598501
manage_hzf@163.com

Xinran Shao
Internet of Things security
Zhengzhou University
China
+86 18903862198
ranxin101@gmail.com

Yuanyuan Xiao
Internet of Things Engineering
Zhengzhou University
China
+86 13253525949
xyy_manage@163.com

ABSTRACT
This paper designs an intelligent study desk and chair for home education. It can detect the height of the human body, control the height of the table according to the height of the person, record each user's data, and automatically adjust the state of the table and chair when the user uses it twice. It can also use a clever way to correct the user's sitting posture and remind the user to take a reasonable rest after the user has worked for a long time.

CCS Concepts
• **Information Embedded and cyber → physical systems → Sensors and actuators**

Keywords
Intelligent study desk and chair; detection height; automatic height adjustment; record user data.

1. INTRODUCTION
With the development of the Internet of Things technology, the concepts of automation and intelligence have become popular. IoT devices have entered every corner of our lives. With the popularization of smart terminals such as smart phones, our lives have become more convenient and faster. At present, the application of automation and smart products is mainly aimed at the smart home industry. Waleed [1] defines smart homes as "providing a living environment." It uses advanced intelligent technology to operate and respond to residents' needs.

After investigation and research, it is found that currently there are "smart doors", "smart windows", "smart curtains", "smart lamps", "smart refrigerators", etc. on the market, but there is no one on the market that can meet people's work Table and chair system for learning needs. In response to this pain point, this paper proposes a smart table and chair solution based on face recognition.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388214

The design consists of "smart table" and "smart chair", in which the legs of the table and chair are replaced by a pusher motor that can be controlled by current. Stm32 microcontrollers, raspberry pies, desk lamps, relays, ultrasonic sensors and other components related to this solution are integrated on the table and chair.

This solution can use face recognition to obtain the user's height, and analyze and match the height. According to the user's relevant data, the optimal height of the table and chair is selected, and the data is packaged into instructions and sent to the table and chair through communication such as Socket. The table and chair decode the data packet to obtain the optimal height h1. The table and the chair obtain the height of the table h2 and the chair h3 through two ultrasonic waves. H1 and h2 are compared with H3 to control the relay output signal and control the push rod motor to rise or fall to make the table And the actual height of the chair is equal to the height required by the user. Give users the best experience.

At the same time, the design of the "smart chair" provides a voice reminder service to prevent users from losing their attention due to long hours of work. The chair obtains the sitting posture of the user by detecting the pressure analysis of different contacts on the chair surface, and issues a voice reminder to correct the sitting posture of the user when the user does not sit down properly.

2. SOLUTION ADVANTAGE
The height of tables and chairs on the market is usually not adjustable, which will cause users to change tables and chairs as their height changes. Some adjustable tables and chairs are manually adjusted (see Figure 1). The adjustment method is not accurate enough. The design can automatically adjust the height of tables and chairs, suitable for users of different ages and heights. At the same time, the user is authenticated through facial recognition, so that the user can automatically obtain the best state of the table and chair when using it twice, which is very convenient. Figure 1 is a picture of traditional tables and chairs

Figure 1. Traditional table and chair.

Shao Qingqing et al. Proposed a smart table with adjustable height. [2] "The intelligent lift controller is mainly composed of WIFI

module and MCU. WIFI module receives and returns relevant communication data, MCU completes data collection and related peripheral device drivers. Users use the one-click network function of mobile APP to After the WIFI module of the controller is connected to the designated router, the mobile APP sends a UDP broadcast response after sending the UDP broadcast to the designated port; the user uses the mobile APP. The WIFI module of the lifting platform receives relevant instructions of the MCU through the UART port to control the State. "In this solution, the height of the table and chair needs to be measured by the user, which is not smart enough. At the same time, when users (users are elementary and junior high school students) get along with mobile phones connected to the Internet, it is difficult to concentrate on continuing work and learning, and reducing work efficiency. Figure 2 is a picture of Electric lift tables and chairs on the market

Figure 2. Electric lift tables and chairs on the market.

This program is designed for growing young students, with automatic recognition of height function, automatic adjustment of table and chair height function, data storage function, sitting posture correction function, sedentary reminder function, voice interactive function. It not only solves the problem that the traditional table and chair is difficult to adjust the height, but also uses the Internet of Things solution to make the height adjustment more intelligent, automatic and convenient, and meet the needs of users. In addition, in order to solve the problem of adolescent users sitting in a wrong position (bad sitting posture will affect the poor sitting posture will cause students' vision loss, causing developmental malformation, affecting breathing and circulation function, etc.), the intelligent chair is used to detect the sitting position of the user. Voice to remind the correction; in order to solve the user sitting for a long time to work ([3] people need to sit a lot of time a day, such as sitting, eating, sitting, watching TV, sitting and working, etc. Studies have shown that sedentary It is one of the important causes of musculoskeletal diseases, but the sedentary hazard is not fully recognized compared with the risk of heavy labor such as handling. [4] Sedentary will cause many health problems, such as lower back legs. Pain, cardiovascular disease, etc., for example, in 3 months, an average of one in four American adults will have at least one symptom of low back pain. Especially the sedentary posture in a bad posture will increase the body's back pain, arthritis, Thrombosis, lumbar disc herniation, spinal deformity, cervical spine, body hypoxia, prostate problems, and rectal cancer.), intelligence The chair detects the user's sitting time and provides a voice reminder when the value exceeds the threshold to protect the user's health. Of course, not only these, the white noise function of this solution can also improve the user's attention and improve the user's learning efficiency.

3. DESIGN ARCHITECTURE

In this page, I will introduce the system architecture of this design in a total way. The first is the function overview, then the module is introduced to implement the solution, and finally the effect of the solution is summarized.

3.1 Project Overview

The design is divided according to software and hardware. The hardware is divided into automatic lifting module, height detecting module, sitting posture detecting module, sedentary reminding module, voice reminding module, Bluetooth communication module; software aspect is divided into Socket communication module, face recognition module , height detection module. The software and hardware components of the solution are shown in Figure 3.

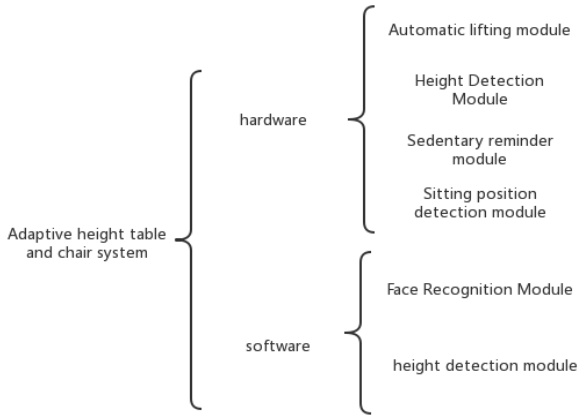


Figure 3. Schematic diagram of the scheme.

3.2 Module Introduction

3.2.1 Automatic lifting module

This program uses STM32 F103ZET6 as the main control chip. Three relays are connected through the DuPont line, one relay determines whether the motor starts, and two relays control the forward and reverse rotation of the motor to drive the table and chair to lift. The Bluetooth hc05 module is used for communication between the table and the chair, and exchanges the user's weight information measured by the chair with the user's height information measured by the table. The intelligent automatic lifting of tables and chairs can maximize the user's learning or working comfort. Figure 4 is the wiring diagram of three relays

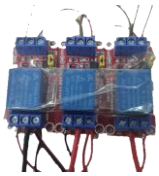


Figure 4. Three relay wiring diagrams.

3.2.2 Height Detection Module

In this solution, an ultrasonic module is placed at the appropriate position of the table and the chair, and the height of the current table and the ground, the height of the surface of the chair and the ground are obtained by ultrasonic ranging, and the two height values are packaged as instructions through the corresponding protocol. The Bluetooth serial port is sent to the Raspberry Pi.

[5] $L = 340m/s * \Pi * T/2 = T * 170m/s = T * 58\mu s/cm$

3.2.3 Sedentary reminder module

This program will place an Fsr pressure sensor on the chair every 1/3, read the Adc signals of the three sensors through Stm32 and convert them to a pressure value A0 [3] through the digital-to-analog conversion module (representing the values of three pressure sensors) When value: A0 [1] changes, stm32 sends instruction 1 to Raspberry Pi via hc05 (the format is at the end of the text). Raspberry Pi starts or stops the timing function to obtain the user's learning time. When the time exceeds the threshold (the threshold can be set manually), the Raspberry Pi will wake up the speaker to issue a voice reminder to remind the user to rest. Figure 5 is the implementation flowchart of this function

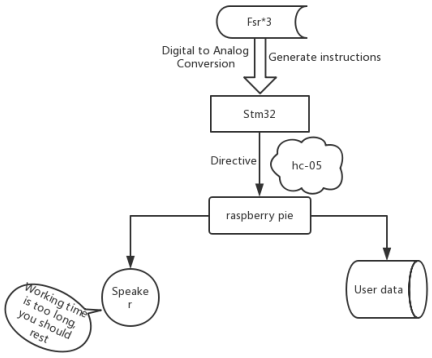


Figure 5. Sedentary reminder flow chart.

3.2.4 Sitting position detection module

Place the human infrared sensor on the table to detect the distance between the person and the table. When the distance is too close, the buzzer will give a reminder. In addition, three fsr film pressure sensors were placed on the surface of the chair to detect the pressure difference at different positions on the chair to obtain the user's sitting posture, and generate instruction , and then feedback to the user to adjust the sitting posture. Figure 6 is the flow chart of sitting position detection.

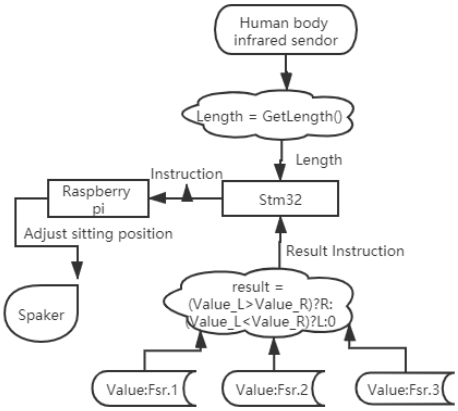


Figure 6.Seated position detection flowchart.

3.2.5 Face Recognition Module

On the Raspberry Pi side, the open cv and the effective deep convolutional neural network model Lightfacenet [6] were used for model training. When new users use this solution, the Raspberry Pi database will automatically register the user's identity information, including facial features, height, gender, and the height of the best table and chair. When the user uses it twice, it will automatically match the face recognition function and recognize it, then adjust the table and chair to the optimal state.

Note: Training model using FaceNet model.FaceNet uses a complete model to output 128-dimensional features of face information, and uses the Triplet Loss loss function to train and learn the model. The complete process is shown as figure 7.

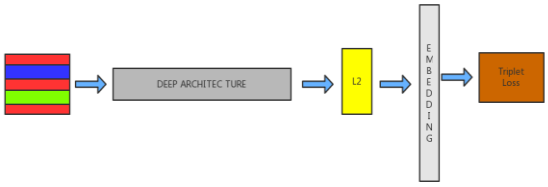


Figure 7. FaceNet processing basic process.

As shown in the figure 7, Deep Architecture in the figure extracts the feature matrix of the output image, and normalizes it through L2 norm, and obtains Embedding code. This code is the face information projected into a Euclidean space. The code, through this code, we can complete the above face recognition, face verification, face retrieval work.

The innovation of this model is that the feature is optimized directly by the Triplet Loss loss function, so that better recognition indicators can be obtained. Table 1 is part of the development environment and version

Table 1. Configuration Environment

Idle name	Version
operating system	Windows 7
IDE	PyCharm professional
TensorFlow	1.9
Python interpreter	Anaconda python 3.5
data set	Full LFW Data set

Since the resolution of the LFW dataset used in this article is 250 * 250 resolution, the input data size required by Google Inception-ResNet is 160 * 160 resolution, and we corrected the resolution to 160 * 160 during the training process. Face detection and alignment have been completed. After data preprocessing is complete, model training can begin. After completing the model and training program, import the processed data into the corresponding folder, and then start the training process, preprocessing process and results. As shown in Figure8

Figure 8. Model training results andModel training process.

3.2.6 height detection module

This scheme uses image recognition to identify the height. The camera takes a random object in the environment as a reference object, trains the opencv model to detect the image height, and roughly calculates the height of the human body. Users can manually adjust on this basis, the system will remember the user's adjustments, and record it into the database, so that users can use it next time.

3.3 Module Summary

This program combines image recognition, single-chip application, various sensor coordination applications and other methods to propose an intelligent, automated smart table and chair solution, which can effectively solve the problem that the height of the table and chair does not match the height of the human body, the user is not correct, the user Problems such as long-term work and harm to the body can basically meet the needs of home users.

4. SOLUTION APPLICATION SCENARIO

This program is suitable for various scenarios such as home and school.

In the family, this program can be used as a family learning (work) sharing platform, which can remind students to study on time and on time. It can also remind workers (parents) to take a break after working for a long time. The function of automatically adjusting the height can also meet different users of the family. Different needs.

In the school, the height of the students is different due to the difference in height of the students. When using this program in the classroom, the students of different heights can meet the needs of different height tables and chairs, and the face recognition function can be Protect the student's private information as an encryption method.

This program has a wide range of strengths and is suitable for different groups of people in different scenarios.

5. COST ANALYSIS

In the model design stage, the system components include desktop, push rod motor, serial screen, stm32 microcontroller, raspberry pie, relay, ultrasonic, Bluetooth, and wires. The total price is about $ 175. For details, please see the following. List of materials. According to the development experience, when the actual production operation is performed, the stm32 microcontroller and the Raspberry Pi will be deleted and merged. The cost will be reduced to about $ 20. The cost of the putter motor will be reduced to $ 20. Will be reduced, according to this, users can spend a minimum of $ 100 to enjoy the comfort and convenience brought by this table and chair. Table2 is the price of some materials

Table 2. Material list

Material name	Unit price	Material name	Unit price
Tables, chairs	$30	Putter motor	$40
MCU-Stm32	$11.2	raspberry pi	$39.29
HC-05	$4.6	HC-SR04	$0.6
SDWe070C01	$25.57	FSR	$17.04

6. CONCLUSIONS

According to theoretical analysis and physical verification, this program addresses the current social pain points-people of different heights have different requirements for the height of tables and chairs, and proposes a thinking based on the application of the Internet of Things based on the intelligent work of MCU and various sensors Table and chair system. Image recognition is applied to height detection and identity verification, making the solution more intelligent and convenient. In addition, in order to effectively correct the poor sitting posture of adolescents. Added a sitting detection function to the system. At the same time, sedentary reminder function can make users reasonably distribute work, and voice playback makes the system more intelligent. The solution is relatively complete and can meet the needs of most people. It can also be applied to other scenarios and is expected to be adopted. Figure 9 is the final appearance of the system. Table 3 is some test data

Figure 9. Scheme finished product model.

Table 3. Some test data

Name	Sex	Height	Desk-height	Chair-height
Han	Male	185	90	70
Wang	Male	174	83	65
Shao	Female	166	75	57
...	...	...	...	...

7. REFERENCES

[1] J. Waleed, A. M. abduldaim, T. M. Hasan, and Q. S. Mohaisin, “SmartHome as a New Trend, a Simplicity Led to Revolution” in 2018 1stInternational Scientific Conference of Engineering Sciences – 3rdScientific Conference of Engineering Sciences (ISCES), pp. 30-33.

[2] Shao Qingqing, Zhou Jianhua, Xu Chen, Li Luyang. Intelligent Lifting Table Controller Based on ESP8266+STM32[J]. Mechanical Engineering and Automation, 2017(06): 155-156.

[3] Status and data survey of work-related musculoskeletal diseases in Europe, EU Work Safety and Health Organization, 2010, ISSN 1830-5946

[4] Jannique G.Z. van Uffelen, Jason Wong, et. al. Occupational Sitting and Health Risks - A Systematic Review. Am J Prev Med 2010;39(4): 379–388

[5] Li Zhuohua, Yang Shangqi, Yan Yaxin, Zheng Mengying, Yang Ruojun. ARM-based smart table and chair system for smart homes[J] .Electronic world,2018(02):179-180

[6] Zhang Dian, Wang Haitao, Jiang Wei, Chen Xing. Research on real-time face recognition algorithm based on lightweight network [J/OL]. Computer Science and Exploration: 1-9[20191106].http://kns.cnki .net/kcms/detail/11.5602.TP.20191104.1815.012.html

Improving Recognition of Thai Handwritten Characters with Deep Convolutional Neural Networks

Sarayut Gonwirat
PhD Student, Multi-agent Intelligent Simulation Laboratory
Department of Information Technology
Faculty of Informatics, Mahasarakham University
Maha Sarakham, Thailand
61011262003@msu.ac.th

Olarik Surinta
Multi-agent Intelligent Simulation Laboratory
Department of Information Technology
Faculty of Informatics, Mahasarakham University
Maha Sarakham, Thailand
Olarik.s@msu.ac.th

ABSTRACT
For handwritten character recognition, a common problem is that each writer has unique handwriting for each character (e.g. stroke, head, loop, and curl). The similarities of handwritten characters in each language is also a problem. These similarities have led to recognition mistakes. This research compared deep Convolutional Neural Networks (CNNs) which were used for handwriting recognition in the Thai language. CNNs were tested with the THI-C68 dataset. This research also compared two training methods, Train from scratch and Transfer learning, by using VGGNet-19 and Inception-ResNet-v2 architectures. The results showed that VGGNet-19 architecture with transfer learning can reduce learning time. Moreover, it also increased recognition efficiency up to 99.20% when tested with 10-fold cross-validation.

CCS Concepts
• **Applied computing → Optical character recognition**
• **Computing methodologies → Neural networks.**

Keywords
Handwritten Character Recognition; Convolutional Neural Network; VGGNet; Inception-ResNet; Transfer Learning.

1. INTRODUCTION
Character recognition is fundamental to research that can lead to document analysis, text transcription, or development of automatic reading systems [12]. The recognition method can be beneficial in many fields, e.g. historical document recognition systems, text image retrieval, signature verification, and traffic-sign recognition.

In general, the data used in recognition research about Handwritten Character Recognition (HCR) includes digit, vowel, consonant, and special characters which depend on the writing style of each country [8, 11, 19]. The widespread traditional method is the feature extraction method, including Histogram of Oriented Gradients (HOG), Scale-Invariant Feature Transform (SIFT) [19], and Local Binary Pattern (LBP) [7]. Subsequently, the extracted data are made as an input for various types of machine learning, including K-Nearest Neighbors (KNN) [19], Support Vector Machine (SVM) [5, 19], Multi-layer Perceptron (MLP) etc.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

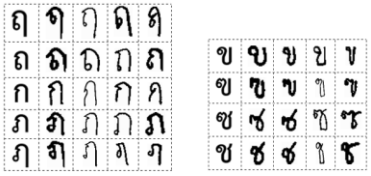
ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388181

The Convolutional Neural Network (CNN) method [10], which is a deep learning algorithm for fixing the problems in HCR [8, 11], has higher recognition efficiency than traditional machine learning. The differences is that the convolution process in CNN can calculate and find special features automatically which makes CNN Architecture have more layers; for example, VGGNet [18] consists of 16 and 19 layers, ResNet [2] consists of 50, 101 and 152 layers. This directly affects the amount of parameter in calculation. Some research has developed architecture for reducing the number of parameters, for example the Squeeze and Excitation Module [3] and Global Average Pooling Layer (GAP) [16, 20]. The regularization can also be used as an adjustment for weight [21], dropout, and batch normalization [6] in order to increase the efficiency of deep CNN architectures and decrease the data overfitting problem. Furthermore, the data augmentation method is a method for increasing the amount of information used in learning of network and transfer learning. The learning process uses weight values from the model that have previously been learned, then the researcher improved the weight values. The new weight values will be consistent with new information resulting in reduction of learning time and increased network efficiency.

The challenge of handwriting character recognition is the writing style of each person, e.g. emphasizing weight while writing, curve, head of alphabet, and differences in tail-line drawing (stroke, head, loop, and curl). Some characters are similar to other characters. The writing style of the same person at different times is also unstable. Figure 1 shows some characters which share some similarities. In Figure 1(a) the characters have some similar structure, but there are differences at the head of the letter and traits of the tail lines. For Figure 1(b) there are zigzag at the head of the letter. If the writer writes it quickly, the wavy line might not be clear. Then, it will be considered as another character.

Feature Extraction is a part that makes high accuracy rate for character recognition. Studies of Thai handwritten character recognition [5, 19] have used various methods to find unique characteristics. Surinta et al. [19] used two local descriptor methods; Scale-Invariant Feature Transform Descriptor (siftD) and Histogram of Oriented Gradients (HOG). The feature vectors from both descriptor methods were sent to a classifier, including K-Nearest Neighbors (KNN) and Support Vector Machine (SVM) by using Radial Basis Function (RBF) Kernel. The experimental

results show that siftD with SVM was the most effective method at 94.34% accuracy.



(a) (b)

Figure 1. Examples of similar character groups. (a) Characters with different tail traces and (b) characters with different indentation at head positions.

Inkeaw et al. [5] have developed a method for finding special features called Gradient Features of Discriminative Regions (GFoDRs), which use HOG to calculate the gradient values. This method was called HOGFoDRs. The special features were sent to the SVM classifier for character classification. The HOGfoDRs were designed for discrimination of similar characters. The accuracy rate of this method was 98.76%.

Contribution: The objective of this research is to perform the efficiency of deep CNN on character recognition of Thai handwritten character. The architecture of CNN in this research is composed of VGGNet [18] and Inception-ResNet [20], which do not need to calculate special characteristics because convolutional layers in deep CNN calculates lower-level feature. The test compares both learning style, including scratch learning and transfer learning in order to find the most suitable model for Thai handwritten analysis. We did not use data augmentation to increase training data for learning the deep CNN in both architectures due to compare the experimental results with the siftD+SVM [19] and HOGfoDRs methods [5]. The experiment found VGGNet Architecture with transfer learning were the most effective in recognition while compare to other methods. Therefore, this method is suitable for solving the problem of character recognition in Thai handwritten.

Paper outline: This paper is organized as follows: in Section 2, the background of convolutional neural networks is explained. Two deep CNN architectures are described in Section 3. Section 4 describes the Thai handwritten character dataset that is used in the experiments. The experimental results of the deep CNN methods and other methods are presented in Section 5. The conclusion and future work are presented in Section 6.

2. BACKGROUNDS

2.1 Convolutional Neural Network

The convolutional neural network (CNN) presented by LeCun [11] for English character recognition. CNN has become popular in image recognition after Krizhevsky et al. [9] presented AlexNet Architecture and won the ImageNet Challenge in 2012. After that, the researchers developed various CNN architectures in different series, e.g. VGGNet, GoogLeNet, ResNet, DenseNet [4], and MobileNet [16]. Each CNN had different architecture and different name, e.g. number of convolutional layers, inception module [6, 20], shortcut connection module [2, 16, 20], and depthwise convolutional filters [16]. The basic structure of CNN architecture describes as follows;

2.1.1 Convolutional Layer

The Convolutional Layer (Conv) is the main layer which is used for calculating feature extraction. The convolution process is to find dots from the input layer (Image) or output of previous convolutional layer as shown in Equation 1. The input layer is required to have feature map (x_p), while p is the hierarchy of the layer in CNN. The CNN has amount of parameters equal to $w_p \times h_p \times d_p$, while w_p is length, h_p is width, d_p is channel. From calculating convolution and filter kernel (K), the result is a feature map (x_{p+1}) which has size equal to $d_k \times d_k \times d_p \times d_{p+1}$ while d_p is the width and length of kernel (K) in the hierarchy p.

$$X_{k,l,n}^{p+1} = \sum_{i,j,m} K_{i,j,m,n}\, x_{k+i-1,l+j-1,m}^{p} \quad (1)$$

Output or feature map from each layer was sent to the activation function in a Rectified Linear Units (ReLU): as shown in Equation 2 [13]. Then, it was sent to batch normalization (BN) process [6]. BN Layer normalizes the input data by scaling all data in order to provide data in the same range. This speeds up the learning and reduces data overfitting. As a result, the dropout configuration can be set to a low level, resulting in reduction of information lost during the dropout.

$$ReLU(x) = \max(0, x) \quad (2)$$

2.1.2 Pooling Layer

A Pooling Layer is a spatial computation layer in the feature map layer which helps reduction of parameter sizes in the architecture by finding of maximum, minimum, and average values.

2.1.3 Fully Connected Layer

A Fully Connected Layer (FC) is a connection of every node from one layer to every node of the next Layer. This is the same process as Multi-Layer Perceptron (MLP) while the output layer of FC layer has the number of nodes equal to the number of categories. Softmax function was used for output calculation (shown in Equation 3).

$$softmax(x) = \frac{\exp(x)}{\sum_i^N \exp(x_i)} \quad (3)$$

2.2 Optimization Method

The processing of the CNN results in the most probability type of recognition, but sometimes the answers do not match with the expectations. It is error value. Therefore, the error value could be minimized by adjusting weight parameters. In this research, the researcher uses Stochastic Gradient Descent (SGD) with momentum [15] for weight parameters adjustment (shown in Equation 4).

$$\theta_{t+1} = \theta_t + v_{t+1} \quad (4)$$

$$v_{t+1} = \mu v_t - \alpha \nabla f(\theta_t) \quad (5)$$

where μ is momentum coefficient, α_t is learning rate, and $\alpha \nabla f(\theta_t)$ is error gradient for weight parameter θ adjustment. Learning rate will be reduced when epoch of the learning increase, show in Equation 6.

$$\alpha_{\mathrm{t}} = \frac{\alpha_{\mathrm{o}}}{1+dt} \quad (6)$$

where α_{o} is the initial learning rate, d is learning rate decay.

2.3 CNN based Scratch and Transfer Learning

CNN learning method was divided into 2 processes; comprising learning from scratch and transfer learning. Learning from scratch [14] is a complex process and takes a long time to learn due to the learning beginning with creation of a random weight, by sending batches of images (batch) to learn. The sizes can be small or large

depending on the computer used in the learning. Weights are calculated and adjusted in each round depending on the input data. Finally, this process produces a model for prediction.

Transfer learning [14, 17] is applying knowledge from previous domains that have been learned, to solve problems with the same characteristics or maybe a new problem. It is assumed that the parameters from the original model can be used as a starting point to learn new information. It is called the *Pre-trained model* which directly results in faster training and higher effectiveness. This is because of pre-trained model was created from the ImageNet data set, that contains over a million images, in which sample data is organized in up to 1,000 categories. Therefore, if we want to use the Pre-trained Model for further processing with another dataset, the output node of the FC layer must be adjusted until it match the amount of that category.

3. CNN ARCHITECTURES

Since 2012, researchers have developed high effective CNN Architectures with structural adjustment methods, e.g. VGGNet [18]. In addition, the layers were increased up to 16 and 19 layers. GoogLeNet architecture [6, 20] designed Inception module. The module was assigned to use multi-size convolution including, 1x1, 3x3, and 5x5 which is called a filter. The output of each Inception module is put through each filter together (Filter Concatenation). ResNet architecture [2] was designed Residual block which is a shortcut connection that makes training processes able to skip more than one layer. ResNet was designed to have from 18, 34, 50 and 101, to 152 layers. The trend in CNN architectures development is to increase the number of layers, but to decrease the amount of parameters, e.g. Inception-ResNet [20] and DenseNet [4]. In this paper, two CNN architectures were tested. These were VGGNet and Inception-ResNet.

3.1 VGGNet Architecture

In 2014, a research team sent VGGNet [18] to compete in the ImageNet Large Scale Visual Recognition Challenge (ILSVRC). The architecture has as many as 19 layers, tiled into stacks, connected with 3 layers of FC. The first 2 layers have 4,096 nodes. The third layer has 1,000 output nodes. The highlight of VGGNet is the use of a convolution filter that is very small, only 3x3 filter when using convolution processing. When we compare with the AlexNet architecture, it can be seen that there are more layers, but it has higher efficiency.

Table 1 shows VGGNet architecture with 16 and 19 layers. VGG16 consists of convolution layer (Conv) with 3x3 (Conv3), 13 filter layers, and 3 FC layers, total 16 layers. The amount of feature maps has increased to 64, 128, 256, 512, 512, and 512 layers consequently. Max Pooling Layers were added between convolutions in order to reduce the dimension of width and length. The VGG19 also consists of 16 convolution layers and 3 FC layers.

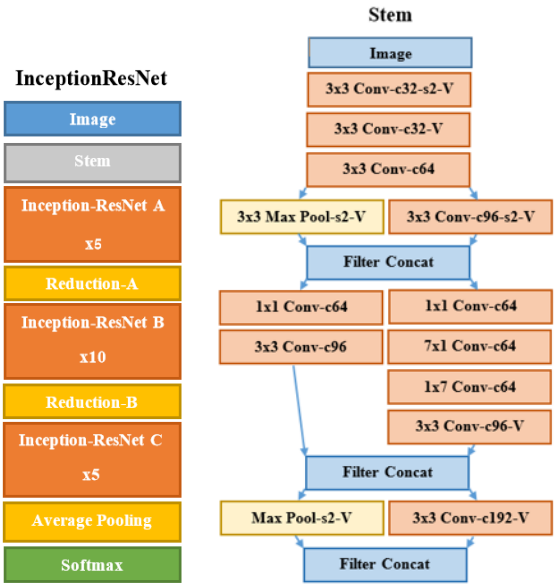
3.2 Inception-ResNet-v2 architecture

Inception-ResNet-v2 [20] was developed using batch normalization for improving the training speed. Only 7% of training steps can increase the effectiveness of the architecture. It uses Factorization to reduce the filter size, resulting in reduction of the overfitting problem, number of parameters were also reduced. The increasing of Residual block between Inception module leads to large number of Inception modules.

The main structure of Inception-ResNet-v2 divides the work function as a block, including Stem, Inception-ResNet, and Reduction blocks as shown in Figure 2(a).

Table 1. Configuration of the VGG16 and VGG19 architectures

VGG16	VGG19
Input	Input
Conv3, c64x2	Conv3, c64x2
Max Pooling	Max Pooling
Conv3, c128x2	Conv3, c128x2
Max Pooling	Max Pooling
Conv3, c256x3	Conv3, c256x4
Max Pooling	Max Pooling
Conv3, c512x3	Conv3, c512x4
Max Pooling	Max Pooling
FC-4096	FC-4096
FC-4096	FC-4096
FC-1000, Softmax	FC-1000, Softmax



(a) (b)

Figure 2. Inception-ResNet-v2 architecture. (a) Core architecture and (b) detail of the Stem block.

3.2.1 Stem Block

The Stem block is the first layer of architecture. It is a layer before the Inception module. The convolution filter in the Stem block is 3x3, stride values are 2 (s2), therefore the feature map would become smaller, which will directly decrease the parameter values as shown in Figure 2(b)

3.2.2 Inception-ResNet Block

The advantage of Inception module is the combination of ResNet Architecture and Inception layer. That is why it has been called Inception-ResNet block. The Inception-ResNet has 3 blocks, which are called blocks A, B, and C as shown in Figure 3. The

gap between Inception-ResNet blocks are separated by Reduction blocks due to parameter reduction.

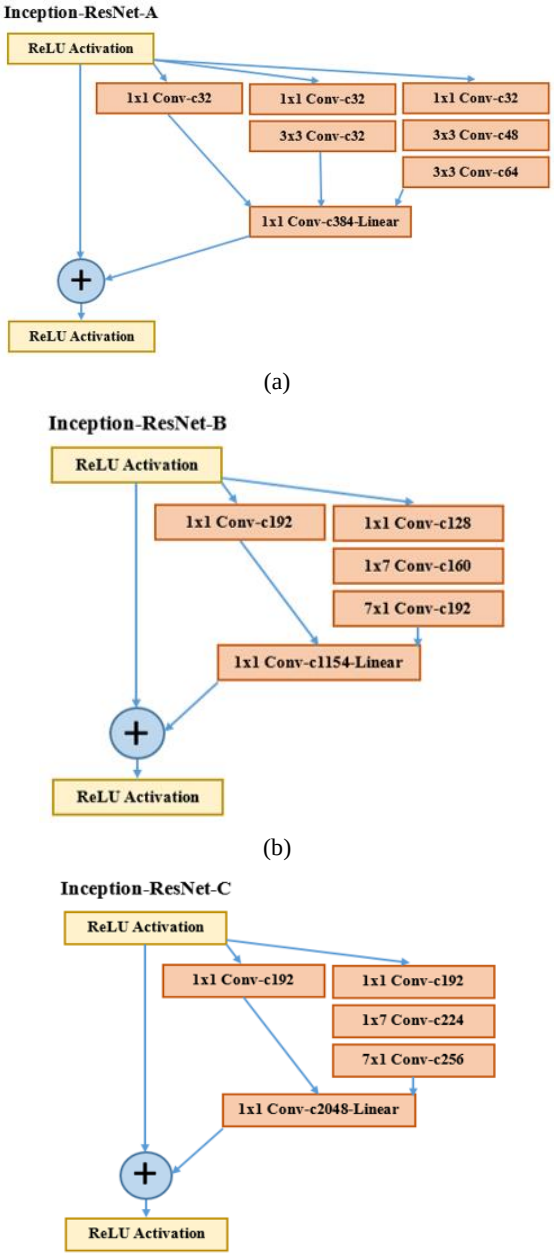


Figure 3. Architecture details of the Inception-ResNet. block (a) A, (b) B, and (c) C.

3.2.3 Reduction Block

The purpose of the Reduction block at the gap between Inception-ResNet blocks is to reduce the feature map size. Inception-ResNet architecture has 2 Reduction blocks. These are Reduction block A and B as shown in Figure 4.

4. THAI HANDWRITTEN CHARACTER DATASET

The Thai handwritten character dataset in this research is ALICE-THI dataset [19], which includes 78. types of Thai characters; consonants, vowels, tones and digits. The dataset contains writing from 150 people, aged 20-23, who were studying in a university. This research used only the THI-68 dataset which eliminated the number. Therefore, the number of characters used in recognition was 68 Characters. The data size was 14,490 characters, including 44 consonants, 17 vowels, 4 tones, and 3 symbols as show in Figure 5.

Surinta et al. [19] used special features siftD take it to learn by SVM algorithm. The accuracy rate was 94.37%. Moreover, Inkeaw et al. [5] used special feature HOGFoDRs with SVM algorithm. The accuracy rate was 98.76%. Due to the similarity of characters, this dataset is challenged for higher effective rate.

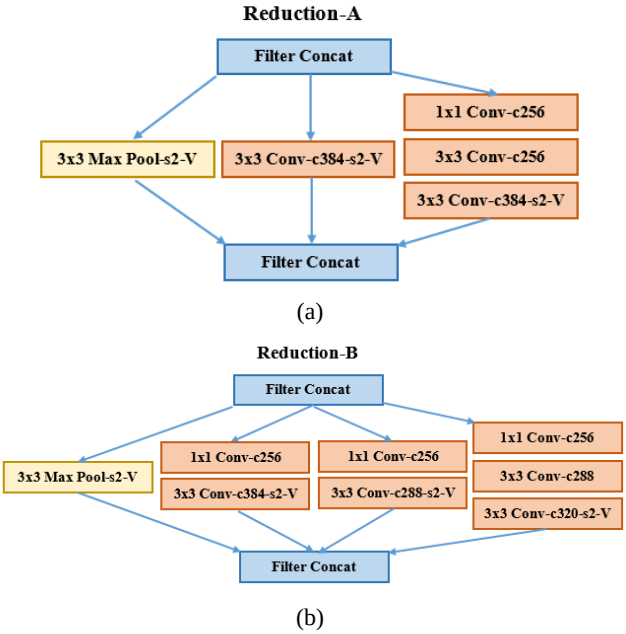


Figure 4. The reduction block (a) A and (b) B.

Figure 5. Example of 68 Thai handwritten characters.

5. EXPERIMENTAL RESULTS

This research performed the handwritten character recognition of Thai characters with ALICE-THI dataset by choosing a specific test on THI-C68 dataset which has 14,490 characters in 68 classes. This research used deep CNNs, consists of VGGNet [18] and Inception-ResNet-v2 architectures to compare the performance between both deep CNN architectures. The effectiveness of the methods were compared with siftD-SVM [19] and HOGFoDRs-SVM [5] on computer Intel(R) Core-i5, 7400 CPU @ 3.00GHz, 8GB RA, GPU GeForce GTX 1080Ti, Memory 16GB, Linux Operating system. The experiment divided the data into 2 sets. (Training and Test sets), including 5-fold, and 10-fold cross-validation. The 5-fold data and 10-fold data were set at the following ratios; Train:Valid:Test, 7:1:2 and 8:1:1, respectively.

The CNNs experiment resized all images to 128x128 pixels, which is the smallest input size of Inception-ResNet-v2. Training processes had 100 Epochs, used SGD Learning Method, Learning Rate = 0.001, Decay Rate = 0.0001, and momentum = 0.9. Learning processes were divided into 2 types which were training from scratch and transfer learning. Weight Parameters in transfer learning were derived from previous learning process by ImageNet Dataset [1]. It was called Fine-tuned.

Table 2. Performances of different models on THI-C68 dataset

Methods	Accuracy Rate (%)	
	10-cv	**5-cv**
SiftD-SVM [19]	94.34	-
HOGFoDRs-SVM [5]	-	98.76
VGGNet-Scratch	97.93 ±0.55	96.93 ±0.48
Inception-ResNet-Scratch	98.15 ±0.24	97.79 ±0.29
VGGNet-Transfer	**99.20 ±0.27**	**98.81 ±0.25**
Inception-ResNet-Transfer	98.88 ±0.24	98.61 ±0.14

To ensure comparison equality, data augmentation was not used in [5, 19]. This research also did not use data augmentation due to several studies e.g. [14] , reporting that data augmentation increases efficiency of CNN Architectures.

Table 2 is a comparison of the efficiency and accuracy of Thai handwriting characters in 6 different methods. When we analyze only deep CNN architectures, it shows that VGGNet-Transfer had the highest efficiency in both 5-fold and 10-fold with 99.2% and 98.81% accuracy rate. It was found that VGGNet in the experiments was VGG-19, which has 19 layers. Transfer learning increased the accuracy rate for CNN architecture by 1-2% when compare to the training from scratch method. The VGGNet-Scratch learning process compare to 10-fold cross-validation achieved an accuracy rate of 97.93%, which is 3% higher than siftD-SVM. However, when the researchers tested with 5-fold cross-validation, VGGNet-Transfer (98.81%) achieved an insignificantly higher effective rate than HOGFoDRs-SVM (98.76%).

From these experiments, comparison of VGGNet-19 and Inception-ResNet-v2 found that VGGNet-19 learning by transfer learning has the highest recognition rate. The size of this model is only 160.6 MB comparing with Inception-ResNet-v2 which is 437.5MB. The number of parameters comparison, VGGNet-19 has only 20M parameters which is almost 3 times less. Finally, when comparing the test speed, VGGNet-19 speed was 0.0014 second per image, while Inception-ResNet-v2 speed was 0.0043 second per image. We can conclude that VGGNet-19 speed was up to 3 times faster.

Surprisingly, InceptionResNet-v2 architecture [20] tested with ImageNet dataset achieved 5.7% higher efficiency than VGGNet-19. In contrast, when it was tested with the THI-C68 dataset, which is Thai character, we found that VGGNet with transfer learning achieved a higher accuracy rate. Therefore, in this experiment VGGNet-19 is an appropriate model to solve the problems of "*Thai Handwritten Character Recognition*" due to the smaller size model, less number of parameter, faster speed in the experiment, and highest accuracy rate. The most important is the model that achieved the highest accuracy rate.

6. CONCLUSIONS

This research compares CNN Architectures that are effective in recognizing Thai handwritten characters with a high rate of recognition. The two models are VGGNet-19 and Inception-ResNet-v2 architectures. Both models were evaluated with THI-C68 dataset. In this experiment, the learning method was determined in two types, which are training from scratch and transfer learning. Transfer learning is a way to reduce learning time and increasing the efficiency of recognition. The research has shown that VGGNet-19 architecture with transfer learning has an accuracy rate at 99.20%. In addition, it was higher than Inception-ResNet-v2 architecture. In this regard, VGGNet-19 architecture is a deep learning that has only 19 layers. It has been designed to be stacked together due to make it easier to learn from the network and for increasing the recognition speed.

In future work, researchers will design deep CNN architecture that reduces the number of parameters and reduce learning time. However, the quality must still be equivalent or better performance than with the previous architecture and it will be tested with handwriting characters in other languages such as Bangla, Lanna etc.

7. REFERENCES

[1] Deng, J., Dong, W., Socher, R., Li, L.-J., Kai Li and Li Fei-Fei 2009. ImageNet: A large-scale hierarchical image database. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (Jun. 2009), 248–255.

[2] He, K., Zhang, X., Ren, S. and Sun, J. 2016. Deep Residual Learning for Image Recognition. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (Dec. 2016), 770–778.

[3] Hu, J., Shen, L. and Sun, G. 2018. Squeeze-and-Excitation Networks. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (Dec. 2018), 7132–7141.

[4] Huang, G., Liu, Z., Maaten, L. van der and Weinberger, K.Q. 2017. Densely Connected Convolutional Networks. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (Nov. 2017), 2261–2269.

[5] Inkeaw, P., Bootkrajang, J., Marukatat, S., Gonçalves, T. and Chaijaruwanich, J. 2019. Recognition of Similar Characters using Gradient Features of Discriminative Regions. *Expert Systems with Applications*. 134, (Nov. 2019), 120–137.

[6] Ioffe, S. and Szegedy, C. 2015. Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift. *The 32nd International Conference on International Conference on Machine Learning* (2015), 448–456.

[7] Joseph, F.J.J. and Anantaprayoon, P. 2018. Offline Handwritten Thai Character Recognition Using Single Tier Classifier and Local Features. *The 3rd International Conference on Information Technology (InCIT)* (Oct. 2018), 8–11.

[8] Kim, I.J. and Xie, X. 2014. Handwritten Hangul Recognition using Deep Convolutional Neural Networks. *International Journal on Document Analysis and Recognition*. 18, 1 (2014), 1–13.

[9] Krizhevsky, A., Sutskever, I. and Hinton, G.E. 2012. ImageNet Classification with Deep Convolutional Neural Networks. *Advances in Neural Information Processing Systems 25* (2012), 1090–1098.

[10] Lecun, Y., Bengio, Y. and Hinton, G. 2015. Deep learning. *Nature*. 521, 7553 (May 2015), 436–444.

[11] Lecun, Y., Bottou, L., Bengio, Y. and Haffner, P. 1998. Gradient-Based Learning Applied to Document Recognition. *IEEE*. 86, 11 (1998), 2278–2324.

[12] Marinai, S. 2008. Introduction to Document Analysis and Recognition. *Studies in Computational Intelligence*. Springer Verlag. 1–20.

[13] Nair, V. and Hinton, G.E. 2010. Rectified Linear Units Improve Restricted Boltzmann Machines Vinod Nair. *The 27th International Conference on Machine Learning* (2010), 807–814.

[14] Okafor, E., Pawara, P., Karaaba, F., Surinta, O., Codreanu, V., Schomaker, L. and Wiering, M. 2016. Comparative Study between Deep Learning and Bag of Visual Words for Wild-Animal Recognition. *IEEE Symposium Series on Computational Intelligence (SSCI)* (Dec. 2016), 1–8.

[15] Ruder, S. 2016. An Overview of Gradient Descent Optimization Algorithms. (Sep. 2016), 1–14.

[16] Sandler, M., Howard, A., Zhu, M., Zhmoginov, A. and Chen, L.C. 2018. MobileNetV2: Inverted Residuals and Linear Bottlenecks. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (Dec. 2018), 4510–4520.

[17] Sawada, Y. and Kozuka, K. 2016. Whole Layers Transfer Learning of Deep Neural Networks for a Small Scale Dataset. *International Journal of Machine Learning and Computing*. 6, 1 (2016), 27–31.

[18] Simonyan, K. and Zisserman, A. 2015. Very Deep Convolutional Networks for Large-Scale Image Recognition. *3rd International Conference on Learning Representations (ICLR)*.

[19] Surinta, O., Karaaba, M.F., Schomaker, L.R.B. and Wiering, M.A. 2015. Recognition of handwritten characters using local gradient feature descriptors. *Engineering Applications of Artificial Intelligence*. 45, (Oct. 2015), 405–414.

[20] Szegedy, C., Ioffe, S., Vanhoucke, V. and Alemi, A. 2017. Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning. *The Thirty-First AAAI Conference on Artificial Intelligence* (2017), 4278–4284.

[21] Wang, B. and Klabjan, D. 2017. Regularization for Unsupervised Deep Neural Nets. *The Thirty-First AAAI Conference on Artificial Intelligence* (Aug. 2017), 2681–2687.

Cross-Sectional Dual Camera Diameter Measurement for Automatic Mangosteen Sorting

Tony K. Hariadi
Dept. of Electrical Engineering
Universitas Muhammadiyah Yogyakarta
Indonesia
tonykhariadi@umy.ac.id

ABSTRACT
Mangosteen has been one of the leading fruit export and production in Indonesia. Due to different demand and harvesting processes, it is classified into several categories according to its external condition, including size and ripeness, stage 1 to 6. Its shape is not round but elliptical on one side. Therefore, it needs cautious measurement to determine the diameter size. This project aims at developing an automatic size calculator for mangosteen using dual camera. Two cameras were needed to do the cross-sectional measurement, then image processing analysis based on Simpson's algorithm calculated the diameter. Statistical analysis; maximum, minimum and average calculation was used to determine the optimum measurement result.

CCS Concepts
• Computing methodologies→Computer vision.

Keywords
Machine vision; mangosteen grading; diameter measurement; image processing for agriculture; precision farming.

1. INTRODUCTION
Indonesia has been one of the major fruit exporters due to its geographical condition and land fertility. According to the Indonesian Central Bureau of Statistics, fruit export has increased annually. Indonesia's fruit export was roughly 33.68 tons with a market value of US$ 19.95 million in 2017. Mangosteen was the third-largest export commodity that contributed nearly 15% of the market value. It indicates that mangosteens demand is high. China, Oman, and Malaysia were the top three of the target market of fruit from Indonesia, which contributed almost 40% of the total export values [1].

Most of the fruit production in Indonesia was done manually, while some automated fruit processing was involved in large fruit industries. Fruit production includes farming, harvesting, sorting, packaging, and transporting to the marketplace. These processes should meet the national or international standard for exporting [2]. The manual process lacks accuracy and speed; therefore, the need for automated process has increased. For traditional farmers and small fruit industries, large automated machine is too expensive. This project aims to overcome the need for automated fruit process on a small scale and low-cost environment [3].

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388189

2. PREVIOUS RESEARCH
Many methods for fruit grading based on ripeness and surface quality have been developed. The methods involve image processing technique to increase grading accuracy on vegetable and fruit such as starfruit, strawberry, papaya, orange, and apple [4] [5] [6] [7]. Area calculation methods have also been developed using image processing technique to indicate leaf area using a smartphone camera. Leaf area calculation using a smartphone camera resulted in 99% accuracy [8]. Other research was done using a fuzzy algorithm for fruit detection and also for nylon measurement which has resulted in 95% accuracy [9] [10]

The methods for quality inspection were mostly done on a still object. While measurement on moving objects was not adequately investigated for low-cost application. Laser technology was introduced for 2D objects modeling using a graph and vector algorithm on a moving robot [11]. Failure of precision measurement or inspection mostly due to inadequate feature extraction technology [12].

2.1 Machine Vision Technology
Agricultural industries involve machine vision technology for fruit grading, land inspection, and other applications. Hyperspectral, infrared, and thermal camera have been used alongside regular industrial camera [13]. Hyperspectral and multispectral imaging can give a different or maybe better perspective on image analysis. However, these technologies need high investment. While a regular camera, when combined with a precise algorithm, will also result in an adequate to high precision measurement [14]. Oher application of computer vision has also been introduced for cell localization [15]

2.2 Image Processing Technology
Image processing technology has been used in many applications such as medicine, agriculture, engineering, and many other fields of interest. Digital image processing can be used to extract signature, quantification, edge detection, or filter of an image [16]. Some of the image processing algorithms used in this research were segmentation and thresholding. Segmentation is one of the most important functions in image processing. Its tasks are to divide an image into many uniform image divisions that have the same characteristic. Thresholding is used to quantify image into a histogram for separation and edge detection [17].

3. METHODOLOGY

This project aimed to build a low-cost automatic mangosteen sorting machine based on diameter. Two cameras were used for visual inspection. The shape of the mangosteen is not round from any angle. Its shape is different when viewed from above and form side. Hence, it results in different diameter measurement if it is not carefully inspected.

Mangosteen always comes with a crown as part of the fruit, also contributes to its quality (fig. 1). From the top side, it looks round without crown. Camera vision captures the crown as part of the fruit and will calculate it as the body of the fruit. Therefore, the cross-sectional measurement was used to calculate the length of the fruit. The two cameras were used for calculation conformity, which involved statistical methods. They were also needed when the fruit was tilted or lied on one side.

Figure 1. Mangosteen shape.

3.1 Hardware Design

Mangosteen image acquisition was done in a specific chamber that was designed with uniformly light, and it allows movement of fruit passing the chamber. LED bulbs with natural lighting condition with 6500K color temperature was used to get the best image acquisition [18]. Two cameras were placed on the top and the side of the chamber for two cross-sectional image analysis.

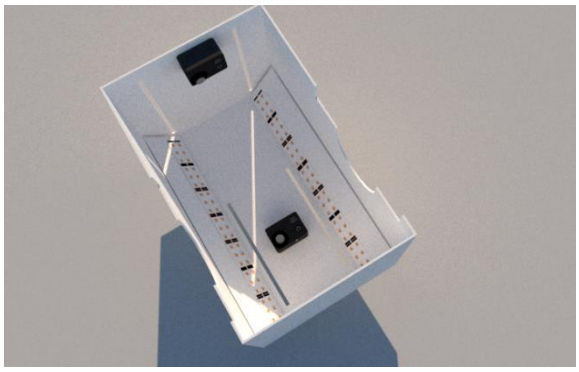


Figure 2. Chamber with LED and cameras (seen from bottom side).

Fruit entered one side of the chamber and triggered a sensor to activate the cameras. Both cameras captured the picture. Furthermore, image processing calculated the diameter of the fruit. Outside the chamber, a special device was designed to sort the fruit to its diameter group based on the information sent by the computer.

3.2 Software Design

Image thresholding and pixel segmentation were used to calculate the diameter of the fruit. The image was converted into black and white based on the histogram (HSV) extracted from the image using the thresholding technique (fig. 3). This process returned an image separation between background and object of interest.

Diameter measurement in this technique was a calculation window on the highest horizontal and vertical counts. The basic unit called window, in this case, was the pixel size. It needed to be converted into metric which is millimeter. This process was done during calibration. Fig. 4 presents the cross-sectional measurement where Dy indicates the vertical diameter, and Dx is the horizontal diameter. The area of interest (measured diameter) was only on the body of the fruit which was indicated by the meshed area. Each box in the meshed area represented a specific length for pixel to metric conversion.

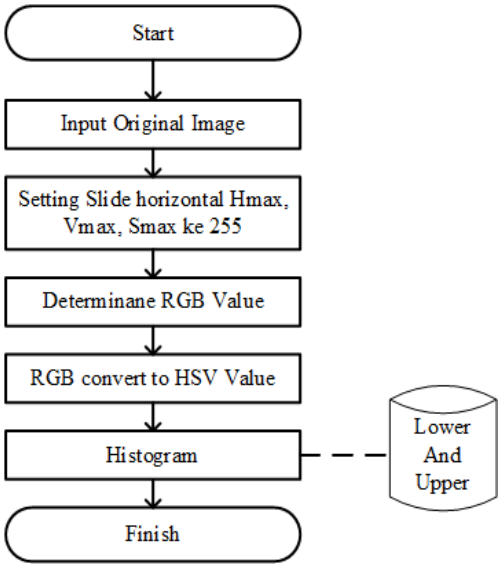


Figure 3. HSV conversion.

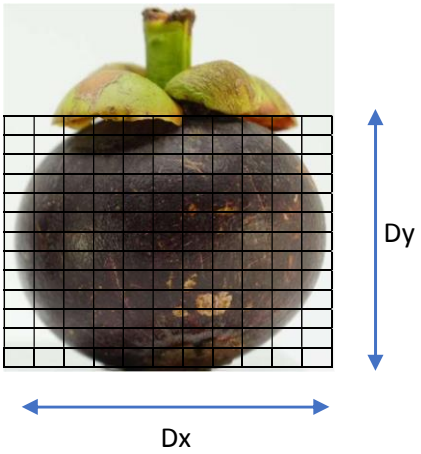


Figure 4. Horizontal and vertical measurement.

A significant value of the pixel was added when the white pixel was found. The algorithm of the size measurement was as follows:

- *Determine C as window size in millimeter*
- *Determine n as max count of horizontal pixel*
- *Determine d as the diameter*
- *Take row 1 to m*
- *Take column 1 to n, evaluate pixel color*
- *If pixel color is black then D=D+0*
- *If pixel color is white then D=D+1*
- *Repeat until n*
- *Repeat until m*
- *Found Diameter as D*C*

The same algorithm applied to the vertical measurement. At the end of the analysis, four diameter values were defined, two counts from the top camera and two counts from the bottom camera. Further statistical analysis was done to determine the final diameter result using average and maximum values. Maximum accuracy was evaluated after comparing the result from both methods.

3.3 Calibration

Any measurement device needs to be calibrated to give the smallest error. Calibration for this project was done to provide a scale measurement for one pixel as the smallest measurement window. This method used one-point calibration where higher accuracy result was expected within a specific range of deviation from the calibrated value [19] [20]. Mangosteen size ranged from 40mm to 80mm. Therefore, the device was calibrated with approximately 47mm, 52mm, and 63mm to evaluate the measurement fall-off.

4. RESULT AND ANALYSIS

4.1 Static Measurement

Measurement experiment was done using several objects and was repeated several times. Figures below demonstrate the measurement result where accuracy is shown in y-axis in % and x-axis indicates the real diameter of the object under evaluation. Actual diameters were acquired using a micrometer. Two cameras were used for image acquisition and were called as Top and Side Cam. Whilst the cross sectional orientation of the image were notified as H (horizontal or X axis) and V (vertical or Y axis).

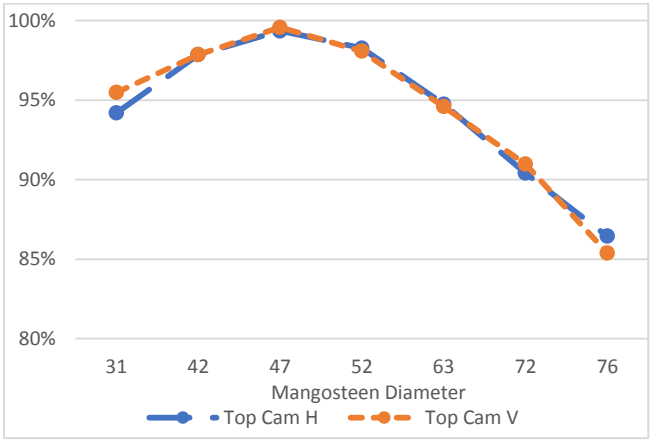


Figure 5. Accuracy graph for top camera measurement with 47mm calibration.

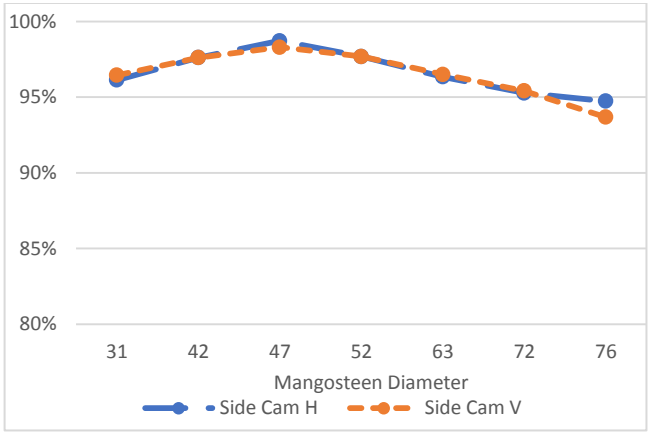


Figure 6. Accuracy graph for side camera measurement with 47mm calibration.

Figure 5 and 6 demonstrated the measurement result with calibration at 47mm. The measurement indicated high accuracy for fruit size around 47mm. Accuracy declined when fruit size deviated higher and lower the calibrated size. A decline occurred when the measured fruit was smaller than 31mm and bigger than 63mm, where the accuracy was less than 95%.

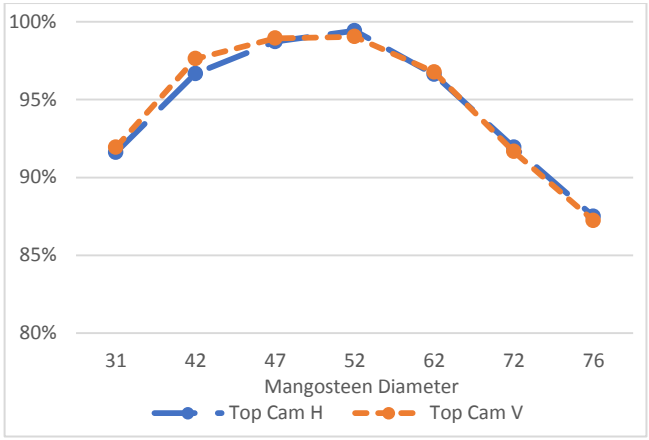


Figure 7. Accuracy graph for top camera measurement with 52mm calibration.

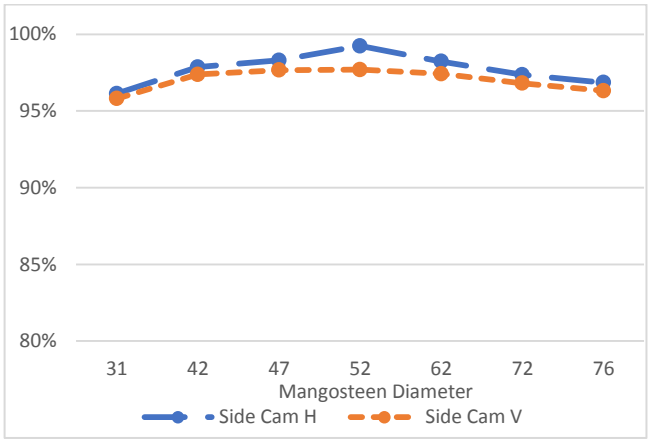


Figure 8. Accuracy graph for side camera measurement with 52mm calibration.

Figure 7 and 8 indicated the measurement result of 52mm calibration. As expected, the accuracy was also high when the measured fruit size similar to the calibrated size. A decline occurred when the measured fruit size was smaller than 38mm and bigger than 64mm. Side camera measurement indicated higher accuracy result with more than 95% accuracy among the entire measurement.

The results of the 63mm measurement were demonstrated in figures 9 and 10. The graph would indicate a decline if the size of the measured fruit was smaller than the calibrated fruit size since most mangosteen were no bigger than 80mm. The chart indicates that a decline in measurement accuracy happened when the fruit was smaller than 47mm.

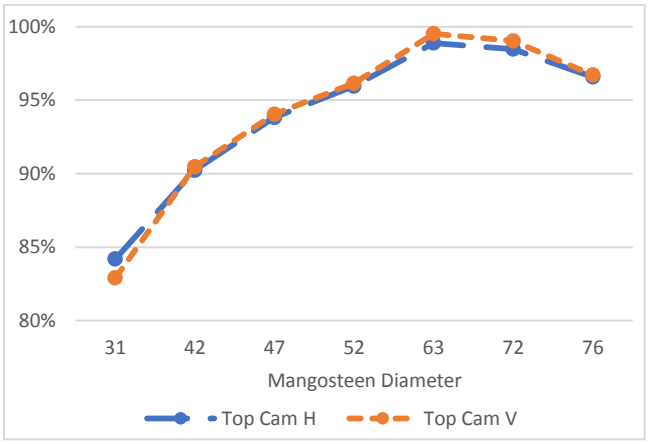


Figure 9. Accuracy graph for top camera measurement with 63mm calibration.

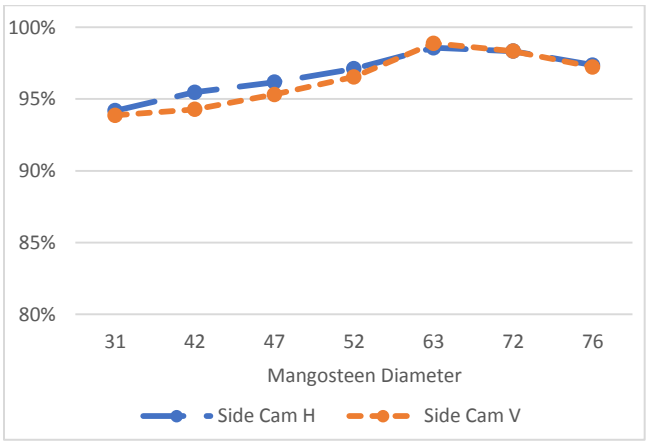


Figure 10. Accuracy graph for side camera measurement with 63mm calibration.

The graphs indicate a high accuracy result. Significant measurement errors occurred when the actual size of the measured object was highly deviated from the calibration value. High accuracy of more than 95% was acquired when the measured objects lie within the range of ± 20mm from the size of the calibrated objects. Those measurement results indicated that the methodology was reliable for diameter measurement. The next step was to put the method in the real simulation of moving mangosteen measurement.

4.2 Moving Object Classification

As aforementioned, this project aims to classify mangosteen based on diameter. In this step, the mangosteen was conveyed into the measurement chamber, while at the end, a specially designed tool would separate it into designated container based on diameter. The statistical features of average, min, and max were involved for comparison.

Thirty mangosteens of different sizes: 10 sized below 55mm, ten sized between 55-65mm and ten sized above 65mm were classified in this experiment. The measurement was done several times to increase samples and to achieve the best accuracy measurement. The result of mangosteen classification is shown below. True measurement data was presented in table 1.

Table 1. Percentage of true measurement

Statistic Method	Mangosteen Diameter		
	<47mm	*55-65mm*	*>65*
Dmin	69%	83%	77%
Dmak	70%	57%	53%
Average	82%	71%	67%

The following graph presents the measurement results distinctively:

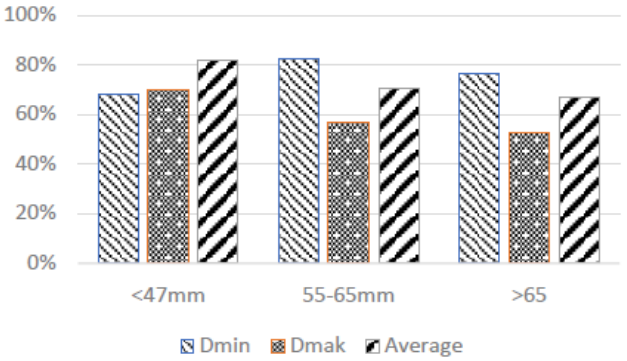


Figure 11. True measurement graph.

The graph in figure 11, indicated that calculation using Dmin, where least measurement of the four cross-sectional results was taken as the final diameter, resulted in higher percentage in medium mangosteen (83%) and large mangosteen (77%). Whereas in small mangosteen, the average method resulted in the highest true measurement of 82%. For medium and large mangosteen, the crown contributed significant length for the total measured pixel calculated by the image processing. Therefore, the average or max method resulted in a less accurate measurement.

Movement of the object conveyed into the chamber also contributed to the error measurement. The fruit could change position or rolled that affected the image acquisition.

5. CONCLUSION

Measurement method in this project indicated high accuracy result with only 1% error. The use of dual camera also increased the range of accuracy for different object sizes. Deviation of approximately 30% smaller or larger than the calibrated size indicated 95% of accuracy. However, a significant decrease in

accuracy indicated that in field test using the conveyed object (moving object), the highest true measurement merely recorded 83% of accuracy.

To increase the accuracy in the field testing, the conveyor system needs to be designed to better hold the object or fruit from rolling or shifting as it will affect the image acquisition process.

6. REFERENCES

[1] Sub-directorate of Horticulture Statistics, Statistics of Annual Fruit and Vegetable Plants Indonesia 2017, Jakarta: Statistics Indonesia, 2018.

[2] Badan Standardisasi Nasional, "Manggis," Badan Standardisasi Nasional, Jakarta, 2009.

[3] E. Setiawan and R. Poerwanto, "Produktivitas dan Kualitas Buah Manggis (Garciana manggostana L.) di Purwakarta," *Agrovigor*, vol. 1, no. 1, pp. 12-20, 2008.

[4] M. M. Mokji and S. A. R. Abu Bakar, "Starfruit Classification Based on Linear Hue Computation," *Elektrika*, vol. 9, no. 2, pp. 14-19, 2007.

[5] O. Mahendra, H. F. Pardede, R. Sustika and R. B. S. Kusumo, "Comparison of Features for Strawberry Grading Classification with Novel Dataset," in *International Conference on Computer, Control, Informatics and its Applications (IC3INA)*, 2018.

[6] P. Baranowski, W. Mazurek, J. Wozniak and U. Majewska, "Detection of early bruises in apples using hyperspectral data and thermal imaging," *Journal of Food Engineering*, vol. 110, no. 3, pp. 345-355, 2012.

[7] S. Riyadi, A. J. Ishak, M. M. Mustafa and A. Hussai, "Wavelet-Based Feature Extraction Technique For Fruit Shape," in *International Symposium on Mechatronics and its Application*, Amman, 2008.

[8] T. K. Hariadi, S. Riyadi and Z. Fadholi, "Development of Leaf Area Meter Using Open CV for Smartphone Application," *Telkomnika* , vol. 16, no. 4, pp. 1857-1863, 2018.

[9] B. Suksawat, "Diameter Error Prediction Using Fuzzy Logic for Cast Nylon 6 Turning Operation," in *International Conference on Future Information Engineering*, Thailand, 2014.

[10] M. Sharma , V. P. N. Jaiswal and A. Goyal, "Fruit Detection with Multiple Features using Fuzzy Logic," *International Journal of Advance Research in Computer Science and Software Engineering*, vol. 3, no. 11, pp. 856-861, 2013.

[11] Iswanto, O. Wahyunggoro and A. I. Cahyadi, "3D Object Modeling Using Data Fusion from Laser Sensor," in *Advances of Science and Technology for Society*, 2016.

[12] C. Zheng, H. -J. He and D. -W. Sun, "Chapter 3 - Object Measurement Methods," in *Computer Vision Technology for Food Quality Evaluation (Second Edition)*, Academic press, 2016, pp. 65-85.

[13] Y. R. Chen, K. Chao and M. S. Kim, "Machine vision technology for agricultural applications," *Agriculture*, vol. 36, no. 2-3, pp. 173-191, 2002.

[14] T. K. Hariadi, H. Zidni, K. T. Putra and S. Riyadi, "High Accuracy Real Time Machine Vision for Diameter Measurement Using Simpson Algorithm," in *The 9th International Conference on Information and Communication Technology Convergence*, Jeju, 2018.

[15] E. Bostanci and B. Bostanci, "Object Localization and Spatial Analysis Using Computer Vision," *International Journal of Machine Learning and Computing*, vol. 1, no. 2, pp. 120-124, 2011.

[16] X. Liu and D. Zhao, "Image Processing Technology and Its Application on Precision Stage. In: Jin D., Lin S. (eds)," in *Advances in Mechanical and Electronic Engineering. Lecture Notes in Electrical Engineering, vol 178*, Heidelberg, Springer, Berlin, 2013, pp. 349-352.

[17] T. Acharya and A. K. Ray, Image Processing Principles and Applications, New Jersey: John Wiley & Sons, Inc., Hoboken, 2005.

[18] Y. Zhang, Y. Gao, Y. He, Y. Shi and K. Liang, "Research on the Color Temperature & White Balance for Multimedia Sensor," *Procedia Computer Science*, vol. 107, pp. 878-884, 2017.

[19] S. Carmignato, "Calibration," in *The International Academy for Produ, Laperrière L., Reinhart G. (eds) CIRP Encyclopedia of Production Engineering*, Heidelberg, Springer, Berlin, 2014.

[20] Z. Mahmoudi, M. D. Johansen and J. S. Christiansen, "Comparison Between One-Point Calibration and Two-Point Calibration Approaches in a Continuous Glucose Monitoring Algorithm," *Journal of diabetes science and technology*, vol. 8, no. 4, 2014.

[21] C. Zheng, H. -J. He and D. -W. Sun, "Chapter 3 - Object Measurement Methods," in *Computer Vision Technology for Food Quality Evaluation (Second Edition)*, Academic Press, 2016, pp. 65-85.

Comparative Study between Texture Feature and Local Feature Descriptors for Silk Fabric Pattern Image Recognition

Thananchai Khamket
Applied Informatics Group
Department of Information Technology
Faculty of Informatics, Mahasarakham University
Maha Sarakham, Thailand
thananchai.k@msu.ac.th

Olarik Surinta
Multi-agent Intelligent Simulation Laboratory (MISL)
Department of Information Technology
Faculty of Informatics, Mahasarakham University
Maha Sarakham, Thailand
Olarik.s@msu.ac.th

ABSTRACT
Thai silk fabrics have unique patterns in different regions of Thailand. The designers may have been inspired and took ideas from the natural environment to create new silk patterns. Hence, many new silk patterns are modified from the original silk pattern. It is challenging for people to recognize a pattern without any prior knowledge and expertise. This paper aims to present a comparative study between texture feature and local feature descriptor for silk pattern image recognition. First, two feature extraction techniques: texture feature and local feature descriptors are proposed to create robustness features from sub-regions that are divided by the grid-based method. Second, the robust features are then classified using the well-known and effective classifier algorithms: K-nearest neighbor (KNN) and support vector machine (SVM) with the radial basis function. We experimented with silk pattern image recognition on two silk fabric pattern image datasets: the Silk-Pattern and Silk-Diff-Pattern. The evaluation results show that the texture feature called the local binary pattern (LBP) when combined with the KNN and SVM algorithms outperforms other feature extraction methods, even deep learning architectures.

CCS Concepts
• Computing methodologies→Image representation • Information systems→Image search • Computing methodologies→Support vector machines.

Keywords
Texture feature; Local feature descriptor; Silk fabric pattern image recognition; Support vector making; K-nearest neighbor.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388201

1. INTRODUCTION
In Thailand, people wear silk fabric because silk fibers are tough, lightweight, and can be worn in all weather conditions. People tend to wear a dress that sewn with silk fibers only during celebrations or luxury activities because silk fabric is difficult to maintain and expensive. The pattern design of Thai silk is an identity, so each region has its pattern and style. However, new silk patterns are not much different from the originals due to them being designed and modified from the previous patterns. They are difficult to identify without any knowledge. Maybe only experts of the silk patterns can identify them.

The researchers proposed methods of silk image retrieval and classification using local descriptor and texture feature techniques [7, 19]. Raksaard and Surinta [19] provided the Silk-Pattern dataset to evaluate the image retrieval algorithms. The Silk-Pattern dataset used in the experiments, including 300 silk images in 10 categories, with 30 images per category. The challenge of the Silk-Pattern dataset is to classify the silk pattern in which the test set is randomly cropped 30 and 40% from the whole image. Traditional machine learning techniques and deep learning techniques are proposed to evaluate the performance of silk image retrieval algorithms. As a result, the combination of the histogram of oriented gradients (HOG) and one-nearest neighbor (1NN) performed better than the deep learning techniques (LeNet and AlexNet).

Dittakan and Theera-Ampornpunt [7] proposed texture analysis based on a local binary pattern method: rotated local binary pattern (RLBP) and complete local binary pattern (CLBP), to create the feature vector. Then, three feature selection techniques: chi-squared, information gain, and gain ratio were proposed to select the optimal features. Furthermore, seven classification techniques were used to evaluate the performance of each technique.

Contribution: To address the silk pattern classification problems, as our main contribution, a grid-based method is proposed that uses feature vectors extracted from local binary patterns (LBP) to classify silk fabric pattern images. We evaluate the accuracy result of different techniques on two silk fabric pattern image datasets called a Silk-Pattern dataset [19] and Silk-Diff-Pattern dataset (see Figure 3). In the experiments, we compare the accuracy results between texture feature called local binary patterns (LBP) method and local feature descriptors: Histogram of oriented gradients (HOG) and scale invariant feature transform (SIFT). Additionally, the results also show that the LBP method, when combined with the support vector machine and K-nearest neighbor methods, outperform the convolutional neural network architectures: LeNet and AlexNet architectures.

Paper outline: The remainder of this paper is organized as follows. In Section 2, the silk fabric pattern image recognition approaches are described. In Section 3, we explain a detailed of the silk fabric pattern image dataset. Experimental results are presented in Section 4. Conclusions and suggestions for future work are considered in Section 5.

2. SILK FABRIC PATTERN IMAGE RECOGNITION METHODS

In this research, first, we propose a grid-based method, which has been successful in many areas, such as face recognition [12], people tracking [4], and fast image retrieval [5], for diving the fabric silk image into small regions. Second, we compare two well-known feature extraction techniques: the texture feature and local feature descriptor due to the study of the robustness and effectiveness. Each feature extraction technique is proposed to calculate a feature from a small region. Third, we concatenate the features from each region and use them as the robust feature vector. Finally, two classifiers called the K-nearest neighbor (KNN) and the support vector machine (SVM) [22] methods are used to create a model and classification process. The method of computing local binary pattern (LBP) using the grid-based method is shown in Figure 1.

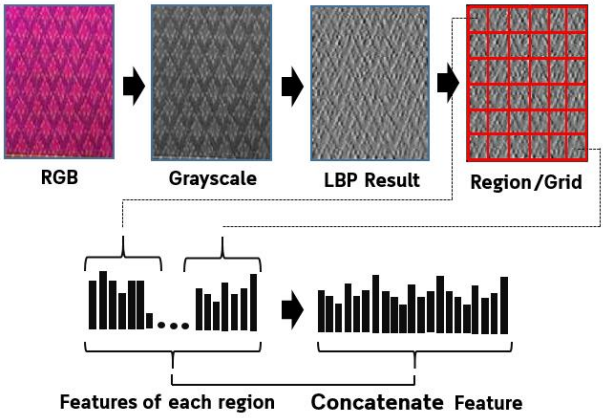


Figure 1. Method of computing the local binary pattern feature from the silk pattern image.

2.1 Texture Feature

Texture features are widely used in many pattern recognition applications such as Melanoma classification [13], hand detection system [16], remote sensing, biomedical imaging [9], character recognition [14], signature recognition [2], and face recognition [11]. The texture always contains information such as colors, intensities, and structure that are represented in the spatial domain. In this research, we focused on the analysis of local structures of silk fabric image using a local binary pattern method (LBP) [23].

Local Binary Pattern (LBP): Wang and He [23] originally proposed the local binary pattern (LBP) for texture spectrum classification. Firstly, the spectrum image was converted to a gray image and resized to 256x256 pixels to calculate the texture spectrum. Secondly, the sub-images of 30x30 pixels were randomly selected. Then, the matrix of 3x3 pixels slides with overlap across the sub-image. Thirdly, the neighborhood pixels around the center pixel of the matrix are transformed into a texture unit with a value of 0, 1, and 2. Finally, the absolute difference values were calculated.

Ojala et al. [18] proposed a robust two-level version of LBP, in which the number of possible texture units was reduced from 6,561 to only 256 (2^8 when 8 is a neighbor pixels). With this method, the matrix size of 3x3 pixels was used. Then, the pixel values around the center pixel of the matrix were transformed into the binary value with a value of 0 and 1 and then considered only the value of 1. From the first to the last neighborhood pixel, the values were calculated as 2^n, where $n = 0,1,..,7$. Finally, the values of the neighborhood pixels were summed and used as a texture unit.

2.2 Local Feature Descriptors

Initially, the local feature descriptors such as the scale-invariant feature transform (SIFT) [15] are proposed for image matching and also applied to image stitching. The local features are used to represent neighborhood pixels of interest points in an image such as edge and corner, called keypoints. In this method, the gradient orientations and magnitudes are computed from each keypoint and count to the orientation histogram. Consequently, the orientation histogram from keypoints is then compared between the two images by the distance function. Hence, the closest distance is the most matching.

In this paper, we use local feature descriptors SIFT and the histogram of oriented gradients (HOG) [6] methods as the representation of the silk fabric image.

2.2.1 Histogram of Oriented Gradients (HOG)

Dalal and Triggs [6] proposed the histogram of oriented gradients (HOG) method for detecting humans in images. Nowadays, it has become a well-known and most successful method in object detection, such as human detection, object tracking and motion detection [1, 8]. In this method, first, the image is transformed into the edge image using a simple convolution kernel, such as Sobel. Second, we divide the image into small blocks. Third, the gradient orientation and magnitudes are computed from each block and stored into orientation bins. Finally, the orientation bins are used for the local feature to create a model using the linear support vector machine (SVM) technique. In the detection process, the detector windows in various sizes are scanned through to the image and then fed the HOG feature to the linear SVM for human classification. In this paper, we extracted HOG features from all grids on the silk fabric image.

The equation of the HOG method [3] can be written as follows:

$$\Phi_f(\mathrm{X}) = \mathbf{Db} * \left[(g_x * \mathbf{X}) \odot (g_y * \mathbf{X})\right] \quad (1)$$

where

X is an image that convolved with the simple kernel g in the horizontal g_x and vertical g_y directions.

Db is orientation bins which are the weighted vote of the gradient orientation and magnitude and normalized using L2-Norm [6].

The g_x and g_y are calculated as follows:

$$g_x = f(x+1, y) - f(x-1, y) \quad (2)$$
$$g_y = f(x, y+1) - f(x, y-1)$$

The gradient magnitude (m) and orientation (θ) are computed as follows:

$$m(x,y) = \sqrt{G_x^2 + G_y^2} \quad (3)$$

$$\theta(x,y) = \tan^{-1}\frac{G_y}{G_x} \quad (4)$$

2.2.2 Scale-Invariant Feature Transform (SIFT)

Lowe [15] invented a method that extracted the distinctive features from scale-invariant keypoints, called the scale-invariant feature transform (SIFT). The features are calculated on the candidate invariant keypoints. Hence, the SIFT features are invariant to different image sizes and orientations.

The SIFT features are computed from each grid due to the grid-based method. The input image is computed using the Gaussian kernel:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \quad (5)$$

where

$I(x, y)$ is the pixel value at location x, y of image I

$G(x, y, \sigma)$ is the Gaussian kernel and σ is the width of the Gaussian kernel

$*$ is the convolution operation

The G_x and G_y are calculated as follows:

$$G_x = L(x+1, y, \sigma) - L(x-1, y, \sigma) \quad (6)$$
$$G_y = L(x, y+1, \sigma) - L(x, y-1, \sigma)$$

where G_x and G_y are the horizontal and vertical components of the gradients.

The gradient orientation $\theta(x, y)$ and magnitude $m(x, y)$ are computed from the image $L(x, y, \sigma)$ according to Equation (3) and (4).

Then, the region of each keypoint is divided into 4x4 blocks, and each block contains eight orientations. For one key point, the SIFT feature vector contains 128 dimensions.

2.3 Classification Algorithms

In this section, we briefly explain the basic concepts of K-nearest neighbors and the support vector machine algorithms.

2.3.1 K-Nearest Neighbors Algorithm

The K-Nearest neighbors (KNN) algorithm is a supervised learning technique in machine learning. In this method, we compute the distance value between the unknown data and all training data to find the nearest member using a distance function such as the Euclidean function [10, 20]. Euclidean distance function is computed as follows:

$$d(x, y) = \sqrt{\sum_{i=1}^{N} (x_i - y_i)^2} \quad (7)$$

where N is the number of features. x, y is the data in the training data, and y is the unknown data.

The K nearest members are considered as the candidate members, where K is an odd number. Furthermore, the majority vote is applied to collect the category of candidate members. Finally, the unknown data is assigned to be categorized according to the most vote category. Given an unknown data x_q to be classified. Let $x_1, .., x_k$ denote the k nearest members from training data $(x, f(x))$ that are nearest to x_q. The KNN algorithm [17] is computed as follows:

$$\hat{f}(x_q) = argmax \sum_{i=1}^{k} \delta(v, f(x_i)) \quad (8)$$

where $\delta(a, b) = 1$ if $a = b$, otherwise $\delta(a, b) = 0$.

2.3.2 Support Vector Machine

Vapnik [22] invented the support vector machine (SVM) algorithm for linear binary classification problem. The SVM algorithm finds out the optimal hyperplane, which the largest decision boundary between the two classes, that separates all data points. The training set is $(\mathbf{x}_i, y_i), i = 1, \ldots, l$ where $\mathbf{x}_i \in \mathbf{R}^n$ with labels $y_i \in \{+1, -1\}$ [21]. The optimal hyperplane is defined as follows:

$$\mathbf{W}^T \mathbf{X} + w_0 = 0 \quad (9)$$

where $\mathbf{W}$ is the weight vector. $\mathbf{W}^T \mathbf{X} + w_0 > 0$ for $y = +1$ and $\mathbf{W}^T \mathbf{X} + w_0 < 0$ for $y = -1$.

To deal with the non-linear problem, many kernel functions such as radial basis function (RBF) and polynomial kernel are proposed. In this paper, we choose the RBF kernel to handle the non-linear problem. The RBF kernel is defined as follows:

$$K(x_i, x_j) = exp\left[-\gamma \left\| x_i - x_j \right\|^2\right] \quad (10)$$

where γ is the RBF kernel parameter.

$\left\| x_i - x_j \right\|^2$ is the Euclidean distance from the set of feature points x_j

3. THE SILK FABRIC PATTERN IMAGE DATASET

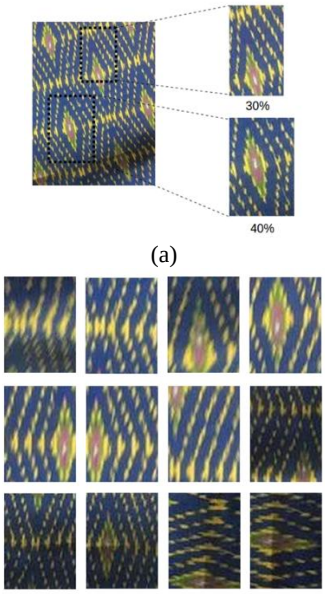
Raksaard [19] introduced a new dataset of Thai silk patterns. The objective of this dataset was to evaluate the retrieval systems including feature extraction method, image classification, and retrieval. The Silk-Pattern dataset was collected from a silk shop in Maha Sarakham, located in the northeast of Thailand. Thai silk fabric includes two parts; the main pattern and the bottom of the fabric, called fabric feet, as shown in Figure 2. In this dataset, the researcher decided to use only the main pattern of the silk fabric, as shown in Figure 2(b).

Figure 2. Illustration of the a) Thai silk fabric, b) main pattern and c) fabric feet.

The Silk-pattern dataset consists of ten Thai silk pattern classes and contains 300 images captured using a smartphone to illustrate the silk fabric from different orientations. The Silk-Pattern images are stored in the RGB color space with a size of 450x650 pixels. Sample images of the Silk-Pattern dataset are illustrated in Figure 3.

In the Silk-Pattern dataset, the test set is randomly cropped only 30% and 40% from the whole silk fabric pattern image, as shown in Figure 4(a) and cropped three times from one silk image. The Silk-Pattern images consist of 300 training samples, 900 test samples of cropping 30% (Crop-30), and 900 test samples of cropping 40% (Crop-40). Figure 4(b) illustrates the sample images of the Crop-30.

Figure 3. Illustration of the training set of the Silk-Pattern dataset.



(a)

(b)

Figure 4. Illustration of the test set of the Silk-Pattern dataset. (a) randomly cropped 30% and 40%. (b) The sample images with cropped 30%.

In addition, we introduce a new dataset of Thai silk pattern images, which is more complex and challenging, called the Silk-Diff-Pattern dataset. The advantage of our new dataset is that the silk pattern images include all components of the silk pattern; pattern and fabric feet. Examples of the Silk-Diff-Pattern dataset are shown in Figure 5. Our dataset also has ten classes and contains 300 images. We used the same process as with the Silk-Pattern dataset to collect the test data. The test data consists of two sets; 900 samples of Crop-30 and 900 samples of Crop-40. Furthermore, we carefully checked all the test images. Also, the test image contained only the pattern of the silk fabric.

Figure 5. Illustration of the training set of the Silk-Diff-Pattern dataset.

4. EXPERIMENTAL RESULTS

We briefly explain the experimental setups used for the dataset. After that, the results are presented and discussed.

To provide data for the silk fabric image recognition, we used two silk datasets; the Silk-Pattern and the Silk-Diff-Pattern datasets. Each dataset contains 300 training images. We also divided the image into 2x2 blocks according to the grid-based method. Then, we calculated the robust features by sending each block to the texture feature and local feature descriptors. To test the performance of image recognition, we used two test sets, including Crop-30 and Crop-40 sets. These test sets were randomly cropped three times from the silk fabric image. Therefore each test set included a total of 900 images.

The experimental results are based on 5-fold cross-validation. We compute average recognition accuracies and standard deviations for all experiments. Also, the grid-based method is performed.

Table 1. Evaluation of the classification results on the Silk-Pattern dataset

Method	Accuracy (%)	
	Crop-30	Crop-40
LBP+KNN	**93.48±0.64**	**99.26±0.12**
HOG+KNN [19]	92.05±0.31	89.73±0.79
SIFT+KNN	23.03±0.36	57.99±0.33
LBP+SVM	92.61±0.16	98.46±0.08
HOG+SVM	74.92±1.94	82.68±4.67
SIFT+SVM	42.80±6.98	40.24±1.08
LeNet [19]	64.06±2.25	76.98±2.29
AlexNet	44.70±0.94	55.58±1.04

Table 2. Evaluation of the classification results on the Silk-Diff-Pattern dataset

Method	Accuracy (%)	
	Crop-30	Crop-40
LBP+KNN	65.70±0.84	79.20±0.45
HOG+KNN	76.58±0.98	88.45±0.23
SIFT+KNN	49.59±0.99	59.44±1.14
LBP+SVM	**90.97±0.74**	**92.81±0.74**
HOG+SVM	48.18±1.55	73.22±0.95
SIFT+SVM	41.40±0.94	34.58±1.04

Table 1 shows the recognition accuracy results of the eight different techniques. According to these experimental results, we combined both the texture feature and local feature descriptors with the classifiers, including the K-nearest neighbor (KNN) and support vector machine (SVM) algorithms. The combination of the local binary pattern (LBP), which is the texture feature, and the K-nearest neighbor algorithm (KNN), called LBP+KNN perform the best for the Silk-Pattern dataset on both test sets; Crop-30 and Crop-40. The accuracy result of the LBP+KNN method increased by 1% more than the HOG+KNN [19] method. Moreover, this method shows a significant performance gain of 20-30% compared to the LeNet and AlexNet architectures [19], which are the deep learning techniques.

In Table 2, we report the results of the average accuracy and standard deviation on the Silk-Diff-Pattern dataset. The results show that the LBP with the support vector machine (SVM), called the LBP+SVM, achieves the best accuracy performance on both test sets. The HOG+KNN method is around 4-14% more accurate than the HOG+KNN method, which is the second-best method. Surprisingly, the scale-invariant feature transform (SIFT) method performed very low performance while combined with KNN and SVM algorithms on two datasets.

5. CONCLUSION

In this paper, we compared methods of silk pattern image recognition. First, we proposed a grid-based method for dividing the image into sub-areas. Second, the two well-known feature extraction techniques: texture feature and local feature descriptor, were proposed to extract robust features from each sub-area. The grid-based method allowed the feature extraction technique to extract more useful features. Finally, we concatenated the robust features and fed them to the classifier algorithms: K-nearest neighbor and the support vector machine algorithms.

The results showed that the LBP algorithm outperforms other methods when combined with both the KNN and the SVM algorithms. On the Silk-Pattern dataset, the LBP+KNN method performs much better than the other methods for all test sets. Subsequently, the LBP+SVM method shows the best performance on the Silk-Diff-Pattern dataset. We also compared our results with two basic deep learning architectures: LeNet and AlexNet architectures. We found that the deep learning architectures showed low accuracies when the training set is inadequate. To the best of our knowledge, the scale-invariant feature transform (SIFT) algorithm always showed the best performance. On the other hand, surprisingly, the SIFT algorithm had very low performance when combined with KNN and SVM algorithms on the silk image dataset.

We conclude that deep learning architecture obtain high accuracy on many pattern recognition problems. In future work, we want to study deep learning architecture and apply it to the silk image dataset. We are also interested to improve the performance by using transfer learning and data augmentation.

6. ACKNOWLEDGMENTS

This research was supported by the Faculty of Informatics at Mahasarakham University, Thailand (IT2-03/2561).

7. REFERENCES

[1] A. H. Ahmed et al. 2017. Human Detection Using HOG-SVM, Mixture of Gaussian and Background Contours Subtraction. *13th International Conference on Signal-Image Technology Internet-Based Systems (SITIS)* (2017), 334–338.

[2] Bharadi, V.A. et al. 2015. Performance Analysis of Grid & Texture Based Feature Vector for Dynamic Signature Recognition. *International Conference on Pervasive Computing (ICPC)* (2015), 1–6.

[3] Bristow, H. and Lucey, S. 2014. Why do linear SVMs trained on HOG features perform so well? (2014).

[4] Chen, L. et al. 2015. Hierarchical Grid-based Multi-People Tracking-by-Detection With Global Optimization. *IEEE Transactions on Image Processing*. 24, 11 (2015), 4197–4212. DOI:https://doi.org/10.1109/TIP.2015.2451013.

[5] Choi, S. and Han, S. 2014. Fast image retrieval with grid-based keypoint detector and binary descriptor. *International Conference on Information and Communication Technology Convergence (ICTC)* (2014), 679–680.

[6] Dalal, N. and Triggs, W. 2005. Histograms of Oriented Gradients for Human Detection. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)* (2005), 886–893.

[7] Dittakan, K. and Author, N.T.-A. 2018. Pum-Riang Thai Silk Pattern Classification Using Texture Analysis. *Pacific Rim International Conference on Artificial Intelligence* (2018), 83–90.

[8] Drozdz, M. and Kryjak, T. 2016. FPGA Implementation of Multi-scale Face Detection Using HOG Features and SVM Classifier. *Image Processing & Communications*. 21, 3 (2016), 27–44. DOI:https://doi.org/10.1515/ipc-2016-0014.

[9] Humeau-HeurTier, A. 2019. Texture Feature Extraction Methods: A Survey. *IEEE Access*. 7, (2019), 8975–9000. DOI:https://doi.org/10.1109/ACCESS.2018.2890743.

[10] Jie, H. et al. 2018. An Improved kNN Based on Class Contribution and Feature Weighting. *Measuring Technology and Mechatronics Automation, International Conference on* (2018), 313–316.

[11] Kambi Beli, I.L. and Guo, C. 2017. Enhancing Face Identification Using Local Binary Patterns and K-Nearest Neighbors. *Journal of Imaging*. 3, 3 (2017). DOI:https://doi.org/10.3390/jimaging3030037.

[12] Karaaba, M. et al. 2015. Robust face recognition by computing distances from multiple histograms of oriented gradients. *Computational Intelligence (SSCI), IEEE Symposium Series on* (2015), 203–209.

[13] Kavitha, J.C. and Suruliandi, A. 2016. Texture and Color Feature Extraction for Classification of Melanoma using SVM. *International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE)* (2016), 1–6.

[14] Liu, L. et al. 2010. Simplified Local Binary Pattern Descriptor for Character Recognition of Vehicle License Plate. *Computer Graphics, Imaging and Visualization, Seventh International Conference on* (Aug. 2010), 157–161.

[15] Lowe, D.G. 2004. Distinctive Image Features from Scale-Invariant Keypoints. *International Journal of Computer Vision*. 60, 2 (2004), 91–110. DOI:https://doi.org/10.1023/B:VISI.0000029664.99615.94.

[16] Misra, S. and Laskar, R.H. 2017. Taxonomy of Texture and Color-Texture Features for Developing Hand Detection System under Non-Ideal Conditions. *14th IEEE India Council International Conference (INDICON)* (2017), 1–6.

[17] Mitchell, T. 1997. *Machine Learning*. McGraw Hill.

[18] Ojala, T. et al. 1996. A comparative study of texture measures with classification based on featured distributions. *Pattern Recognition*. 29, 1 (1996), 51–59. DOI:https://doi.org/https://doi.org/10.1016/0031-3203(95)00067-4.

[19] Raksaard, N. and Surinta, O. 2018. Comparative Study Between Local Descriptors and Deep Learning for Silk Pattern Image Retrieval. *Journal of Science and Technology Mahasarakham University*. 37, 6 (2018), 736–746.

[20] Roempluk, T. and Surinta, O. 2019. A Machine Learning Approach for Detecting Distributed Denial of Service

Attacks. *Digital Arts, Media and Technology, International Conference on* (2019), 146–149.

[21] Surinta, O. et al. 2015. Recognizing Handwritten Characters with Local Descriptors and Bags of Visual Words. *6th International Conference on Engineering Applications of Neural Networks (EANN)* (2015), 255–264.

[22] Vapnik, V.N. 1998. *Statistical Learning Theory*. Wiley.

[23] Wang, L. and He, D.-C. 1990. Texture classification using texture spectrum. *Pattern Recognition*. 23, 8 (1990), 905–910. DOI:https://doi.org/https://doi.org/10.1016/0031-3203(90)90135-8.

Chapter 3

Artificial Intelligence and Intelligent Computing

Bidirectional Database Synchronization to the Cloud Computing Platform

Danijel Filipović
Faculty of Organization and Informatics
Pavlinska 2
42000, Varaždin
dfilipovi@foi.unizg.hr

Danijel Sokač
Faculty of Organization and Informatics
Pavlinska 2
42000, Varaždin
dsokac@foi.unizg.hr

Ruben Picek
Faculty of Organization and Informatics
Pavlinska 2
42000, Varaždin
rpicek@foi.unizg.hr

ABSTRACT
Diversity of subsystems in the organization can lead towards bad business results. Many companies decide to patch their business system with multiple subsystems which are usually not interoperable. Along with that, organizations have the dilemma of deciding whether to implement best-of-breed or one vendor solution. There is no correct answer to the dilemma. The outcome of the dilemma depends on each organization individually based on their analysis and needs. This article analyzes how to overcome data inconsistency caused by patching the business system and presents an approach to the synchronization of different databases to the Cloud. Usage of database synchronization tools to unify data in the Cloud is practical for mature organizations which aim to establish data consistency. The goal of this article is to consider some tools for database synchronization and to choose one for the practical example considering the known constraints. In the approach, we used few different databases to verify its compliance with chosen synchronization tool. The approach is based on practical example where couple of databases are synchronized to the Cloud ensuring the data consistency and bidirectional data flow. The solution includes chosen tool and the recommendation on how to ensure flawless data integration in the Cloud. Tests of synchronization duration with chosen databases and row quantities are conducted and analyzed at the end of the article.

CCS Concepts
•Information systems→Cloud based storage.

Keywords
Data inconsistency; Cloud Computing; Database synchronization.

1. INTRODUCTION
The modern era and well-adapted systems are usually a road towards many databases in single organization – no matter if we talk about multiple applications or multiple subsidiaries of the organization. Both use cases are direct causes of data inconsistency. The reasons behind choosing different applications are financial and organizational reasoning, which means that the organization considers pros, cons and costs of single information system's implementation and it may be shown that it is cheaper to just buy a third-party application which works well. However, the cost of repairing this mistake is incomparable higher. The data inconsistency among the subsidiaries is caused by keeping on premise solutions and missing Cloud storage to unite all subsidiaries under one database. When you start to gather all data in one place, naturally, you try to get most of the data and begin to implement analysis appropriate for your domain. Such issues are addressed in this article.

The structure of this paper is the following: 2nd section is about the dilemma that usually troubles the organizations; 3rd section mentions several research papers that were found on the subject of data consistency and database synchronization; 4th section explains how and which database synchronization tool was chosen for use in the use case; and the 5th section describes the use case, our solution for it, conducted and analyzed a synchronization duration test with chosen databases and row quantities, and several remarks regarding our proposed solution.

2. BACKGROUND RESEARCH
Many organizations came across the dilemma to choose "best of-breed" (BOB) solutions or single vendor unifying whole organization with single database. The choice depends on the company itself.

Single vendor is considered Enterprise Resource Planning (ERP) System in the article. ERP offers simple solutions to data issues as mentioned in [1]. Important issues of choosing one solution for entire company offers a company one information system across the organization, difficult implementation and hidden costs of the implementation as stated in [2].

On the other hand, "best-of-breed" (BOB) solutions are better customized to fit business process needs entirely. Geshecker L. [3] elaborates arguments why BOB solutions are good or bad for organization. Some of BOB solution's advantages are (1) fits the process very well, and (2) implementation is simple and straightforward. Some of its disadvantages are (1) the customization and programming efforts may raise as the time passes, (2) supports finite number of hardware, and (3) the more complex system the more interfaces are needed.

Light B. et al [2] wrote a comparison of features offered by BOB and ERP solutions; the bottom line is that BOB solutions are more adapted to particular organization while ERP solutions aim to satisfy broader range of organizations and their solutions are not particularly customized to fit one organization's specific needs. Other comparison conducted by Geshecker L. [3] lists pros and cons of each options which are confirmed by latter statement.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388204

There is no wrong choice in this issue. Choosing BOB or ERP system is highly dependent on other parameters like organization size, long-term goals, financials, the determination to implement either solution. The advantage of BOB is its nearly perfect fit in business process. The ERP system, on the other hand, is great choice for organization which wants to connect whole company and use generated data to improve their position in the market.

3. RELATED WORK

The use case described in this paper focuses on keeping consistent data between multiple databases on different servers via database synchronization (more on this is explained in sections 3 and 4), several existing papers were read on the subject of data consistency and database synchronization.

Wijegunaratne et al. [4] propose an architecture, "federated architecture", which would minimize the dependency and coupling between applications via "federal highway". "Federal highway" is basically a Message-Oriented Middleware[1] (MOM) which application uses to either send and/or receive contextual messages to indicate that new data has been added, or that existing data has been either updated or removed. A similar architecture is also proposed by Svensson et al [6].

Svensson et al. [6] present a service-oriented architecture for synchronizing data between applications with different (heterogeneous) data models for their data. The architecture also uses MOM, also called Enterprise Service Bus (ESB) by the authors in their paper. Applications communicate with each other through the ESB (via SOAP messages). The data synchronization with different data models is implemented by converting the data from application's local data model into ESB's global data model, and vice versa.

Both Wijegunaratne et al. [4] and Svensson et al. [6] recommend architectures which use MOM for communication between different applications and, in latter's case, to synchronize data between different databases. This could mean that it is recommendable to implement the synchronization mechanism as its own application or service and decouple it or minimize its coupling from actual data applications. Another problem that could occur, and be solved by using MOM, is synchronizing the data between different types of databases. The solution to that would be, as mentioned by Svensson et al. [6], to introduce a global data model which data applications would use to convert data into it and vice versa.

Haossain and Ali [7] present a database synchronization by sending a Structured Query Language (SQL) query from a source database, which made the change, to a target database via Hyper-Text Transfer Protocol (HTTP). They describe a process which checks for the latest queries made by the database management system (DBMS) and sends the queries to the target database's web services which process the query and apply the changes. There is no middle layer in this architecture. Basically, the source database server is responsible for detecting and sending changes to all target databases.

Yu and Zhou [8] present another solution where they introduce a layer between the database, and the Internet and/or a Web server. This layer, called "castway", reads the changes in its database server and forwards the tracked changes to other databases via multicast or anycast protocols. Those changes then must go through the target database's Web server and castway to process the changes before applying them to the actual database. Basically, each database server has its own Web server and castway for communication with the other database server's Web server and castway that would process and synchronize the changes.

[1] Message-Middleware, or MOM, is an "in-between" software layer that allows applications to communicate with each other [5].

4. DATABASE SYNCHRONIZATION TOOL

While searching for the software tools that would enable the database synchronization, a few requirements were set:

- The tool has to be able to synchronize data between databases and not only replicate them.
- The tool has to synchronize data between relational databases.
- The tool has to be able to synchronize data between databases which exist on different servers.
- The tool has to be able to synchronize data between multiple (>2) databases.
- The tool has to be able to synchronize data bidirectionally.

These requirements are tied to the use case scenario where data had to be synchronized between multiple databases with same schema but from different servers. Figure 1 shows the basic idea what the data synchronization tool needs to be able to do: servers (clouds), each with its own database (cylinders), synchronizing the contents of the database with the other servers (dashed line) bidirectionally.

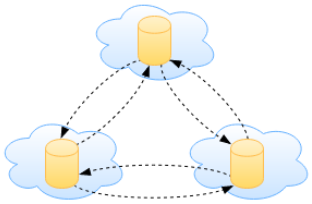


Figure 1. Basic idea of the data synchronization tool's requirements (author's work).

In total, two synchronization tools have been found: *SymmetricDS* and *rubyrep*. Table 1 shows the requirements those two tools meet.

Table 1. Requirements fulfillment of the database synchronization tools.

	Requirement				
Tool	1	2	3	4	5
SymmetricDS	Yes	Yes	Yes	Yes	Yes
rubyrep	Yes	Yes	Yes	No	Yes

Because of *rubyrep*'s lack of support for synchronization of more than two databases, *SymmetricDS* ends up being the best choice and is chosen as a database synchronization tool for the use case.

5. USE CASE

In this section, a use case scenario is described, and its suggested solution is explained upon.

5.1 Scenario

The company has several (more than 1) subsidiaries which use IoT systems for measurement and each subsidiary has its own relational database server for storing the measured data. The relational databases for every subsidiary have the same database schema (or database structure).

The company wants to create a master relational database with the same database schema as the subsidiary database. It would contain every data that exists and/or will be added, updated, or deleted from the subsidiary databases. Basically, every change to the contents of the subsidiaries databases needs to be synchronized with the master database, and only the master database. Also, the subsidiaries have their settings stored in the same database used to store the measured data. The request was made to make the synchronization bidirectional so the settings could be updated both from the master database and from the subsidiary database. Figure 2 shows the graphic representation of the use case scenario.

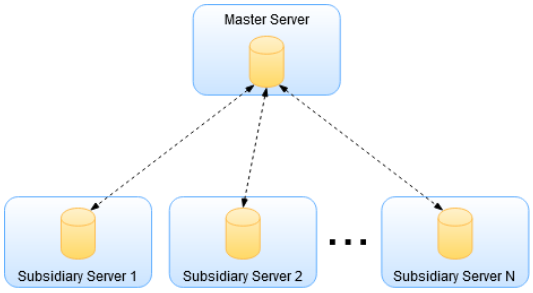


Figure 2. The scenario (author's work).

5.2 Solution

Solution for the described scenario is shown in Figure 3. The company and each subsidiary have their own servers hosting own relational DBMS (RDBMS). The databases must have the same database schema and take into consideration the first remark mentioned in section *5.3. Remarks*. For the following explanation, the company's server and database will be called the 'master server' and the 'master database' respectively.

An instance of a *SymmetricDS* server is started with a configuration which contains:

- data required for it to access the participating databases (database server's URL, username, password, and database name) and register them (synchronization URL, registration URL, group ID to which the database belongs to, and its external ID),
- data defining data synchronization behavior between the master and subsidiary databases.

While the *SymmetricDS* is running, it periodically checks for changes in all of the registered databases. If there has been change in one of the subsidiary databases (e.g. IoT device stores the measured data), the change is pulled to the master database. If there has been a change in the master database (e.g. IoT settings have been changed), the change is pulled to corresponding subsidiary database. There is a remark in section *5.3. Remarks* regarding why does the *SymmetricDS* 'pull' the data to synchronize them.

In this solution, the *SymmetricDS* server serves as a type of proactive MOM: it checks for any changes in either master database or one of the subsidiary databases, processes the changes into an SQL query which is sent to the target database(s).

One of the benefits of *SymmetricDS* is its placement flexibility. *SymmetricDS* can be installed and started on any server. For example, it could be placed on: (1) the master server where the master RDBMS is running, (2) a separate server within the company's local network, or (3) a separate server outside the company's local network. The first option would shorten the communication delay between the synchronization service and the master RDBMS. The second option would separate the responsibilities of the servers for easier maintenance. The third option would need a special reason for separating the *SymmetricDS* server from the company's network, e.g. delegating the maintenance of the synchronization service to the third-party.

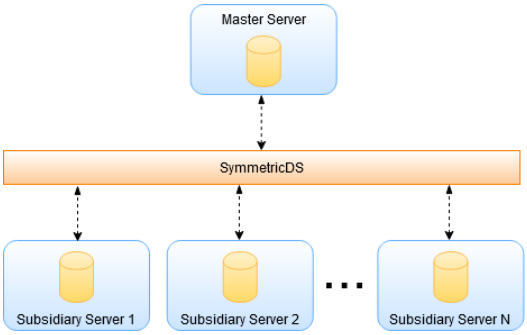


Figure 3. The solution (author's work).

5.3 Measuring the Duration of Synchronization

The measurements between chosen databases are conducted. The synchronization tool measured in test cases is the *SymmetricDS*. The *SymmetricDS* is configured as instructed in their website[2] and its engine configurations [3] contain only required properties. Following databases are chosen: Firebird, MySQL and PostgresSQL. These databases have been used while working on the described use case. The databases are addressed as master and slave which is referred to cloud and local database respectfully. Test cases (TC) are as follows:

TC-1 – slave to master

This scenario shows inserting data into the slave database, observing how SymmetricDS server responds to the changes in the aforementioned database, and viewing the result of the synchronization – data from slave database pulled into the master database.

TC-2 – slaves to master

Random data is inserted in multiple slave databases to simulate parallel synchronization. The result of the test case is that the data from all slaves is pulled into the master database.

TC-3 – master to slaves

Data is inserted into the master database, the test case shows how SymmetricDS server responds to the changes in the database, and the result of the synchronization is pulling data from master database into the slave databases.

These test cases are ran with various number of rows being inserted into the particular database. Chosen quantities of rows are as follows: 500, 1000, 2500, and 5000 rows. Each TC is ran with three setups where the master and slave databases are implemented in: PostgresSQL, MySQL and Firebird.

There is one attribute that will be measured: *the synchronization time* of SymmetricDS.

[2] Configuration: http://www.symmetricds.org/doc/3.10/html/user-guide.html#_configuration

[3] Engine setup: http://www.symmetricds.org/doc/3.10/html/user-guide.html#_node_properties_file

As help, a custom tool was written in programming language Java to assist in sending out SQL queries to the databases. The tool generates randomly generated data to be inserted into the desired table of the desired database. It is written as a command-line application that takes three command-line arguments:

- the configuration files which contain the data needed to connect to the three different databases (DBMS, host address, database, username, and password),
- the name of the table where the new rows will be inserted, and
- the number of randomly generated to be inserted into the table.

For each configuration file added for the first command-line argument a separate thread is started which generates, prepares, and executes the SQL queries which insert new rows of data for each database described in the configuration files.

Each TC populates additional database with start time and finish time of the database synchronization. The times are related to the database which is being updated. For TC-1 and TC-2 these times are converted into durations by subtracting the finish time and the start time. However, the TC-3 is slightly different. The durations of TC-2's results are calculated by subtracting the latest finish time and the earliest start time which represent the beginning of first slave synchronization and the end of the last slave synchronization respectively.

5.4 Analysis of Test Results

Results of the measurements described in section 5.3 are presented here. Results of the test cases are grouped by number of rows inserted into initial database and that is why there are four tables – each table represents each quantity of rows inserted into initial database. Every test case synchronized single table. Tables shows the duration of synchronizing between master and slave databases.

Synchronizing 500 rows is quite fast. The PostgresSQL database was the fastest and the Firebird database the slowest, which is visible in Table 2. Increasing the row quantity for 500 rows caused the PostgresSQL and Firebird databases lose some pace while the MySQL database still keep it the same, which is shown in Table 3. The title "the fastest" still holds PostgresSQL firmly and the title "the slowest" belongs to the Firebird database again.

Table 2. Test case results when inserting 500 rows

	Databases		
Test Cases	PostgresSQL	MySQL	Firebird
TC-1	0 s	10 s	20 s
TC-2	0.54 s	10 s	20 s
TC-3	13 s	18 s	48 s

Table 3. Test case results when inserting 1000 rows

	Databases		
Test Cases	PostgresSQL	MySQL	Firebird
TC-1	9.96 s	10 s	30 s
TC-2	9.98 s	11 s	40 s
TC-3	13 s	32 s	82 s

The results in synchronization durations of inserting 2500 rows are presented in Table 4. The PostgresSQL and Firebird databases lost quite some pace, but the MySQL database still maintains the same performance except for the poor result of TC-2 with the duration 62 seconds. The title "the slowest" is still with its owner, but this time the MySQL database lost the victory because of the TC-3 and therefore, the title "the fastest" is still by the PostgresSQL database. The final attempt is running the test cases with double amount of previous quantity and its results are displayed in Table 5. The duration times went up as expected. This time, the PostgresSQL database is the fastest and the Firebird database is still the slowest.

Table 4. Test case results when inserting 2500 rows

	Databases		
Test Cases	PostgresSQL	MySQL	Firebird
TC-1	10.31 s	10 s	70 s
TC-2	20.01 s	11 s	81 s
TC-3	24 s	62 s	194 s

Table 5. Test case results when inserting 5000 rows

	Databases		
Test Cases	PostgresSQL	MySQL	Firebird
TC-1	20.42 s	30 s	150 s
TC-2	29.99 s	30 s	161 s
TC-3	38 s	120 s	390 s

In conclusion, the database synchronization duration is clearly dependent on the database performance. Therefore, the TC-3 lasts longer than other test cases because of the number of slave databases which has to be synchronized. The PostgresSQL database is meant to operate with Big Data so it shows better performance with higher number of rows. The PostgresSQL database is the fastest database overall. The slowest database is the Firebird database which shows its poor performance in comparison to other two databases.

5.5 Weaknesses

There are several weaknesses that need to be mentioned regarding the described architecture.

One of the weaknesses is regarding changes to either the table structure or the database schema. If a table has its structure changed (e.g. a new column is added, existing column is changed or dropped, etc.), then the same change has to be carried out manually on all other participating databases. *SymmetricDS* does provide some command-line tools that message the synchronization server about the changes, but it still needs to be done manually. As for the changes in the database schema, if a table is created or dropped then only the synchronization behavior has to be updated to take into consideration the new table or take out of consideration the dropped table. The recommended steps are described in [9].

Another weakness lies with the connection data that *SymmetricDS* needs to read from and write to databases participating in the synchronization. If for some reason the database host address is changed, or the database user created for the *SymmetricDS* is altered in any way (e.g. username or password are changed, roles have been altered, etc.) then the same changes have to be applied to database configuration files on *SymmetricDS'*s end. This could end up being a major inconvenience.

5.6 Remarks

There are five remarks that need to be mentioned for this use case regarding: (1) the way the data from the subsidiary databases can be differentiated in the master database, (2) the choice of the database management system, (3) how the *SymmetricDS* sets up its synchronization functionality, (4) if the *SymmetricDS* should 'push' or 'pull' the changes, and (5) can the database workload be optimized with indexes.

For the first remark, each subsidiary has its own data in the database, which could lead to the collision of the identity columns (primary keys) when the database tables are synchronized to the master database. To remedy this, the use of composite keys is suggested where:

- One of the keys represents the identity of a row in the database table;
- The other member of the keys represents the subsidiary, and its value would be specific for them.

The second remark is tied to the list of database management systems which the *SymmetricDS* is able to work with. When implementing the suggested solution, one has to take into consideration which database management system is supported by the *SymmetricDS*. The software does support the popular DBMSs like PostgreSQL, MySQL, and Oracle's DBMS, but the company should be careful if it uses a less known DBMS.

For the third remark, to set up its synchronization capabilities the *SymmetricDS* has to create its own set of tables and triggers in every database, which it uses to know how to synchronize the data database.

For the fourth remark, the *SymmetricDS* has two ways of doing the synchronization: either by 'pushing' or 'pulling' the changes. When pulling the changes, the *SymmetricDS* periodically checks the then starts synchronizing the data if the changes have been made. When pushing the changes, the *SymmetricDS* instantly starts synchronizing the changes. However, there is catch with the push method: it only works if the changes are made by using the *SymmetricDS*'s own SQL tool. If the change is made in any other way, like with the SQL query executed by the application, then the push method will be ineffective.

Fifth remark answers the question if the database workloads can be optimized with the use of indexes. Indexes in RDBMSs are used to speed up the SELECT queries, and in some cases both UPDATE and DELETE queries. This is useful in databases where data is constantly read from. However, this paper describes a scenario where data is being constantly inserted into the databases. As mentioned in [10], indexes speed up queries, but they slow down modifications. Also, indexes would have to be rebuilt for every new data inserted into the database. In short, indexes for this type of system are more of a hindrance than a help.

6. FUTURE WORK

With the system that synchronizes and accumulates data into one point, it could be used as a starting point for the development of specialized cloud-computing services that would utilize the gathered data for analytics. As mentioned in [11], implementing cloud-computing would provide on-demand computing services to both first-party and third-party users. This could be implemented either as:

- a software-as-a-service (SaaS) that could act as an assistant tool to the company and/or encapsulate the way data can be analyzed for first-party or third-party users,
- a platform-as-a-service (PaaS) that would let first-party or third-party users have freedom in performing analysis on the data. or

Also, the cloud-computing idea could also be left-out in the favor of making a data-as-a-service (DaaS) [12]. This would provide users even more flexibility in creating the way data could be analyzed. Optionally, at some cost.

7. REFERENCES

[1] M. A. Elghany, M. A. Elghany, and N. Khalifa, 'Best-of-Breed of ERP Systems: Pros and Cons', vol. 04, no. 03, p. 5.

[2] B. Light, C. P. Holland, and K. Wills, 'ERP and best of breed: a comparative analysis', *Business Process Management Journal*, vol. 7, no. 3, pp. 216–224, Jan. 2001, doi: 10.1108/14637150110392683.

[3] G. Lee, 'ERP vs. best-of-breed', *Strategic Finance; Montvale*, vol. 80, no. 9, pp. 62–67, Mar. 1999.

[4] I. Wijegunaratne, G. Fernandez, and J. Valtoudis, 'A federated architecture for enterprise data integration', in *Proceedings 2000 Australian Software Engineering Conference*, 2000, pp. 159–167, doi: 10.1109/ASWEC.2000.844573.

[5] 'Message-Oriented Middleware (MOM) (Sun Java System Message Queue 4.3 Technical Overview)'. [Online]. Available: https://docs.oracle.com/cd/E19340-01/820-6424/aeraq/index.html. [Accessed: 17-Jan-2020].

[6] E. Svensson, C. Vetter, and T. Werner, 'Data consistency in a heterogeneous IT landscape: a service oriented architecture approach', in *Proceedings. Eighth IEEE International Enterprise Distributed Object Computing Conference, 2004. EDOC 2004.*, 2004, pp. 3–8, doi: 10.1109/EDOC.2004.1342500.

[7] I. Hossain and M. Masroor Ali, 'SQL query based data synchronization in heterogeneous database environment', presented at the 2012 International Conference on Computer Communication and Informatics, Coimbatore, India, 2012, doi: 10.1109/ICCCI.2012.6158818.

[8] S. Yu and W. Zhou, 'A Novel Middleware Based Web Database Model', in *Proceedings of the 2004 IEEE/WIC/ACM International Conference on Web Intelligence*, 2004, pp. 533–536.

[9] E. Long, 'Sync Schema (DDL) Changes', Oct-2012. [Online]. Available: https://www.symmetricds.org/docs/how-to/sync-schema-ddl-changes. [Accessed: 16-Feb-2020].

[10] H. Garcia-Molina, J. D. Ullman, and J. Widom, *Database Systems: The Complete Book, 2nd Edition*. Upper Saddle River: Pearson, 2009.

[11] L. Arockiam and A. Stanislas, 'A Unified Architecture for Optimal Resource Utilization in a Heterogeneous Cloud Environment', *IJMLC*, vol. 4, no. 4, pp. 383–388, 2014, doi: 10.7763/IJMLC.2014.V4.441.

[12] X. Zong, Q. Li, K. He, and D. Velev, 'Comprehensive Management Platform of Natural Disasters Based on Cloud Computing', *International Journal of Machine Learning and Computing*, vol. 6, no. 3, pp. 179–183, 2016.

Genetic Ant Colony Algorithm Improves Resource Scheduling in Cloud Computing

AoFeng Zhou
Software school of Zhengzhou University,
Zhengzhou,450000, China
Tel:008613460548700
E-mail:1970189129@qq.com

ABSTRACT
When a large number of users request cloud computing resource services, rational organization of resources and task scheduling is one of the key technologies of cloud computing. Aiming at the problems of low efficiency and slow convergence speed of existing cloud computing resource scheduling algorithms, combined with the characteristics of global search ability of genetic algorithm and positive feedback convergence of ant colony algorithm, a resource scheduling algorithm is proposed. The initial pheromone distribution is generated by the genetic operator, and the exact solution is obtained by the bidirectional convergence ant colony operator. The experimental results show that the proposed algorithm is superior in solving accuracy and convergence speed, and it is an effective cloud computing resource scheduling algorithm.

CCS Concepts
• **Computing methodologies → Distributed computing methodologies→Distributed algorithms→Self-organization.**

Keywords
cloud computing; resource scheduling; genetic algorithm; ant colony algorithm

1. INTRODUCTION
The quality of resource allocation algorithms has always been an important indicator of cloud computing capabilities. The QoS-driven scheduling algorithm in [1-2] optimizes the total execution time, load balancing and delay of cloud computing; the NNDNSGA-II algorithm in [3] dynamically plans the optimal allocation scheme for different number of task flows; [4-6] Improved ant colony algorithm, under the probability model, the mathematical expectation optimal allocation scheme is obtained. The above algorithms all improve the cloud computing resource scheduling algorithm to varying degrees, but rarely can balance the time, load, task traffic and cost. In this paper, a cloud computing resource scheduling method is presented. The algorithm uses genetic operators [7-9] to generate an initial pheromone distribution. Based on this, the bidirectional convergence ant colony algorithm [10] is used to solve iteratively. The algorithm does not fall into the local optimal solution, nor does it appear premature convergence, and has a good global search ability.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388213

2. DESCRIPTION OF THE PROBLEM OF CLOUD COMPUTING RESOURCE SCHEDULING
The introduction of virtualization in cloud computing makes its resource scheduling mode different from traditional distributed resource scheduling. The resource scheduling of cloud computing is shown in Figure 1. First, each task is divided into several independent subtasks. When the system receives the request, it allocates certain virtual resources to cope, and each subtask corresponds to one virtual resource node.

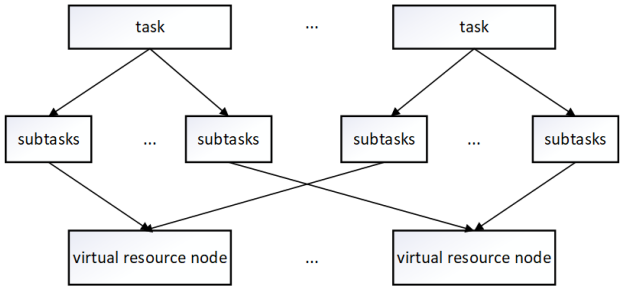


Figure 1.Resource scheduling in cloud computing

The definition of resource scheduling in cloud computing is as follows：The task is divided into n independent subtasks and assigned to m virtual resource nodes, where m<n. Use T= $\{t_1,t_2,...,t_n\}$ to represent the set of subtasks Here, t_j ($0 < j \leqslant n$) represents the j-th subtask. With VM=$\{vm_1,vm_2,...,vm_m\}$ to represent a collection of virtual resource nodes, where vm_i($0 <i\leqslant m$) represents the i-th virtual resource node, and each t_j can only be in one executed on vm_i. The correspondence between T and VM can be assigned to the relational matrix X. Expressed as

$$X=\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \quad (1)$$

Here x_{ij} represents the correspondence between t_j and vm_i, $x_{ij} \in \{0,1\}$, $\sum_{i=1}^{m} x_{ij}=1$, $i\in \{1,2,...,m\}$,$j\in \{1,2,...,n\}$, Indicates that if t_j is executed on vm_i, $x_{ij}=1$, otherwise $x_{ij}=0$. The expected time for t_j

to complete on vm_i is represented by ET_{ij}, which corresponds to the distribution matrix matrix X, and the ET matrix is

$$ET = \begin{bmatrix} ET_{11} & ET_{12} & \cdots & ET_{1n} \\ ET_{21} & ET_{22} & \cdots & ET_{2n} \\ \vdots & \vdots & & \vdots \\ ET_{m1} & ET_{m2} & \cdots & ET_{mn} \end{bmatrix} \quad (2)$$

Let vm_i start at c_i, then the expected completion time of the vm_i processing task is $CT_i = c_i + \sum_{j=1}^{n} ET_{ij} \times x_{ij}$, where i ∈ {1,2,...,m},j∈{1,2,... , n}. Define CT_{max} = max{CT_i}, CT_{min} = min{CT_i}. Therefore, the expected time for the completion of the total task is CT_{max}, and the fitness function for the total task completion time is

$$f_{CT} = \frac{CT_{\max} - CT_{\min}}{\sum_{j=1}^{m} (CT_i - CT_{\min})} \quad (3)$$

Similarly, the total cost of t_i on vm_j is represented by EC_{ij},making A_{ij} Representing the resources occupied by t_i on vm_j, EC_{ij} is positively correlated with the consumed time ET_{ij} and the occupied resource A_{ij}, and the correlation coefficient is ξ, then

$$EC_{ij} = \xi \times ET_{ij} \times A_{ij} \quad (4)$$

Corresponding to the distribution relationship matrix X, the EC matrix is

$$EC = \begin{bmatrix} EC_{11} & EC_{12} & \cdots & EC_{1n} \\ EC_{21} & EC_{22} & \cdots & EC_{2n} \\ \vdots & \vdots & & \vdots \\ EC_{m1} & EC_{m2} & \cdots & EC_{mn} \end{bmatrix} \quad (5)$$

Let EC_i handle the cost of the task for vm_i, where i ∈ {1,2,...,m}, then $EC_i = \sum_{j=1}^{n} EC_{ij} \times x_{ij}$. Therefore, the fitness function of the total cost of task costs is

$$f_{EC} = \frac{\sum_{i=1}^{m} EC_i}{\sum_{i=1}^{m} \sum_{j=1}^{n} EC_{ij}} \quad (6)$$

Then the resource scheduling adaptation function of the optimization algorithm is

$$F_{fitness} = a \times f_{CT} + b \times f_{EC} \quad (7)$$

Where: a+b=1, 0≤a, b≤1. The goal of the algorithm is to find a suitable matrix X that minimizes the $F_{fitness}$ value.

3. RESOURCE SCHEDULING BASED ON GABAC ALGORITHM IN CLOUD COMPUTING

The basic idea of the algorithm is to combine the advantages of the genetic algorithm with the two-way convergence ant colony algorithm and apply it to the cloud computing resource scheduling, so as to overcome the shortcomings of the respective algorithms, making it better than the ant colony algorithm in time. Better than genetic algorithm. The idea of the algorithm is to fully exploit the randomness of the genetic algorithm and the fast global convergence to generate a pheromone distribution of the resource scheduling problem. This distribution is used as the initial pheromone distribution of the ant colony algorithm. Based on this, the bidirectional convergence strategy is adopted, and its positive feedback, parallelism, and high accuracy are fully utilized to obtain a comprehensive understanding of resource scheduling.

3.1 Model Selection of Genetic Operators in GABAC Algorithm

3.1.1 Coding and fitness function

The length of the defined chromosome represents the number of subtasks in the resource scheduling, and the task is coded so that the value of the gene is the resource number occupied by the corresponding task. In the cloud computing resource scheduling process, the larger the fitness function value of the solution, the greater the possibility of being passed to the next generation, and the greater the chance of survival. The time fitness function of this paper is $Fit_{time}=f_{CT}$, and the cost fitness function $Fit_{cost}=f_{ECOST}$. The better the allocation strategy in resource scheduling, the less time it takes for the task to complete, and the lower the cost of running the required cost, the greater the value of the fitness function. In this paper, the time fitness function and the cost fitness function are combined with a certain weight ratio, and the comprehensive fitness function is

$$Fitness(I) = a \times Fit_{time} + b \times Fit_{cost} \quad (8)$$

Among them, a, b represents the weight of time and cost, and is set as needed, requiring a+b=1, a∈[0,1], b∈[0,1].

3.1.2 Race generation and chromosome selection

Randomly generate a certain amount of decimal real number coding population, select the operator to generate roulette [11], according to the ratio of resource scheduling fitness function value to all fitness function values, select a pair of chromosome parent strings ready to be mated, express as follows

$$P(I) = \frac{Fitness(I)}{\sum_{k=1}^{S} Fitness(k)} \quad (9)$$

The solution chosen thus includes individuals with short task completion times, as well as individuals with low mission cost costs, achieving both-way optimization of time and cost.

3.1.3 Crossover operator

Use the sequential crossover method to first cross the two points and then modify the tour route while maintaining the original relative access sequence. The specific cross method is as follows:

(1)Select two parent strings arbitrarily, and randomly select a mating area based on this;

(2)Add the mating regions of the two parent strings to the front of the other parent string to get the two generated new parent strings;

(3)In the original part of the two generated new parent strings, find the same area as the mating area, and delete it one by one to get two substrings.

3.1.4 Mutation operator

The fragmentation fragments are inserted in reverse order by inverse transformation. For example, the chromosome (1-2-3-4-5) produces a break at 3-4 between regions 1-2 and between regions,

and the chromosome obtained after reversal becomes (1-3-2-4-5). Here, "initialization" means that after the reversal, only the fitness function value is improved, it is accepted, and the mutation occurs; otherwise, the reversal is invalid and cannot be mutated.

3.2 Model Selection of Ant Colony Operators in GABAC Algorithm

The ant colony operator selection in GABAC algorithm is based on MMAS (Max-Min ant system) algorithm and adopts bidirectional convergence strategy to improve search ability, speed up convergence and avoid falling into local optimal solution.

3.2.1 Max-Min ant colony algorithm

Compared with the basic ant colony algorithm, the MMAS algorithm has the following improvements: 1) Find the optimal solution in each cycle or pheromone update of ants that may find the known optimal solution; 2) set [τ_{min}, τ_{max}] as the pheromone interval. When the pheromone concentration on a certain path exceeds the range of the interval, it is adjusted by coercive means to prevent extreme situations; 3) according to the genetic operator The result obtained gives an initial value pheromone step on the path.

3.2.2 Two-way convergence strategy

During the operation, the k-th ant selects the node through the probability function at time t, and the probability function is

$$p_{ij}^{k}(t)=\begin{cases}\dfrac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}]^{\beta}}{\sum_{\tau_{il}\notin t_k}[\tau_{il}(t)]^{\alpha}[\eta_{il}]^{\beta}}, \tau_{il}\notin t_k\\ 0\cdots\cdots\cdots\cdots\cdots\cdots, other\end{cases} \tag{10}$$

$$\eta_{ij}(t)=\frac{1}{F_{Fitness}^{k}(t)} \tag{11}$$

In the formula: τ_{ij} (t)—x_{ij} node residual pheromone at time t; η_{ij}(t)—local heuristic factor; t_k—the forbidden path table of the k-th ant. Intensify measures for poor routes, and strengthen measures for better routes, so that after each update, the pheromone concentration of the better route becomes higher, and the pheromone concentration of the poorer route becomes lower, thereby improving the search speed. Here, the MMAS algorithm pheromone update equation for the bidirectional convergence strategy in resource scheduling is

$$\begin{cases}\text{Better route}\begin{cases}\tau_{ij}(t+n)=(1-\rho)\times\tau_{ij}(t)+\sum_{k=1}^{m}\Delta\tau_{ij}^{k}(t)\\ \sum_{k=1}^{m}\Delta\tau_{ij}^{k}(t)=F_{Fitness,best}\end{cases}\\ \text{Poor route}\ \ \tau_{ij}(t)=\tau_{ij}(t)\times\sigma,\sigma\in(0,1]\end{cases} \tag{12}$$

In the formula: σ—the penalty factor, the role of which is to make the pheromone concentration of the poor route lower, thereby reducing the probability that the ant selects the line; when σ=1, there is no influence on the intersecting route; when σ→0 will cause the pheromone concentration of the poor route to decrease rapidly and return to zero. Thereby the bidirectional convergence effect of the algorithm is achieved.

3.3 The Connection between Genetic Operators and Ant Colony Operators in GABAC

The key to the over-extension of two kinds of operators is how to convert the optimal solution value obtained by the genetic operator into the initial information distribution of the ant colony operator. In general, the MMAS algorithm sets the initial pheromone value of each path to the maximum value τ_{max} for a given pheromone interval. Since some optimization solutions have been obtained by genetic operators, the value of the initial pheromone distribution is set to: $\tau_s=\tau_{min}+\tau_G$, where the value of τ_G represents the prime distribution value obtained by the genetic operator.

3.4 Algorithm Description

The flow of GABAC algorithm in cloud computing resource scheduling is shown in Figure 2. It can be divided into two parts. The left part is the genetic operator process, and the right part is divided into the BDC-MMAS operator process.

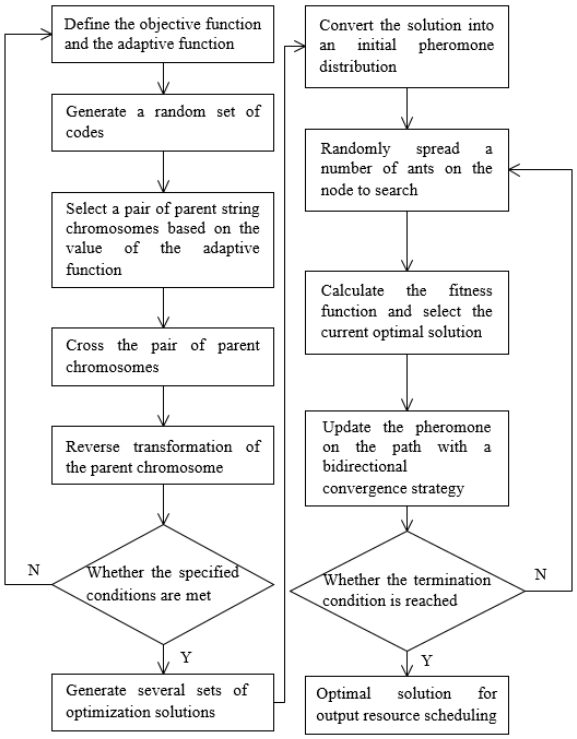


Figure 2.Resource scheduling process of GABAC algorithm

Parameters required by the algorithm: the amount of information left on each node is valued α, heuristic information is valued β, evaporation factor ρ, Gaussian variation factor(When performing mutation, replace the original gene value with a random number with a normal distribution with a mean value of 0 and a standard deviation of σ).

4. EXPERIMENT AND ANALYSIS

The cloud computing resource scheduling environment is simulated on the Cloudsim [12] platform to verify the effectiveness and feasibility of the GABAC algorithm. Initial algorithm parameter settings: α =1, ρ =0.5, σ =0.5, τ_{min}=0.15, τ_{max}=1, ξ =1, number of ants Ants=25, simulation experiment setting For 60 tasks, assign them to 60 resource nodes, each task is

randomly divided into 1 to 60 subtasks, and the time ET_{ij} of the virtual resource node processing task is randomly generated within 0 to 2, and the task is randomly generated within 0 to 2. A resource A_{ij} occupying a virtual resource node, where $i \in \{1, 2, ..., m\}$, $j \in \{1, 2, ..., n\}$.

In the experiment, analyze the total task completion time as the main target, let a=0.8, b=0.2, and compare the genetic (GA) algorithm, the bidirectional convergence ant colony (BDC-MMAS) algorithm and GABAC through experiments. algorithm. For each iteration, each algorithm is run 15 times, and the measured data is averaged 15 times. The experimental results are shown in Figure 3.

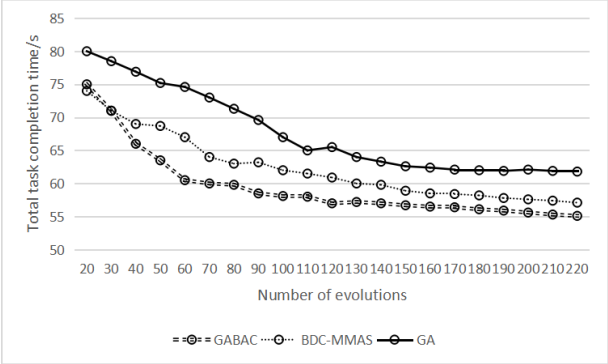


Figure 3.Total task completion time comparison

It can be seen from Fig. 3 that with the increase of evolutionary algebra, the total task completion time of the GABAC algorithm converges faster than the GA algorithm and the BDC-MMAS algorithm, and is more stable and evolved in the convergence process than other algorithms. When the algebra is not low, the total task completion time consumed by the GABAC algorithm is significantly lower than the other two algorithms, and the solution obtained is better.

In the same way, it can be concluded from experiments that with the increase of evolutionary algebra, the average cost of the task completion of GABAC algorithm is faster than that of GA algorithm and BDC-MMAS algorithm, which is more stable than other algorithms in the convergence process. When the evolutionary algebra is not low, the average cost of the task completed by the GABAC algorithm is significantly lower than the other two algorithms, and the solution obtained is better.

In summary, under the condition that the evolutionary algebra is not low, the total task completion time and task completion cost of the GABAC algorithm proposed in this paper are faster than the GA algorithm and BDC-MMAS algorithm, and the effect is better. More stability and optimization. Considering the time and cost factors of resource scheduling in cloud computing, the GABAC algorithm proposed in this paper is optimized in terms of completion time, cost and service quality.

5. CONCLUSION

This paper proposes a resource scheduling algorithm combining genetic algorithm and ant colony algorithm in cloud computing environment. The algorithm uses the fast global convergence of genetic operators to generate an initial pheromone distribution. Based on this, a two-way convergence ant colony algorithm is used. Solve the characteristics of high precision, and iteratively solve it repeatedly to achieve complementary advantages. The experimental results show that the algorithm is superior to genetic algorithm and BDC-MMAS algorithm in terms of time and cost, and has a fast convergence speed and good QoS. It is an effective resource scheduling method.

6. REFERENCES

[1] Bansal, N., Maurya, A., Kumar, T.,Singh, M.and Bansal, S. 2015. *Cost Performance of Qos Driven Task Scheduling in Cloud Computing.*Third International Conference on Recent Trends in Computing. University of Shobhit at College Electronics and Communication Engineering.

[2] Nie, Q. B.,Chen, F. X,Qin, M. F. and Cao, Y. Q., 2019. *Task Scheduling Optimization Based on Qos Cloud Computing*. Journal of Chongqing University.Southwest Jiaotong Unversity.ISSN 1000-582X,CN 50-1044/N.

[3] Ismayilov, G. and Topcuoglu, H. R. 2019. *Neural Network Based Multi-objective Evolutionary Algorithm for Dynamic Workflow Scheduling in Cloud Computing*(307-322). Future Generation Computer System. University of Marmara at College Computer Engineering.

[4] Nie, Q. B.,Cai, T.and Wang, N. 2016. *Application of Improved Ant Colony Algorithm in Resource Allocation of Cloud Computing.*Computer Engineering And Design. DOI= http://dx.doi.org/10.16208/j.issn1000-7024.2016.08.008.

[5] Wu, J. , 2018. *Improved Algorithm of Cloud Task Scheduling Based on Ant Colony Simulated Annealing*. China Computer and Communication.School of Maths and Information Science,Neijiang Normal University.

[6] Zhang, H. R., Chen, P. H., and Xiong, J. B.. 2014. Journal of Guangdong University of Technology. In *Task Scheduling Algorithm Based on Simulated Annealing Ant Colony Algorithm in Cloud Computing Environment*(Guangdong, China, September 77 - 81, 2014). DOI= http://dx.doi.org/10.3969/j.issn.1007-7162.2014.03.014.

[7] Ju, C. E., Zhao, X. X, Wang, M. M. and Wen, Y. L., 2018. *Application of Improved Genetic Algorithm in Optical Scheduling of Cloud Computing Resources*. Software Guide.Kunming University of Science and Technology.DOI=http://dx.doi.org/10.11907/rjdk.172641.

[8] Yang, Y. L., Jin, T. B. and Yin, J. Y. 2019. Industrial Control Computer. In *A Scheduling Algorithm for Cloud Computing Resource Based on Genetic and Simulated Annealing Algorithm*,Jiangsu Institute of Automation,China.

[9] Jiang, M. Y. 2013. *Application Research of Genetic Simulated Annealing Algorithm in Cloud Scheduling*,Computer and modernization. College of Computer and Software.

[10] Yie, F. 2014. *Application of Two-Way Convergence Ant Colony Algorithm in Qos of Cloud Computer Computing Resource Scheduling.*Electronics Optics and Control. Vol.21,No.11,Nov.2014. Guangdong Industry Technical College,China.

[11] Xu, F.,Wang, S. and Yang ,W.,2019. *Cloud Resource Scheduling Algorithm Based on Game Theory*. Computer Science. Vol.46,No.6A,June 2019,University of Xi'an Technological.

[12] Calheiros, R. N., Ranjan, R. and Beloglazov, A., CloudSim:A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software:Practice and Experience,2011,41(1):23-5.

Route Optimization by using Dijkstra's Algorithm for the Waste Management System

Mohammad Asif Hossain,
Ismail Ahmedy*,
Muhammad Zar M. Z. Harith,
Mohd Yamani Idna Idris,
Tey Kok Soon
Faculty of Computer Science and Information Technology,
University of Malaya
Kuala Lumpur, Malaysia.
*ismailahmedy@um.edu.my

Rafidah Md Noor
Faculty of Computer Science and Information Technology,
Centre for Mobile Cloud Computing Research
University of Malaya
Kuala Lumpur, Malaysia.
fidah@um.edu.my

Sumiani Binti Yusoff
Institute of Ocean and Earth Sciences,
University of Malaya
Kuala Lumpur, Malaysia.
sumiani@um.edu.my

ABSTRACT
Unplanned waste collection causes environmental pollution, cost increment and large consumption of fuel. Optimized route planning is one of the most important factors in the smart waste management system (WMS). In this work, an optimal route planning model and algorithm based on Dijkstra's algorithm are proposed. For the link-cost calculation, real-life parameters such as the bins' status (fill-levels), road congestion status, distance are considered. Data analysis is done based on the practical scenario. The proposed model is found more cost-effective and Eco-friendly than the conventional model.

CCS Concepts
• **Networks→Network management.**

Keywords
Smart waste bin; smart waste management system, route optimization; Dijkstra's algorithm; smart & green city.

1. INTRODUCTION
In Malaysia, around 38000 tons of waste is generated daily [1] and the number is increasing as the population growth is increasing. One the other hand, in Malaysia, CO_2 emission was recorded in 2018 as 251.52M mt, which had a 7.21% of growth rate [2]. These two statistics are very alarming for our eco-system. Unplanned and inappropriate waste management leads to an unhealthy environment and creates a threat to our lives. A smart and planned waste management system (WMS) is highly needed to achieve green and smart cities.

Traditionally, in Malaysia, waste bins are emptied at certain intervals by the responsible stakeholder and sometimes the waste collection processes are not well scheduled. This causes some drawbacks where some waste bins fill up much faster than the rate of emptying and they are full before the next collection. This problem has consequences where the waste is overflowing and poses an unpleasant view and odor, and hygiene as well as health risks. The impacts of the waste in our lives were described in detail in [3]. There are some special periods such as festivals when the waste bins fill up very quickly and some are not at other places. This situation is a challenge for the stakeholder to maintain a clean city [4].

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388186

There are several elements can be optimized in WMS such as route optimization (to find the best route), labor cost optimization (how many labors will be needed for the waste collection), optimized schedule (the optimum timing for the waste collection), waste collecting truck requirement optimization (how many and which size of trucks are needed and so on), etc. In this work, route optimization and truck requirement optimization has been focused. In conventional WMS, waste has been collected on a daily basis. This is not an efficient system. On the other hand, in some smart WMS, waste has been collected when there is an overflow of the bins. That means waste is collected on an immediate or emergency basis. This is also not an efficient system [5]. In this paper, we have combined both the issues. In this work, waste collection will be done based on the bin's status as well as the distance, road condition (congestion), truck's capacity and so on.

Dijkstra's algorithm [6] is a very popular algorithm in computer science used to solve the single-source shortest paths for a given graph with nonnegative edge weights. In our proposed model and the algorithm, this algorithm has been applied. We have formulated the route from the garage, dumping station and the bins as the computer networking node problem. The link-cost of the routes has been calculated based on the bins' status (fill-levels), distance and road congestion. The garbage truck will follow the shortest path for the waste collection.

The contribution and the advantages of the proposed works compared to other related works:

- Various real-time and practical parameters such as distance between the garage and the bins, the status of the bins, the congestion of the road, etc. have been considered for the link cost calculation.
- The garage, dumping station and the bins are considered as the network nodes and hence simple Dijkstra's algorithm has been applied for the optimized route calculation.
- Some real values have been used for the data analysis such as the cost of the fuel, fuel economy of the truck, CO_2 emission and so on.

- It can be applied with any other WMS network, only need to change the value of the parameters, it does not need any complex tool or algorithm.

The organization of the paper is as follows: section 1 introduces the idea of the route optimization and other optimization requirements in WMS. Section 2 discusses some related works while section 3 discussed the main idea of the work, link-cost calculation method, the proposed model and algorithm. Section 4 discusses the implementation of the algorithm, results, and analysis of the performances.

2. RELATED WORKS

Several works have been done in the route optimization for WMS. In [7], the authors used Life Cycle Assessment (LCA) technique and heuristic approach to solve the vehicle routing problem. They considered the available working time of each collection truck to assign them collection routes and minimize the number of compactor trucks.

Xue and Cao in [8] proposed an ant colony optimization (ACO)-based multi-objective routing model coupled with Dijkstra's algorithm to find the best route from these waste-generating points to the dumping station considering travel time, accident probability (black spots), and population exposure.

In [9], the authors proposed a modified Backtracking Search Algorithm (BSA) to solve vehicle routing problem models with the smart bin concept to find the best-optimized waste collection route solutions.

The authors in [10] described a case study on a real-life waste collection problem in Eastern Finland. They presented a conceptual model based on Dijkstra's algorithm waste collection route optimization. Other related works in this domain can be found in [11]–[13].

These works considered either only road condition or the distance, or the bins' fill level, but not all the aspects. They even did not consider the fuel cost and CO_2 emission from a practical point of view.

3. PROPOSED MODEL & ALGORITHM

As a case study, in Figure 1, a road map of the bins, the garage, and the dumping station has been considered. For simplicity, the garage, the dumping station, and the bins are assumed as the nodes in the graph theory. The garage has been considered as node 0 and the dumping station as node 9, and the bins' nodes are as numbered. For the cost calculation, three parameters have been considered. They are i) the distance between the nodes, ii) the status of the bin (what % it is full), and iii) the congestion of that road. Following equation has been proposed for the link-cost calculation:

$$C = \frac{\alpha D + \beta R_C}{\gamma B_S} \quad (1)$$

Here, D is the distance between the nodes, R_C is the numerical value of the road congestion, B_S is the status of the bin (% occupied or full). α , β , and γ are the tuning factors for the parameters. The sum of these values must be 1. For example, here we have chosen, $\alpha = 0.5$, $\beta = 0.3$, and $\gamma = 0.2$. That means, we have given the highest priority to the bin's status, then the distance of the road and the least for the congestion. These values can be tuned according to the requirement for the link-cost calculation. The hypothesis for selecting the tuning factors is to ensure the priority of the parameters. All the parameters' priority is not the same. For example, the status of the bins has higher priority over the congestion of the road, but it is also true that we cannot avoid the congestion in our calculation. Therefore, these tuning factors are very much important to be considered. If we don't use these factors, all the parameters' importance would be the same, and that is not feasible.

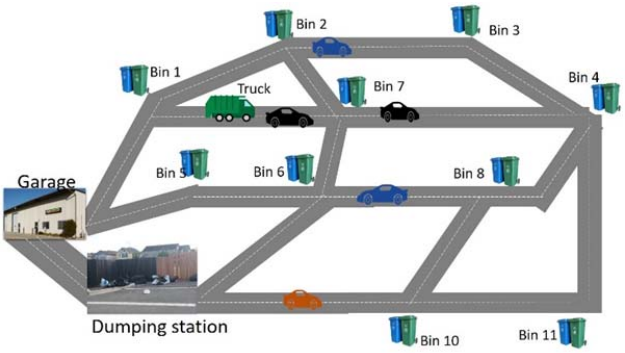


Figure 1. Road map of the bins, garage and dumping station.

Distance is measured in meter and can be measured through the GIS software from the map, IoT (Internet of Thing) based sensors will be used in the bin to measure the status of the bins [14] and the congestion can be measured based on the average speed of the vehicle and the vehicle density. These two values can be measured through the speedometer and the counter sensor by using a laser or ultrasonic sensors. We have calculated the congestion values by using the following concepts:

Table 1. Congestion value calculation

The average speed of the vehicles	Congestion status	Numerical value
0~10 km/h	High congestion	70
11~15 km/h	Medium congestion	50
16~ km/h	Low congestion	30

After calculating the cost, it would be normalized by multiplying with 3 and ceiling the value with the next integer value. These normalized values will be used as the link-cost of the paths for Dijkstra's Algorithm.

After the first step of optimal route selection, the garbage truck will follow the route and collect the bins' waste. After that, the collection bins will be omitted from the graphs. Then again the link-cost will be calculated and another round of Dijkstra's algorithm will be applied. The process will be repeated until all the nodes are visited. The complete algorithm has been given in Algorithm 1:

Algorithm 1

```
for (until all the nodes visited){
    link-cost calculation based on eq. (1)
    Run the Dijkstra's algorithm (Algorithm 2)
    Select the best route and count the nodes selected
    if (number of nodes<=3)
        Use small truck
    else
        Use big truck
    Remove the visited nodes
```

10. Go to step 2 }

Algorithm 2 (Dijkstra's algorithm)

```
1.  function dijkstra(G, S) {
2.    for each vertex V in G
3.      distance[V] <- infinite
4.      previous[V] <- NULL
5.      if V != S, add V to Priority Queue Q
6.    distance[S] <- 0
7.   while Q IS NOT EMPTY
8.    U <- Extract MIN from Q
9.     for each unvisited neighbor V of U
10.      tempDistance<-distance[U]+ edge_weight(U, V)
11.      if tempDistance < distance[V]
             distance[V] <- tempDistance
             previous[V] <- U
12.  return distance[], previous[]; }
```

To evaluate the proposed model and the algorithm, we have considered three cases; i) only a big truck is used to collect the waste, ii) only small truck is used, and iii) both small and big truck are used based on the proposed model and algorithm. We have assumed that small trucks can accommodate only 3 bins' waste and big trucks can carry up to 6 bins' waste. Another assumption is that, for the conventional WMS, everyday trucks are used for the waste collection whether the bins are full or not. But as the proposed model considers the status of the bins for the link-cost calculation, there is very little chance for the bins' overflowed. Therefore, we have assumed that all bins' collection will be done in 2 days. In other words, instead of collecting all the bin's waste in a single day (conventional system), our model will do the same in 2 days. However, if any bin's status goes to 100% full before the collection, the emergency waste collection will be performed. An alert system might be used when the status of the crosses a threshold value (say for example, 90% full). The smaller truck will be used to collect any immediate waste collection. Nevertheless, the probability of being 100% full of the bin within two days is very low and does not impact the overall performance.

4. RESULTS & DISCUSSION

For the implementation of the algorithm and the model, the values of the distance, bins' status, and the congestion values have been considered randomly (but can be replaced easily for any other cases) in Table 2. By using equation (1), Table 1 and based on values of Table 2, link-cost values have been calculated.

Figure 3 shows the steps behind Algorithm 1. Our starting point is the garage (node 0) and the destination point is the dumping station (node 9). At the first step, node 0 > node 1 > node 6 > node 9 will be chosen based on the Dijkstra's algorithm. After that node 1 and node 6 will be removed from the graph and the link cost will be calculated again. Then again the Dijkstra's algorithm will be used to select the best route. In this way, after 4 rounds, all the nodes will be visited and our algorithm will stop.

For the practical point of view, we have assumed that the operational and fuel costs of the big truck are 0.12 RM per meter and it emits 0.04 gm CO_2 per meter traveling while in the case for the small truck they are 0.05 and 0.02 respectively. The fuel cost and CO_2 emission amount have been taken based on [15] and [16] respectively.

Figure 2, 4-5 show the comparative analysis of the proposed model with the only big truck usage and with the only small truck usage. Figure 2 shows the total distance covered by the trucks. It can be seen that if only small trucks are used, more distance it has to cover. If the proposed model is followed, less distance needs to cover per day collection. The proposed model takes around 26.12% less compared to only a big truck case, while 37.08% less than the only small truck case.

Figure 4 shows that the per day costing of the proposed model is very much less than the only big truck usage and only small truck usage cases. The proposed model costs 59.81% and 41.14% less than those cases respectively.

Figure 5 shows that the proposed model is more eco-friendly than in the other two cases. It emits less CO_2 compared to other cases. The proposed model's CO_2 emission is around 55% and 45.08% lesser than those cases.

Table 2. Values of the parameters and the link cost calculation

from link	to Link	Bin status (%fill levels)	distance (m)	Cong-estion	cost	normalized cost (cost*3)
0 (Garage)	1	70	100	50	1.14	4
0 (Garage)	5	50	200	70	2.96	9
0 (Garage)	9 (dump)	8	100	50	10	30
1	2	50	200	30	2.64	8
1	6	50	80	50	1.36	5
1	7	80	100	30	0.9	3
2	3	80	100	70	1.1	4
2	7	80	50	30	0.52	2
3	4	70	80	50	0.97	3
7	4	80	50	30	0.52	2
5	6	50	100	50	1.6	5
6	8	60	80	50	1.13	4
6	7	80	80	50	0.85	3
8	4	70	80	30	0.85	3
9 (dump)	10	40	100	30	1.8	6
10	11	50	200	50	2.8	9
11	4	60	80	50	1.13	4
10	8	70	70	50	0.88	3
6	9 (dump)	60	100	70	1.46	5

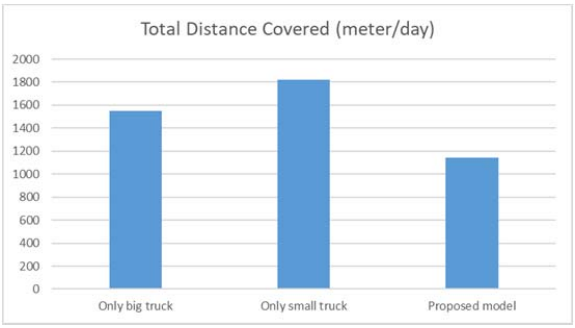


Figure 2. Total distance covered by the trucks in a day.

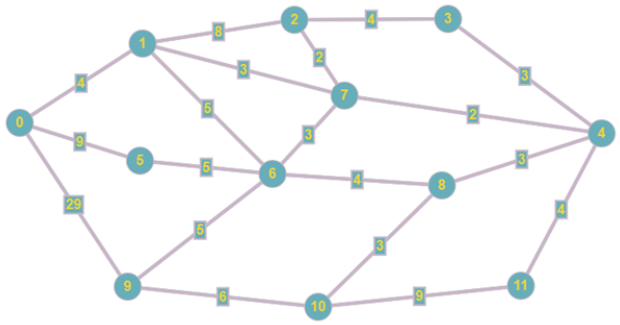
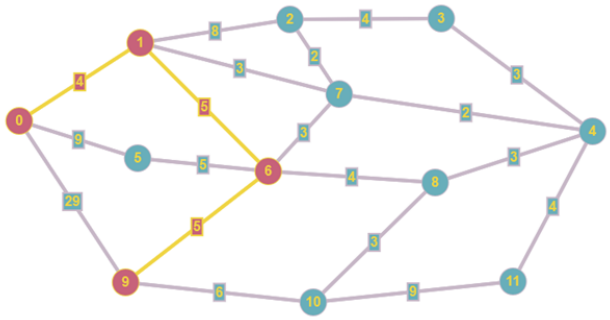
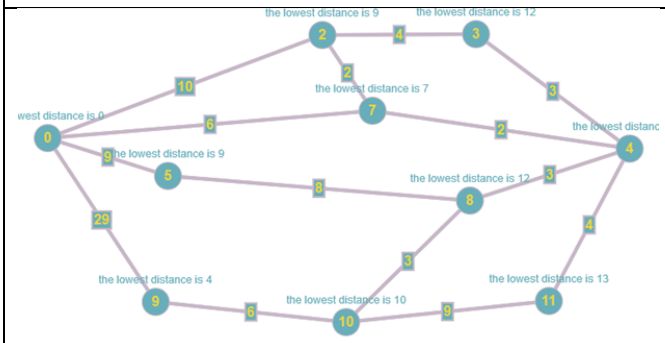
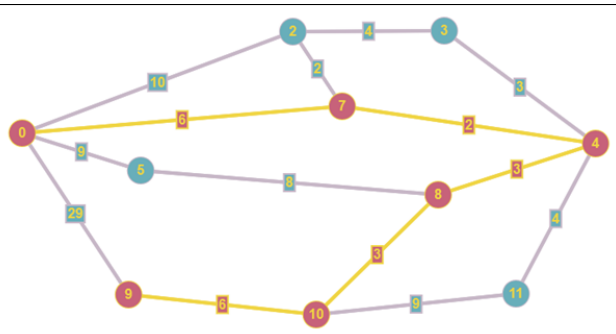
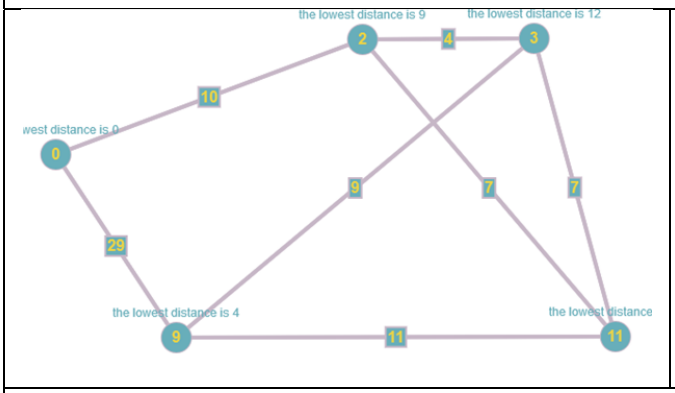
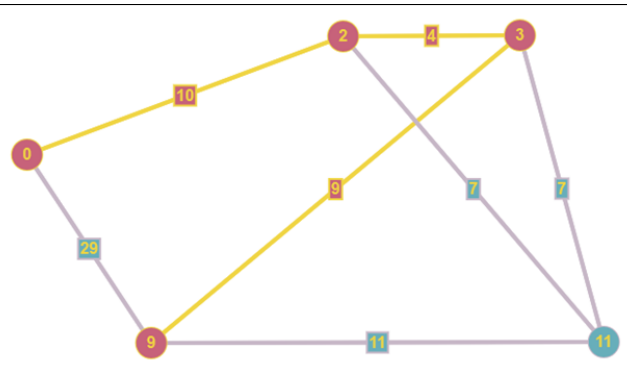
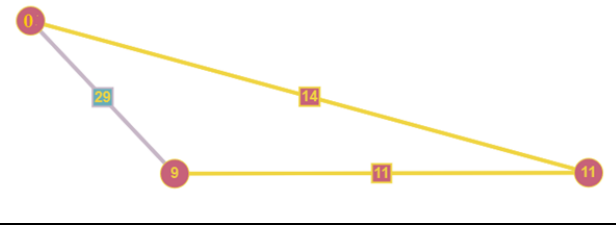
Initial Bin Placement/Reform after waste collection	Shortest path selection by using Dijkstra's Algorithm
	
Step 1: Garage (0)> Bin 1 > Bin 6>Dumping station (9) = Collections of 2 Bins (by small truck)	
	
Step 2: Garage (0)> Bin7 > Bin4> Bin8> Bin10>Dumping station(9) = Collections of 4 Bins (by big truck)	
	
Step 3: Garage (0)> Bin2 > Bin3>Dumping station(9) = Collections of 2 Bins (by small truck)	
	
Step 4: Garage (0)> Bin11>Dumping station(9) = Collections of 1 Bins (by small truck)	

Figure 3. Steps of waste collection using Dijkstra's algorithm.

For the implementation in real-life, the waste collection authority first runs the proposed algorithm with the proposed model. After knowing the best route and the number of bins' waste to be collected, they will send either small or big garbage truck according to the model and the algorithm. In summary, before deploying the truck for waste collection, they will run the algorithm to know the best route and which truck (small or big) is needed. As the bin's level is considered for the route selection, there is no chance of the overflow of the bin's waste. As all the information can be obtained automatically, the whole process would be fully automatic. That means, the route would be automatically determined on a regular basis based on the dynamic changing status of those parameters.

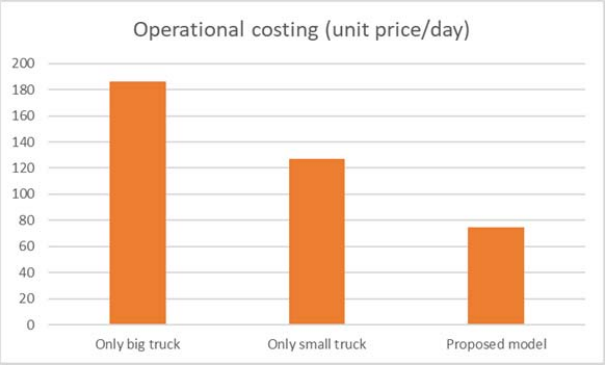


Figure 4. Operational cost comparison.

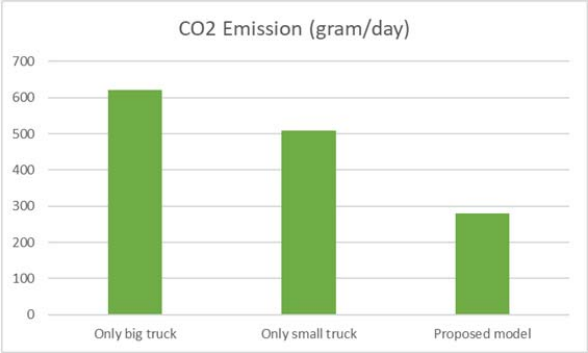


Figure 5. Carbon-dioxide emission comparison.

5. CONCLUSION AND FUTURE WORK

In this paper, a route optimization model and algorithm have been proposed. The algorithm is designed based on Dijkstra's shortest path algorithm. The waste collection problem has been formulated as a single source computer networking problem. Practical values have been considered for the link-costs. The proposed model with the proposed algorithm is found cost-effective, time-efficient and less carbon-dioxide emission.

A prototype of the smart waste management system is under process. After that, this model and algorithm will be verified by using our prototype and the real-life scenarios. Machine learning will be applied to this algorithm for more robust performance.

6. ACKNOWLEDGMENTS

This project is funded by the Malaysia Research University Network (MRUN) Long Term Research Grant Scheme (LRGS) for Smart Waste Campus Program (LR003-2019 and LRGS MRUN/F2/01/2019 /001).

7. REFERENCES

[1] S. L. LEOI, "Malaysians generate 38,000 tonnes of waste every day," *Star 2*, 2019. [Online]. Available: https://www.star2.com/living/2019/05/21/waste-environment-issue/#pFGDIbduVC7EOiLz.99. [Accessed: 11-Jul-2019].

[2] Y. Charts, "Malaysia Carbon Dioxide Emissions," 2018. [Online]. Available: https://ycharts.com/indicators/malaysia_carbon_dioxide_emissions. [Accessed: 26-Sep-2019].

[3] L. Giusti, "A review of waste management practices and their impact on human health," *Waste Manag.*, vol. 29, no. 8, pp. 2227–2239, 2009.

[4] F. Folianto, Y. S. Low, and W. L. Yeow, "Smartbin: Smart waste management system," in *2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2015, pp. 1–2.

[5] X. Bing, J. M. Bloemhof, T. R. P. Ramos, A. P. Barbosa-Povoa, C. Y. Wong,and J. G. A. J. van der Vorst, "Research challenges in municipal solid waste logistics management," *Waste Manag.*, vol. 48, no. 2016, pp. 584–592, 2016.

[6] E. W. Dijkstra, "A note on two problems in connexion with graphs," *Numer. Math.*, vol. 1, no. 1, pp. 269–271, 1959.

[7] A. Gilardino, J. Rojas, H. Mattos, G. Larrea-Gallegos, and I. Vázquez-Rowe, "Combining operational research and Life Cycle Assessment to optimize municipal solid waste collection in a district in Lima (Peru)," *J. Clean. Prod.*, vol. 156, pp. 589–603, 2017.

[8] W. Xue and K. Cao, "Optimal routing for waste collection: a case study in Singapore," *Int. J. Geogr. Inf. Sci.*, vol. 30, no. 3, pp. 554–572, Mar. 2016.

[9] M. Akhtar, M. A. Hannan, R. A. Begum, H. Basri, and E. Scavino, "Backtracking search algorithm in CVRP models for efficient solid waste collection and route optimization," *Waste Manag.*, vol. 61, pp. 117–128, 2017.

[10] T. Nuortio, J. Kytöjoki, H. Niska, and O. Bräysy, "Improved route planning and scheduling of waste collection and transport," *Expert Syst. Appl.*, vol. 30, no. 2, pp. 223–232, 2006.

[11] N. V Karadimas, K. Papatzelou, and V. G. Loumos, "Optimal solid waste collection routes identified by the ant colony system algorithm," *Waste Manag. Res.*, vol. 25, no. 2, pp. 139–147, Apr. 2007.

[12] U. Gazder, "Framework for Route Optimization of Solid Waste Collection," *IET Conf. Proc.*, pp. 39–44, 2018.

[13] A. B. Melo, A. M. Oliveira, D. S. d. Souza, and M. J. d. Cunha, "Optimization of Garbage Collection Using Genetic Algorithm," in *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2017, pp. 672–677.

[14] Muhammad Zar Mohd Zaid Harith, Mohammad Asif Hossain, Ismail Ahmedy, Rafidah Md Noor, Mohd Yamani Idna Idris and Tey Kok Soon, "Prototype Development of IoT Based Smart Waste Management System for Smart City," in *Sustainable & Integrated Engineering International Conference 2019 (SIE 2019)*, 8-9 December 2019, Putrajaya, Malaysia.

[15] Omnicalculator, "Gas calculator," 2019. [Online]. Available: https://www.omnicalculator.com/everyday-life/gas. [Accessed: 04-Oct-2019].

[16] N. R. Canada, "2019 Fuel Consumption Guide," 2019. [Online]. Available: https://www.nrcan.gc.ca/sites/www.nrcan.gc.ca/files/oee/pdf/transportation/tools/fuelratings/2019 Fuel Consumption Guide.pdf. [Accessed: 04-Oct-2019].

A Pedestrian Path-planning Model in Accordance with Obstacle's Danger with Reinforcement Learning

Thanh-Trung Trinh
Shibaura Institute of Technology
3-7-5 Toyosu, Koto-ku, Tokyo
135-8548 Japan
(+81)50-5339-3233
nb18503@shibaura-it.ac.jp

Dinh-Minh Vu
Shibaura Institute of Technology
3-7-5 Toyosu, Koto-ku, Tokyo
135-8548 Japan
(+81)90-6329-5811
nb17502@shibaura-it.ac.jp

Masaomi Kimura
Shibaura Institute of Technology
3-7-5 Toyosu, Koto-ku, Tokyo
135-8548 Japan
(+81)3-5859-8507
masaomi@shibaura-it.ac.jp

ABSTRACT

Most microscopic pedestrian navigation models use the concept of "forces" applied to the pedestrian agents to replicate the navigation environment. While the approach could provide believable results in regular situations, it does not always resemble natural pedestrian navigation behaviour in many typical settings. In our research, we proposed a novel approach using reinforcement learning for simulation of pedestrian agent path planning and collision avoidance problem. The primary focus of this approach is using human perception of the environment and danger awareness of interferences. The implementation of our model has shown that the path planned by the agent shares many similarities with a human pedestrian in several aspects such as following common walking conventions and human behaviours.

CCS Concepts

• Computing methodologies → Neural networks • Computing methodologies → Agent / discrete models • Applied computing → Law, social and behavioral sciences.

Keywords

Pedestrian; navigation; path planning; reinforcement learning; PPO.

1. INTRODUCTION

Recent studies in pedestrian simulation are often fixated within one of the three categories assorted by the level of interaction: *macroscopic*, *mesoscopic* and *microscopic* [1]. The macroscopic simulation models use the concept of fluid and particles originated from physics to construct pedestrian navigations while ignoring the interactions between pedestrians as well as individual characteristics of each pedestrian. For an excessively high-density crowd, a macroscopic model could be sufficient; however, for a smaller size of pedestrians where social interactions are essential, a mesoscopic or microscopic model would be more suitable. A mesoscopic model sits between macroscopic and microscopic, which is still able to simulate a relatively large-sized environment but with the cost of agent's movements and interactions. Compared to mesoscopic, a microscopic model is more realistic as each pedestrian is considered as an independent object or a computer agent whose behaviours and thinking processes could be modelled upon.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388187

Most microscopic pedestrian simulation models use the concept of "forces" applied to the pedestrian agent to replicate the navigation behaviour [2]. The basic idea of these models is that pedestrian agents are attracted to a specific point-of-interest (e.g. pedestrian's destination) and repulsed from possible collisions (e.g. walls, obstacles and other agents). The representation of the force-based models is similar to the interactions between magnetic objects with some certain improvements. There is undoubtedly a sufficient resemblance in basic movement and collision avoidance with the implementation of the model in a simulation. However, when comparing with pedestrian navigation in real life, many human decisions which require strategical thinking or social interacting are not reflected in the force-based simulation. For instance, when an agent plans a path to go from its current position to a destination, a force-based agent often chooses the shortest path without colliding into other obstacles most of the time. In real life, a human pedestrian has many other aspects affecting his decision such as social comfort, law obeyance or his personal feeling. This could be a problem if the simulation needs the preciseness of pedestrian behaviour, for instance, a traffic simulation system for automated vehicles.

The main idea of our research is adopting reinforcement learning in the pedestrian agent's decision-making process. Reinforcement learning is a machine learning paradigm based on the concept of *reinforcement* in behavioural psychology, in which the learner needs to find an action in the current state for an optimum reward. The concept is virtually close to the way humans learn to behave in many real-life situations, including path navigation. When a person plans a path to the destination and feels uncomfortable with his decision, for instance, because of taking a longer path or colliding with obstacles, he will then receive a negative reward and will try to improve his behaviour. As a result, once an environment is observed, that individual will be able to come up with a path using his current optimum policy without the needs of various calculation such as "forces" realised in many microscopic pedestrian models.

The remainder of this paper is structured as follows: The next section provides an overview of studies related to our research. Section 3 presents the backgrounds of reinforcement learning and the *Proximal Policy Optimization* (PPO) algorithm. After that, we describe the methodology in our path planning model in Section 4. The modelling of our model and the formulation of our rewarding

behaviour will be presented in Section 5 and Section 6, respectively. In Section 7, we present the implementation of our model and evaluation with a conventional rule-based model.

2. RELATED WORK

One of the most influential algorithms in microscopic pedestrian simulation is the *Social Force Model* (SFM) by Helbing *et al.* [3]. The concept of this model is that each pedestrian agent will be under influences of different social forces, including driving force, agent interact force and wall interact force. The driving force attracts agent toward the destination, the agent interact force repulses agent from other agents, and the wall interact force repulses agent from walls or boundaries. Since SFM was introduced, there have been a variety of models formulated based on SFM However, such models do not take account of the cognitive thinking process within the human brain, which leads to many deviations from actual human behaviour.

Regarding research in human behaviour, many studies can be found in the field of robotics research. Many researchers have tried to solve the problems in *human comfort* and constructing naturalness [4]. For an agent to navigate naturally, not conflicting with other pedestrians or obstacles is not enough; but the agent also needs to replicate different behaviours from humans. Another concept proposed in human behaviour research is *human bias* or *cognitive bias*, which causes the anomaly in the human decision process. For example, in [5], Golledge *et al.* have shown that pedestrians do not always choose the most optimised decision while selecting a path. Another study by Cohen *et al.* [6] also discussed how the human brain making decisions between exploitation and exploration. These aspects were supportive for forming the agent behaviour in our research.

In using reinforcement learning for pedestrian navigation, the amount of research is moderately limited. In a study by Martinez *et al.* [7], an experiment in using reinforcement learning for a multi-agent navigation system has been implemented; however, the algorithm used was q-learning which is too simple and does not suit well to a dynamic environment. Another approach is learning from observing examples from human behaviour. In their paper by Kretzschmar *et al.* [8], a navigation model was proposed using inverse reinforcement learning. One difficulty in such approach is the example or the dataset from human behaviour is not easy to be extracted or readily available.

3. BACKGROUND

3.1 Reinforcement Learning

Reinforcement learning was first introduced by Surton *et al.* (1998) [9]. A reinforcement learning agent learns to optimise the *policy*, the mapping from a (possibly partial) observed *states* of the environment to *action* to be taken, in order to maximise the expected cumulative *reward*. Different to supervised learning, instead of using existing inputs and outputs, the reward will be given by using the *reward signal*. This could be inferred as a positive or negative experience from humans (such as satisfied or discomfort) in a biological system. However, a positive or negative reward is intermediate, which means that an action is considered bad at that moment but could also yield a better result in the long run. As a result, a reinforcement learning system also needs a *value function* to define the expected long-term reward positivity.

3.2 PPO Algorithm

Many modern reinforcement learning algorithms employ different deep learning techniques to optimise the total cumulative reward. These approaches use the neural network training process to optimise the agent's policy. They often calculate an *advantage value* $\widehat{A_t}$ by comparing the expected reward over the average reward for that state. The advantage function will be then used in the loss function of the neural network, which is consequently trained for a number of steps and outputs the most optimised policy.

For algorithm like Policy Gradient, the policy $\boldsymbol{\pi_\theta(a_t \mid s_t)}$ will be constantly updated after every training step. With a noisy environment, the old policy $\boldsymbol{\pi_{\theta\ old}(a_t \mid s_t)}$, which might actually be better than the new one, will be overwritten; causing the training process to be less efficient. The algorithm PPO introduced by Schulman *et al.* [10] tried to avoid that problem. The objective of the algorithm is to avoid staying away too far from a good policy by keeping the old good policy and compared with updated one using a more efficient loss function.

4. PATH PLANNING MODEL

To design our model of pedestrian path planning and collision avoidance using reinforcement learning, we had to address the following problems: the definition of the environment and the formulation of the rewarding behaviour.

Regarding the definition of the environment, one difficulty is that the model of the designed environment cannot be too complicated. If the environment is too complex (e.g. too large or too many obstacles); the agent might not be able to learn the appropriate behaviour, or it could take an excessive amount of time. In addition to that, the environment also needs to provide a stable training process, or the variation between each training states should be balanced. For the former problem, we limited our environment to a relatively small area with an appearance chance of one obstacle, assumed that a more complex walking environment could be divided into smaller paths. For the latter problem, we introduced a mechanism for resetting the environment to balance the proportion between the cases when there is an obstacle present and ones when there is none. For instance, if the agent fails to navigate without collision with an obstacle when there is one; but in the next training step, there is no obstacle so the agent could produce a path without collision. This could make the agent incorrectly thinks that the current policy is a good one, while it is probably not. As a result, instead of resetting every training step, we suggested resetting the environment only when the agent has already planned a path without conflicting with the obstacle. If the agent fails, we retained the states of the environment for a number of iteration before resetting so that the agent could gain enough experience without being stuck in a bad policy.

We also introduced a definition to the obstacle in our environment so that the agents could output a natural path around it. Different to a physical obstacle in real-world (e.g. a rock, a wall or a construction site), the term obstacle in our research represents the feeling of interference while planning a path. For example, a group of people engaging in a conversation in the middle of the walking area could also be considered as an obstacle. Although there could be a considerable amount of possible walking space within the group's territory, planning a path through this area is considered rude or unusual for a normal person. In a study by Chung *et al.* [11], such areas are called the "spatial effect" in an environment. As the process of constructing a spatial effect area is carried out in the human cognitive system, the interpretation of an obstacle could be slightly different for each person or in different situations (e.g. the crossroad when the traffic light is green or red).

Apart from position, we proposed two properties to our obstacle: *size* and *danger level*, which should have a great impact on the path planned by the agent as suggested in several studies [12]. The size of the obstacle should cover the concept of spatial effect mentioned above, not just the size of the physical obstacle. For example, a damaged or unstable power pole would have a much larger "size" compared to a steady or stable one due to the fear of the pole falling. For simplicity, we assume our obstacle has a round shape; thus, the size of an obstacle will be expressed by a *radius* value. In terms of the danger level, similar to obstacle's size, is also a concept formed within the human mind. The feeling of danger level could have a great impact on the process of planning a path by a pedestrian. For example, in the two settings illustrated in **Figure 1** below, on the left is an obstacle such as a water puddle which has a much less danger level compared to a deep hole on the right. As a result, the planned path would normally stay much further away from the hole than from the puddle. A more detailed description of the obstacle properties was shown in the technical report [13]. The concrete modelling of the environment will be presented in Section 5.

Figure 1. Path planned by an agent in different settings.

In addition to the modelling of the environment, we need to specify the appropriate reward function to the agent. For each taken action, the agent needs to know if the action is possibly good or bad based on the given reward. Different from rule-based methods, in reinforcement learning, rewards are often given based on the results of the agent's actions to help the agent in shaping the behaviour. An improper rewarding, for example, giving a large penalty for an undesirable action might cause the agent to avoid such action completely, although there might be a chance that the action could lead to a higher cumulative result in the long run. Another problem with rewarding is that the agent does not receive each specific reward for each behaviour but only the total reward for every action. While this is corresponding to the concept of reinforcement in human cognition, shaping a specific behaviour is much harder compared to in rule-based methods.

As a result, we chose to formalise our rewarding behaviour based on various factors affecting *human comfort* which were summarised in an article by T. Kruse *et al.* [4]. These are a number of factors applied to robot movement which may cause humans to observe its movement as more natural or human-like. Consequently, a human being should feel the same level of comfort when exhibiting similar behaviour. We will thoroughly present our rewarding formulation in Section 6 of this paper.

5. ENVIRONMENT MODELLING

The modelling of our environment is presented as illustrated in **Figure 2**. In the scope of our research, the size of our environment is limited to an area of 22 meters by 10 meters; the current position of the pedestrian agent will be placed between (-5, -12) and (5, -12); the desired destination of the agent will be placed between (-5, 10) and (5, 10).

The obstacle has a random chance of appearing in the environment. Each obstacle has a *size* ranged from 0.5 to 2 meters and a *danger level* ranged from 0 to 1.

The objective of our research is to let the pedestrian agent plan a path from its position to a pre-defined destination. In order to do this, the agent must observe the environment then provide a path using its current policy. In our model, the agent path is constructed from 10 outputs of the neural network, corresponding to 10 component path nodes' relative x positions. Appropriately, the component path nodes' relative y positions are {-10, -8, -6... 6, 8}.

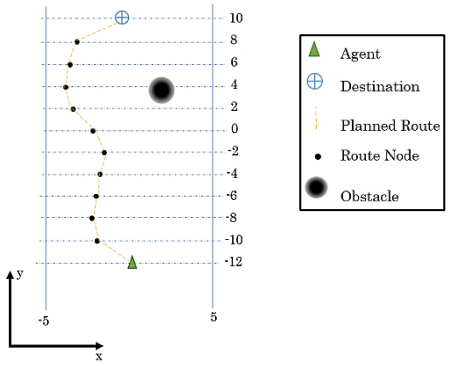


Figure 2. Path-planning model.

Specifically, for each training step, the pedestrian agent observes the following values:

- Relative x positions of agent's current position and its desired destination
- The presence of the obstacle. If the obstacle is present, the agent will observe the relative position, size and the danger level of the obstacle.

The taken action of the agent, which is the planned path in this case, will then be rewarded based on the rewarding behaviour discussed in Section 6. After that, the training step is terminated and the new training environment will be initialised.

6. REWARDING FORMULATION

As suggested in Section 4, we formulise our rewarding behaviour based on the idea of *human comfort*. There are many factors that could affect human comfort level, but within the scope of research, we employed the following factors:

- Choosing the shortest path to the destination.
- Encouraging actions following the basic rules or common sense.
- Discouraging the changing of direction.
- Avoid getting through restricted regions.

Choosing the shortest path to the destination, as discussed in [5], is not always optimised for path planning but still has a very high priority in the process. For calculating the reward, we used the negative of the sum of all squared lengths of all walking paths. The bias *b* used in the reward is for providing a positive reward to the agent when a satisfactory path is taken. The rewarding for taking the shortest path is formulated as follows

$$\mathcal{R}_1 = -\sum_{i=0}^{11} \|p_i\|^2 + b \tag{1}$$

where p_i is a vector representing the path from the previous node to the next node in the agent's planned path and b is the bias.

For discouraging changing direction, we added a small penalty when a change in direction is greater than 30°. The reason for this is that in human navigation, a minor change in direction is still considered acceptable. The rewarding for changing direction is formulated as follows

$$\mathcal{R}_2 = -\sum_{i=0}^{10} \theta(angle(p_i, p_{i+1}) - 30) \tag{2}$$

where *angle*(p_i, p_j) is the value in degree of angle formed by two vectors p_i and p_j; $\theta(x)$ is the Heaviside step function which is defined as

$$\theta(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases}$$

In terms of following the basic rules or common sense, this could be varied depends on regional laws and cultures. In the scope of our research, we implemented the following principles:

- Favour going parallel to the sides. This will help the agent maintain the flow of the movement in the road.
- Following the left side of the road (or the right side, in case of right-side walking countries). Although pedestrians are not explicitly required by the laws to follow this convention in many countries, many people still follow the convention as a rule of thumb in the decision-making process in many situations.
- Avoiding getting too close with the boundaries. As discussed in several studies, especially rule-based models, this is for avoiding accidental injuries when colliding with walls or surrounding objects. [3]

To implement these, we simulated the navigation along the path by sampling the planned path into N samples s_i, then calculate the appropriate rewards

$$\mathcal{R}_3 = -\sum_{i=0}^{N} \|x\_position(s_{i+1}) - x\_position(s_i)\| \tag{3}$$

$$\mathcal{R}_4 = -\sum_{i=0}^{N} \theta(-x\_position(s_i)) \tag{4}$$

$$\mathcal{R}_5 = -\sum_{i=0}^{N} \theta(\|x\_position(s_i)\| - 4.5) \tag{5}$$

where *x_position* function is for getting the x coordinate of the position s_i.

Obstacle avoidance is probably the most essential criteria in path planning as it directly affects the pedestrian's safety. In real life, humans often try to keep a certain distance from the obstacle's centre, but once the distance is assured, the priority in the path planning process will shift to other interests. In the idea of reinforcement learning, when the path does not conflict with the obstacle area, a further distance from obstacle will not provide a higher reward. This idea was formulated in our rewarding for avoiding obstacle as follows:

$$\mathcal{R}_6 = \sum_{i=0}^{N} \begin{cases} \frac{\delta(s_i, obs)}{{r_{obs}}^2} * {danger_{obs}}^2, & \text{if } \delta(s_i, obs) \leq 0 \\ 0.01 * {danger_{obs}}^2, & \text{if } \delta(s_i, obs) > 0 \end{cases} \tag{6}$$

with $\delta(s_i, obs) = d(s_i, obs)^2 - {r_{obs}}^2$,

where $d(s_i,obs)$ is the distance from the sampled position s_i to obstacle's position; r_{obs} and $danger_{obs}$ are the radius and the danger level of the obstacle area, respectively.

The cumulative reward is calculated by the sum of all component rewards mentioned above, each was multiplied by an appropriate coefficient:

$$\mathcal{R} = \sum_{i=1}^{6} \mathcal{R}_i * \kappa_i \tag{7}$$

where $\boldsymbol{\kappa}_i$ is the coefficient for rewarding of each reward.

These coefficients represent the proportion of importance of each reward, which can be different between agents. Variation of these coefficients could alternate the output results, and by that can be a representation of different human personalities. For example, a law-obedient pedestrian could use a high value for the coefficient of walking in the left side, while a cautious agent could use a high value for the coefficient of obstacle avoidance.

7. IMPLEMENTATION AND DISCUSSION

The realisation of our model was made available using Unity-ML [14], a framework which functions as a communicator between Python using TensorFlow and the 3D graphics engine Unity. For each training step, we initialise our environment then let our agent observes the current state. After that, these signals are sent to Python via the communicator for the training process. The output of the neural network using PPO algorithm will be then sent back to Unity and used for positioning the coordinates of each path node. The cumulative reward is calculated based on the output path and sent to Python for the training process.

We built the model for the environment entirely within Unity environment. The environment states could be excessively noisy; therefore, a large size of batch is required. For faster training, we concurrently trained the model using 10 copies of the same environment. We have been able to successfully train the model with a batch size of 20480, buffer size of 204800 and the learning rate of 1.5e-3 in three million steps. As can be seen in **Figure 3** as follows, the reward has seemed to be converged at around -0.3.

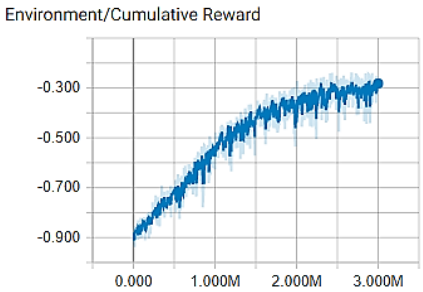


Figure 3. Cumulative reward statistics.

Using the trained model for pedestrian agent's path planning action, the behaviour can be observed from the results presented in **Figure 4**. The environment condition represented in each situation is, respectively: (a) No obstacle; (b) Obstacle area outside agent's path; (c) Obstacle area within agent's path, danger level = 0.1; (d) Same obstacle area with danger level = 1. The path using RL (our model) is on the left and the path using SFM is on the right.

From observation, generally, it can be said that the agent's path resembles a human person's decision of forming a walking path.

In (a), the figure shows that the agent by our model planned a relatively short path that still conforms the walking convention such as walking on the left side of the road and changing direction naturally. On the contrary, the path formed by SFM leads the agent to go straight to the destination. In (b), there is an obstacle but outside of the agent's common planned path. The obstacle, in this case, has little to no effect on the result of its planned path; therefore, there are little changes to the path compared to the situation in (a). Similarly, no change was observed in the path formed by SFM as well. In (c), the obstacle now is in the agent's common planned path. In this case, the danger level of the obstacle perceived by the agent is very small, so our agent only tried to modify the path just enough to not conflict with the obstacle. As for the path by SFM, the agent still chooses to go straight to the destination and only try to avoid the obstacle when being close to it. When the danger level perceived was increased as in (d), our agent tried to stay away from the obstacle much further. As can be seen from the figure, there are parts of the planned path positioned slightly on the right side of the road. Also, the total length of the path is also not the shortest. This path has replicated the common behaviour from humans to ensure their highest safety while walking on the road. The danger level is not present in SFM, therefore there is no change to the path compared to the situation (c).

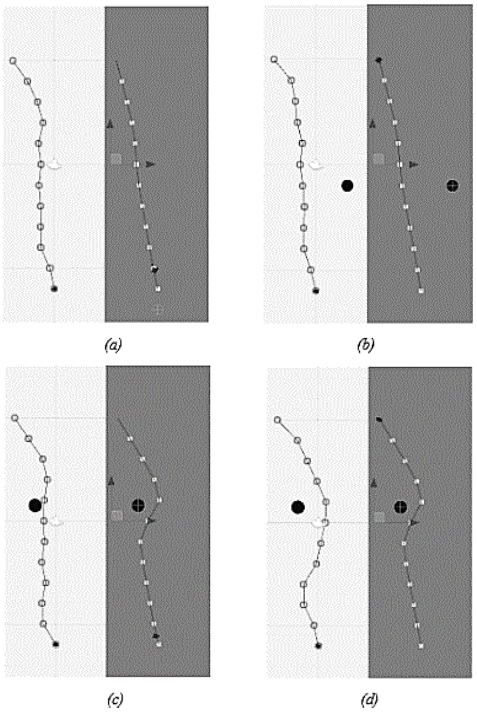


Figure 4. Agent's planned path in different situations.

Compared to a force-based model, SFM in particular, our model has the advantage of replicating the natural behaviour of human navigation. Although a rule-based model, e.g. a finite state machine model, might be able to mimic the exact behaviour precisely, it is prone to have the limitation of the finite number of rulesets. Reinforcement learning, on the hands, has the advantage of creating diversity on human behaviour thanks to the shared concepts between neural network and reinforcement in machine learning and in real life.

However, our model is still in early-stage and require much further research in order to replicate a perfect pedestrian behaviour in multiple situations. The obstacle, for one, cannot represent a moving agent such as automobile or another pedestrian. The reason for that is when encountering with a moving obstacle, the agent needs different ways to plan a path. For instance, the agent might need to plan ahead by making predictions, as discussed in [14]; or adapt to the changes in the environment and make decisions synchronously. Another limitation of our research is the lack of changing in the agent's velocity. The variation in speed of pedestrians is also a major factor in replicating a natural walking behaviour. In the future, we will conduct further research to address these problems using the result presented in this paper as a groundwork.

8. CONCLUSION

We have proposed a novel reinforcement learning model for pedestrian agent path planning and collision avoidance. The implementation of our model has shown that the agent is able to plan a natural path to the destination while avoiding colliding with the obstacle in different situations. The planned path shares many similarities with a human pedestrian, following common walking conventions and human behaviours such as walking on the left side of the road and staying away from dangerous obstacles.

9. REFERENCES

[1] Ijaz, K., Sohail, S. and Hashish, S., 2015, March. A survey of latest approaches for crowd simulation and modeling using hybrid techniques. In *17th UKSIMAMSS International Conference on Modelling and Simulation*, pp. 111-116.

[2] Teknomo, K., Takeyama, Y. and Inamura, H., 2000. Review on microscopic pedestrian simulation model. In *Proceedings Japan Society of Civil Engineering Conference*.

[3] Helbing, D. and Molnar, P., 1995. Social force model for pedestrian dynamics. *Physical review E*, *51*(5), p.4282.

[4] Kruse, T., Pandey, A.K., Alami, R. and Kirsch, A., 2013. Human-aware robot navigation: A survey. *Robotics and Autonomous Systems*, *61*(12), pp.1726-1743.

[5] Golledge, R.G., 1995. Path selection and route preference in human navigation: A progress report. In *International Conference on Spatial Information Theory*, pp. 207-222.

[6] Cohen, J.D., McClure, S.M. and Yu, A.J., 2007. Should I stay or should I go? How the human brain manages the trade-off between exploitation and exploration. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *362*(1481), pp.933-942.

[7] Martinez-Gil, F., Lozano, M. and Fernández, F., 2011. Multi-agent reinforcement learning for simulating pedestrian navigation. In *International Workshop on Adaptive and Learning Agents*, pp. 54-69.

[8] Kretzschmar, H., Spies, M., Sprunk, C. and Burgard, W., 2016. Socially compliant mobile robot navigation via inverse reinforcement learning. *The International Journal of Robotics Research*, *35*(11), pp.1289-1307.

[9] Sutton, R.S. and Barto, A.G., 1998. *Introduction to reinforcement learning* (Vol. 2, No. 4). Cambridge: MIT press.

[10] Schulman, J., Wolski, F., Dhariwal, P., Radford, A. and Klimov, O., 2017. Proximal policy optimization algorithms. *arXiv preprint arXiv:1707.06347*.

[11] Chung, W., Kim, S., Choi, M., Choi, J., Kim, H., Moon, C.B. and Song, J.B., 2009. Safe navigation of a mobile robot considering visibility of environment. *IEEE Transactions on Industrial Electronics*, *56*(10), pp.3941-3950.

[12] Melchior, P., Orsoni, B., Lavialle, O., Poty, A. and Oustaloup, A., 2003. Consideration of obstacle danger level in path planning using A∗ and fast-marching optimisation: comparative study. *Signal processing*, *83*(11), pp.2387-2396

[13] Trinh, T.T. and Kimura, M, 2019. Reinforcement learning for pedestrian agent route planning and collision avoidance, IEICE Tech. Rep., vol.119, no.210, SSS2019-21, pp. 17-22.

[14] Juliani, A., Berges, V.P., Vckay, E., Gao, Y., Henry, H., Mattar, M. and Lange, D., 2018. Unity: A general platform for intelligent agents. *arXiv preprint arXiv:1809.02627*.

[15] Ziebart, B.D., Ratliff, N., Gallagher, G., Mertz, C., Peterson, K., Bagnell, J.A., Hebert, M., Dey, A.K. and Srinivasa, S., 2009, October. Planning-based prediction for pedestrians. In *2009 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pp. 3931-3936.

Resolving XACML Rule Conflicts using Artificial Intelligence

Bernard Stepien and Amy Felty
School of Electrical Engineering and Computer Science
University of Ottawa
Ottawa, Canada
{bstepien, afelty}@uottawa.ca

ABSTRACT

The XACML access control policy specification language provides a simple rule/policy combining algorithm that is invoked when a request is evaluated against a particular policy set, and the results of the policy decision point (PDP) include solutions with both "permit" and "deny" effects. In short, the combining algorithm allows the policy writer to specify which effect should prevail in case of such conflicts. This feature has long been considered as misleading, and a wide variety of research has been done in an attempt to extend it using supplementary language features or algorithms based on priority definitions. We propose a new algorithm that, instead of absolute priorities expressed as numbers, is based on relative priorities that do not use numerical scales. Two kinds of annotations need to be added to policies, one that says if the value of an attribute is sensitive and another that provides information that can be used to determine which attribute is most important in the case when several sensitive values are encountered during the processing of attribute values in a request. This information serves as input to our decision making mechanism, designed to respect the user-specified priorities as best as possible.

CCS Concepts

• General and reference→General conference proceedings • Theory of computation→Logic and verification •Security and privacy→Access control •Computing methodologies→Knowledge representation and reasoning •Computing methodologies→Anomaly detection •Computing methodologies→Policy iteration.

Keywords

XACML; access control; Prolog; artificial intelligence; logical reasoning.

1. INTRODUCTION

XACML [1], [2] is an XML based language for specifying access control policies. It is highly expressive and includes a rich set of datatypes, complex logical expressions and an unlimited number of user-selected attributes. However, it is very verbose and thus large specifications become rapidly unreadable by human readers. It also includes a conflict resolution algorithm which is used when several policies match the values of an access control request and yield conflicting effects (permit/deny) or conflicting obligations. In this case, this algorithm provides the policy maker with a choice of three strategies: first-applicable, permit prevails and deny prevails. While these algorithms were thought to be satisfactory in early implementations of XACML, the increasing use of XACML in industry led to the awareness that these algorithms were, in fact, not satisfactory and sometimes even led to dangerous situations. Consequently, this resulted in extensive research and eventually in new algorithm definitions in version 3.0 of XACML. Among the many proposals, we mention a few that characterize specific approaches. One of the main issues with XACML is to know whether the logic of a XACML policy set can be considered as a pure Boolean expression. Some people ascertain that theory while others deny it on the basis that a XACML policy set has rule/policy combining algorithms that they consider an integral part of the decision logic [3].

A large portion of literature on the subject of rule and policy conflict resolution is based on the belief that a conflict is an error [4] and thus must be eliminated. Thus, research on static and dynamic conflict detection at compile time has prevailed. However, when looking closely at the intention of XACML, instead we discover that policies and rules define authorization spaces for which they are specifically applicable. This is described fully in [5]. However the problem of determining with accuracy which rule prevails in case of an overlap of authorization spaces remains. Also, since policies and rules are composed by various actors who insert different rules at different times, it is difficult to constantly clean the policy sets or policies of such conflicts as discussed in [6]. Instead, it is more appropriate to define methods to determine which policy and rule is applicable in a certain context.

The following medical example is of particular interest because it provides a good illustration of the weaknesses of the XACML rule combining algorithm. Here we are trying to specify the conditions under which a nurse can access electronic records (action *read*). The first rule specifies that a nurse can read a surgery report without further restrictions. The second rule prohibits nurses from reading any document when the location is home care. And finally, the third rule has no restriction on resources or location but operates in the case of an emergency, i.e. a nurse can read anything and anywhere in an emergency. The following policy set can be viewed as a depiction of a horizontal tree. It illustrates the hierarchy of XACML elements showing the name of the XACML

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388188

element and its corresponding target logic. The corresponding full XACML specification is left as an exercise to the reader.

```
01 policySet ConflictingPolicySet :=
02        subject-id matches nurse
04  policy NurseReadPolicy :=
05              action-id matches read
06
07    rule NurseResourceRule -> permit :=
08         resource-id matches surgery report
09
10    rule NurseHomeCareRestrictionRule -> Deny
11         := Location matches home care
12
13    rule NurseEmergencyRule -> Permit :=
14         Emergency matches true
```

In this example, it is clear that the home care rule conflicts with the resource rule and with the emergency rule in the case of a request of {*subject-id = nurse, action-id = read, resource-id = surgery report, Location = home care, Emergency = true*}. Here the use of the XACML rule combining algorithm would produce the following undesired effects:

- Deny prevails would prevent a nurse from reading any document during an emergency.
- Permit prevails would allow a nurse to read documents during home care.

Instead, these three rules provide a complex example of conflicts depending on the situations encountered. Basically, we want the *NurseHomeCareRestrictionRule* to prevail in order to deny access in the case when the location is *home care* and there is no emergency, but we would like to see the *NurseEmergencyRule* prevail to allow access regardless of the location. This example is a case of cascading conflicts that cannot be resolved by a simple XACML rule or policy combining algorithm. This conflict cannot be considered as an error and should not be corrected by removing any of its logic. The traditional recommendation of cleaning the policy of conflicts would also be undesirable because XACML rules can specify only one type of effect, *permit* or *deny*. By cleaning, we mean removing some of the rule logic that is posing a problem.

Also, some may argue that the use of the first-applicable rule combining algorithm and a proper ordering of the rules would solve the problem. It is highly recommended to avoid this. Most industry users that we have talked to have prohibited the use of the first-applicable rule combining algorithm altogether, due to bad experiences using it. In fact, while this algorithm is usable for the above small example, larger policy sets with hundreds or even thousands of rules would easily become unmanageable when trying to determine the correct order. Thus, most authors have decided to come up with new algorithms altogether.

We propose a new solution to deriving the final desirable effect. Instead of any modification such as cleaning, our approach keeps the logic of these three rules (and all rules) intact, and adds a new priority mechanism, based on simple sensitivity assessments of attributes. This mechanism is used in place of the traditional XACML rule/policy combining algorithm. However, we do not use a numerical method such as the one in[7], where priorities are scaled during the evaluation of a request against a policy set, in the process of determining the desired effect. Instead, we propose to use artificial intelligence in the form of automated logical reasoning, which relies on a two-step process of declaring relative priorities: the first step consists of determining which values of an attribute are sensitive, and the second consists of declaring which attributes are more important than other attributes. This information will be used when conflicting cases are encountered. This approach handles the concept of defining authorization spaces as in [5], however without the rule combining algorithm.

The specification of rules is based on the fact that in the absence of an appropriate target logic (i.e., when no policy rule applies), a request would return "not applicable," which is considered as an implicit *deny*. Thus, an explicit *deny* is really meant to ensure that a rule specifying a *permit* effect should exclude any cases covered by rules with an explicit *deny* specification. The problem is that the reverse may also be true.

Although it may appear that our approach supersedes the various methods for conflict detection, we note that these methods can still be very useful. Indeed, they provide material to a policy set administrator that can help to define adequate priorities among authorization spaces. This situation may arise often, mostly because users who define policies may not be aware of other users' policies as indicated in[8]. Also, there are still cases that can be considered as pure errors for which a priority algorithm proves useless. This is the case, for example, when solutions contain exactly the same attributes operating on the same values, such as in the following simple example:

Rule 1: A_1 matches V_1 /\ A_2 matches V_2 => permit
Rule 2: A_1 matches V_1 /\ A_2 matches V_2 => deny

2. BACKGROUND

The list below contains a sample of approaches to conflict detection resolution during the evaluation of requests against access control policies.

[9] proposes an algorithm based on deterministic formal automata, based on matrices representing the effect of a pairwise policy.

[10] proposes an ordered set of conflict resolution rules (CRR). This is in the context of multiple PDPs in collaborative systems.

[11] proposes a system of prioritization of rules and policies using numerical rankings and performing complex operations like computing Eigen values to determine which rule prevails.

[12] proposes a variety of priority concepts as follows:

- Absolute ordering where policies and rules are ordered and the highest order has priority.
- Deny by default where deny effects of rules have priority over permit cases.
- Obsolescence where more recent rules have priority over older rules.
- Specificity where a specific rule overrides a more general rule.
- Authority where a policy defined by a higher authority has priority.
- Privileges where the policy with the strongest rights has priority over weaker rights

[5]proposes a conflict resolution mechanism based on effect constraints of conflicting segments. First, conflicting segments are defined and then a reordering of conflicting segments is compulsory. Basically, no changes are made to the user specified combining algorithms.

[13] proposes a method using the concept of various degrees of majority for a given effect.

[14] proposes an ordering of attributes to determine which attributes are more important in making decisions using weights.

Among the above approaches to resolve rule conflicts at runtime, two stand out: one for the RBAC model in [5] and one for the ABAC model in[11], with the latter one being derived from[14].

3. PRIORITY-BASED CONFLICT RESOLUTION

3.1 Difficulty Determining Exceptions

One of the potential solutions we have explored involves no changes to the policy specification language. In this approach, we defined rules that express exceptions. In the presence of such rules, there are several ways to try to resolve the conflicts:

- Consider all rules as exceptions.
- Consider the fact that some rules have broader coverage than others.

In the above example, the first rule *NurseResourceRule* is restricted only to the document *surgery report*, while the second rule *NurseHomeCareRestrictionRule* has no restriction involving *surgery report*, and actually applies to any value of attribute *resource-id*. It is restricted only to location *home care*. But the reverse is also true so that there is no way to determine which rule has a broader coverage than the other. Indeed, both have broader coverage, but not on the same attribute. Consequently, the only way to determine which rule should win is to apply some priority mechanism.

3.2 Description of the Algorithm

The algorithm has been implemented using the logic programming language Prolog, used widely in artificial intelligence applications due to its suitability for implementing logical reasoning. In logic programming, there are two distinct elements. The first is the knowledge base, which is a database of facts and clauses (which express rules) about the system to be reasoned about. The second element is the logic and reasoning used to solve problems using the knowledge base as an input.

3.2.1 Structure of the Knowledge Base

In our case, the knowledge base is composed of three groups of facts:

- The description of priorities for each XACML attribute and their corresponding values;
- The description of relative priorities used to describe which attributes are more important than others;
- The actual logic of XACML rules in a given access control application.

We note here that this relative priorities approach is closer to human reasoning.

First, for the definition of priorities of attributes we consider attribute/value pairs and specify if a value of an attribute is sensitive or normal. A convincing example is the case of the *Emergency* attribute. When its Boolean value is equal to *true* we consider it as sensitive, while when it is *false* we consider it as normal. The absence of such a definition can also be used to express the fact that a given value is of no consequence in the decision process.

The above example would require the following definition of priorities to operate correctly. For the *subject-id* attribute, we consider the nurse and psychiatrist values to be *sensitive*, in this case, for two different reasons. The nurse is allowed to read medical records of a patient only under certain conditions. Thus, we consider his or her role as sensitive. On the other hand, the psychiatrist deals with highly sensitive information that only s/he can read. Also note that the sensitivity level *normal* for a surgeon is the result of the fact that a surgeon performs his/her skills only in an operating room, thus any other sensitive location is by definition irrelevant, in sharp contrast with the nurses that perform in various locations.

```
priority('subject-id', 'nurse', sensitive).
priority('subject-id', 'anesthesist', normal).
priority('subject-id', 'generalist', normal).
priority('subject-id', 'psychiatrist', sensitive).
priority('subject-id', 'surgeon', normal).
```

The *action-id* attribute has two sensitive values, *read* and *email*. It is interesting to note that the print value is dependent on the read value. You can print only if you can read.

```
priority('action-id', 'read', sensitive).
priority('action-id', 'write', normal).
priority('action-id', 'email', sensitive).
priority('action-id', 'print', normal).
```

The *resource-id* attribute has one particular sensitive value, the *psychiatric report*.

```
priority('resource-id', 'general information', normal).
priority('resource-id', 'surgery report', normal).
priority('resource-id', 'assessment', normal).
priority('resource-id', 'psychiatric report', sensitive).
```

The *Location* attribute has sensitive values for any location outside of a hospital, which here is *ambulance* and *home care.*

```
priority('Location', 'ambulance', sensitive).
priority('Location', 'operating room', normal).
priority('Location', 'home care', sensitive).
priority('Location', 'recovery room', normal).
```

Finally, the *Emergency* attribute has a sensitive value *true*.

```
priority('Emergency', 'true', sensitive).
priority('Emergency', 'false', normal).
```

Second, we define which attributes are more important than others for the case when several sensitive values for different attributes are present in a request. Here we consider that the *Emergency* attribute prevails over any other attribute. In our case, this implies that a nurse should be able to read any medical record in any location. We specify this case using the special keyword *$all*.

```
is_more_important_than('Emergency', '$all').
```

Next, we consider the attribute *Location* as more important than *subject-id*, act*ion-id* and *resource-id*. This is, of course, in order to be able to handle appropriately the situation where the location is *home care*.

```
is_more_important_than('Location', 'subject-id').
is_more_important_than('Location', 'action-id').
is_more_important_than('Location', 'resource-id').
```

In the above definition of facts, note that we have carefully omitted a definition that would have said that *Location* is more important than *Emergency*. The absence of a specification for this case is naturally handled by Prolog since in Prolog, this would generate a fail and force the system to look at the next available solution.

Finally we consider the attribute re*source-id* more important than *subject-id* in order to handle the *psychiatric report* case.

```
is_more_important_than('resource-id',  'subject-id').
```

It is important to note that the definitions for the *is_more_important_than* fact is only partial. This is in sharp contrast with the approach of defining complete matrices used in[7]. This is inspired by the not-applicable effect of the XACML PDP system, used when a request is not matched in the policy set. However, in a Prolog implementation, if complete information were required, the use of backtracking would have the effect of forcing a search for another solution.

3.2.2 Reasoning Mechanism

When presenting a request to a policy decision point (PDP) using the specified policy set, a number of solutions are returned, possibly providing conflicting effects. A solution is defined as a path through the policy set tree and is considered in its entirety regardless of whether or not an element of logic belongs to a particular XACML structuring entity (policy set, policy or rule). Note that our reasoning mechanism is used only in case of conflicts, not redundancies, mostly because our PDP is implemented in Prolog where internal indexing is taking place, reducing considerably the search time for solutions.

In general, we work on the tree representation of a policy set as described in [5]. The tree is composed of sections of subtrees expressing the *anyOf* and *allOf* constructs in a XACML 3.0 target description, as was described in [12]. Here, the XACML *anyOf* constructs are translated into Prolog disjunctions using the "|" operator and the XACML *allOf* into Prolog conjunctions using the Prolog "," operator. We have used the single predicate approach described in [15] both for performance and also to enable easy location of solution traces. However, there are some small but important modifications to this early model that enable collecting the names of attributes and the exact trace through the logic. Our example is represented as follows in Prolog:

```
01 policy_set(PS, P, R, T, [
02          ['subject-id', A_subject_ID],
03          ['action-id', A_action_ID],
04          ['resource-id',  A_resource_ID],
05
06          ['Location', A_Location],
07          ['Emergency', A_Emergency]],
08                                                  EF):
09
10  PS = medex,
11 (A_subject_ID = ['subject-id', nurse],
12                    TPS = tps1),
13 (
14    P = p1,
15     (A_action_ID = ['action-id', read],
16                    TP= tp1),
17        (
18    (
19       R = r1,
20            (A_resource_ID = ['resource-id',
21                  surgery_report],
22               T = [TPS, TP, tr1]),
23                    EF = permit
24          )
25       |
26    (
27      R = r2,
28          (A_Location = ['Location',
29                  home_care],
30             T = [TPS, TP, tr2]),
31                   EF = deny
32          )
33       |
34    (
35      R = r3,
36          (A_Emergency = ['Emergency',
37                   true],
38            T = [TPS, TP, tr3]),
39                  EF = permit
40           )
41    )
42        ).
```

Solution paths are traces composed of tree traversals through policy sets, policies and rules. They are obtained by posing a query using the Prolog built-in *findall* predicate applied to the entire tree:

```
:- findall(policy_set(PS, P, R, T, RQ,
    EF), policy_set(PS, P, R, T, RQ, EF),
                          LS).
```

where *RQ* represents a request, which is composed of values for each attribute of the policy set, *LS* is a variable that will return a list of solution paths, and *EF* is the effect of each solution path. While the request contains values for all attributes used in the entire policy set, the returned solutions contain only subsets of attributes that are effectively used in the path. For example, the request:

```
R1 :=
  'subject-id' = 'nurse',
  'action-id' = 'read',
  'resource-id' = 'surgery_report',
  'Location' = 'home_care',
  'Emergency' = 'true'
```

will return three solution paths. The first one will traverse policy set *medex*, policy *p1* and rule *r1* with an effect of *permit*. This is achieved by the matching statements of lines 11, 12, 15, 16, 20, 21 of the Prolog representation of the XACML policy set above. The subset of attributes for this solution path that contain sensitive values is { *subject-id*, *action-id* }. Note that the attributes *Location* and *Emergency* are absent from this list because there are no corresponding matching expressions for them in this solution trace. The *surgery report* value for *resource-id* has been declared as non-sensitive in the priority facts above and thus does not appear in the subset of attributes. The two other solution traces are left as an exercise to the reader.

In this example, we have three results with two different effects (both *deny* and *permit*). We have tried different mechanisms to resolve such conflicts. First, we experimented with numerical values to express priorities in two different ways.

The first approach consisted of calculating the sum of each attribute's priority based on the values for the attributes that are present in a solution trace through the policy set tree. This solution was rapidly eliminated because it produces misleading results when the solution traces do not contain exactly the same number of attributes. In particular, this case arises when expressions for a given attribute are not provided, which is the way to express that any value of the attribute is applicable.

The second approach consisted of picking the solution trace for which an attribute that is present in the policy logic showed the highest priority value. This provided good results for our above example but could not be generalized.

Consequently, we began exploring an algorithm that does not rely on quantitative numerical values used to describe priorities, but instead uses qualitative relative values as expressed by the Prolog *priority* facts above.

The new algorithm has two steps:

- The first step consists of collecting the attributes for which there is a sensitive value in a particular solution path. Then, the attribute that is the most important among all of those in the subset of attributes in the solution path is chosen using the *is_more_important_than* facts. The algorithm works under the assumption that when using an attribute to specify some exception, policy writers do use sensitive values in the XACML target logic. It is clear that this approach would not work in the case of non-sensitive values. However, access control logic is mostly composed of cases where sensitive values of attributes apply. After this step, we end up with a single attribute that is the most important for a given solution trace and serves as the representative of a solution trace.
- In the second step, using the most important attributes for each solution path determined in the first step, we apply the *is_more_important_than* fact again, but this time to compare the relative priority among solution paths, which determines the most important solution path. The resulting solution path then provides the final effect desired (*permit* or *deny*).

In our case, the request *R1* produces three solutions against our policy set.

The first solution consists of the path that traverses rule *NurseResourceRule*, which is the first one returned when evaluating the request against the policy set by the Prolog inference engine:

Solution 1: policy_set(medex,p1,r1,[tps1,tp1,tr1],
[[subject-id,[subject-id,nurse]],
[action-id,[action-id,read]],
[resource-id,[resource-id,
surgery_report]],
[Location,_G1880],
[Emergency,_G1889]],
permit)

In the above first solution, we notice that Prolog open variable values *_G1880* and *_G1889* are produced when the matching logic does not contain attributes *Location* and *Emergency*. The solution trace actually considers all the attributes in the attribute list of the Prolog representation of the policy set. The solution trace traverses policy set *medex*, policy *p1* and rule *r1*.

A solution trace can be obtained using the following Prolog term to be used in a query to the knowledge base:

```
go_pdp_med_1:-
  nl, write('request 1'),
  retractall(solution(_,_)),
  assertz(solution(_,0)),
  request(request_1, RQ),

  findall(policy_set(medex, P, R, T, RQ,
                     EF),
  policy_set(medex, P, R, T, RQ, EF), LS),
  extract_solution_traces(LS, [ ], LST),
  nl, write('solution traces:'),
  select_solution(LST, SSOL),
  nl, write('overall effect: '),
  write(SSOL).
```

The second solution trace returned by the above query is as follows:

Solution 2: policy_set(medex,p1,r2,[tps1,tp1,tr2] ,
[[subject-id,[subject-id,nurse]],
[action-id,[action-id,read]],
[resource-id,_G1961],
[Location,[Location,home_care]],
[Emergency,_G1979]],
deny)

In the above second solution, we notice that Prolog open variable values *_G1961* and *_G1979* are produced when the matching logic is absent for attributes *resource-id* and *Emergency*. The solution trace traverses policy set *medex*, policy *p1* and rule *r2*.

And finally the third solution trace is as follows:

Solution 3: policy_set(medex,p1,r3,[tps1,tp1,tr3],
[[subject-id,[subject-id,nurse]],
[action-id,[action-id,read]],
[resource-id,_G2051],
[Location,_G2060],
[Emergency,[Emergency,true]]],
permit)

In the above third solution, we notice that Prolog open variable values *_G2051* and *_G2060* are produced when the matching logic is absent for attributes *resource-id* and *Location*.

The solution trace traverses policy set *medex*, policy *p1* and rule *r3*.

For each of these solutions we collect the attributes for which sensitive values are detected in the request and the corresponding policy set targets. For example, in the case of the third solution trace, we would have the following list.

[subject-id, action-id, Emergency]

Then we use the *is_more_important_than* fact to determine which attribute is the most important for that solution, and it will be used to represent this solution when comparing solutions to each other. In this case, it is the attribute *Emergency* because of the *is_more_important_than fact* for target attribute *$all*.

When comparing the *Emergency* attribute against other attributes with matching expressions that operate on a sensitive value, we can successfully derive that the *Emergency* attribute is the most important of all. Thus the *Emergency* attribute will represent the third solution when comparing the solutions among themselves. This is summarized in Figure 1, where solid arrows show the path

of a given solution for request *R1*, grey boxes show the sensitive values for attributes and dotted arrows show the *is_more_important_than* relations.

By repeating this process for each solution, we determine that *Location* is the most important attribute for the second solution trace and the attribute *action-id* will represent the first solution, mainly because there are no *is_more_important_than* definitions for the attributes that are present in this solution path.

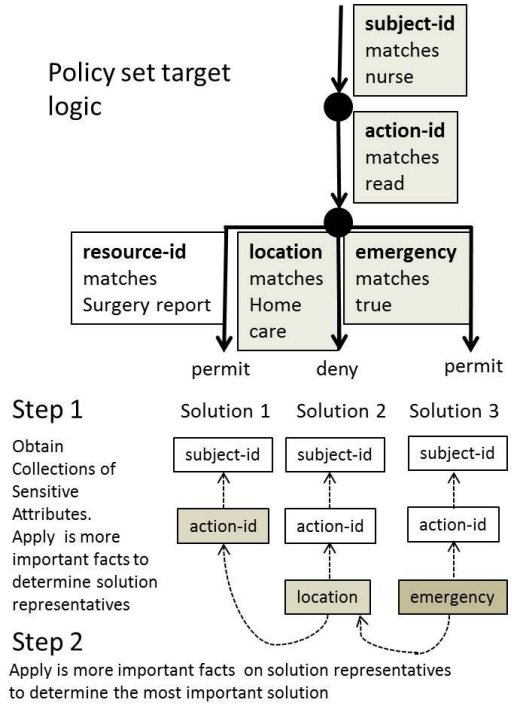


Figure 1. Visual representation of algorithm applied to request 1.

Also, the results for the second request *R2*, where *Emergency* has been set to false, will produce only two solutions, with the attribute *Location* as the most important attribute. This attribute value will be used to determine the final effect, which is *deny*.

R2 :=
'subject-id' = 'nurse',
'action-id' = 'read',
'resource-id' = 'surgery_report',
'Location' = 'home_care',
'Emergency' = '**false**'

Finally, the same method applied to the request *R3* will result in only one solution produced, in which case, we don't need to try to determine priorities among attributes of this solution path. The resulting effect of this solution is *permit*.

R3 :=
'subject-id' = 'nurse',
'action-id' = 'read',
'resource-id' = 'surgery_report',
'Location' = '**operating room**',
'Emergency' = '**false**'

Now, when handling request 1, the second step of our method can be applied. We compare the attribute representatives for each solution as given by the first step. Here the results of the first step produced the following most important attribute representatives for each solution path:

Solution 1: *action-id => permit*
Solution 2: *Location => deny*
Solution 3: *Emergency => permit*

Since *Emergency* has been defined as the most important attribute of all, this will make solution 3 win and the final effect will be *permit*. In other words, a nurse can read any document anywhere during an emergency.

3.2.3 Handling Concurrent Priorities

If we add one more rule that deals with psychiatric reports this system may no longer work.

```
rule NursePsychiatryRule -> Deny :=
        resource-id matches 'psychiatric report'
```

Effectively, since we have declared that the attribute *Emergency* is more important than anything else, when attribute value *Emergency* matches *true* and attribute *resource-id* matches value *psychiatric report* in a request that is presented to the PDP, it will allow a nurse to read a psychiatric report, which is what the above additional rule wants to prevent. Thus, in this context we need to improve our methodology. One easy way to handle this case is to enhance the *is_more_important_than* facts by adding a field for the highly critical value.

```
is_more_important_than('resource-id',
                'psychiatric report', '$all').
```

Then, adding a clause to the Prolog logic to handle this case (lines 01 to 06 below) solves the problem. Here these cases would be made available on the top of the list of alternative predicates and if there is a match, a Prolog cut ("!") will prevent it from considering the other cases as follows:

```
01 determine_most_important:-
02          is_more_important_than(A, V, '$all'),
03          significant(A),
04          request_value(A, V),
05          save_most_important(A),
06          !.
07
08 determine_most_important:-
09          is_more_important_than(A, '$all'),
10          significant(A),
11          request_value(A, V),
12          save_most_important(A),
13          !.
14
15 determine_most_important:-
16          significant(A),
17          (
18                      most_important(nil)
19                      |
20                      most_important(MI),
21                      is_more_important_than(A, MI)
22
23          ),
24          save_most_important(A),
25          fail.
26
```

27 determine_most_important.

The above code makes intensive use of the Prolog internal database which in a way mimics the storage of information of humans in their brains and reasoning as a retrieval of this information.

3.3 Another Example in the Military Domain

The example provided in [12] can be enhanced to create the kind of ambiguity found in the previous medical example, showing again the benefit of priorities. Here we add a policy that considers the unit being engaged.

```
policy agent_a policy :=
   Agent matches a

rule No_fly_zone_rule –> permit :=
      Zone matches no_fly_zone.

  rule  HostilesPresenceRule -> deny
      HostilesPresence matches true.

  rule UnitRule -> permit:=
       Zone = no_fly_zone,
       Unit matches special forces.
```

In this case, special forces are allowed to enter the no fly zone even when a hostile presence is detected. This is achieved using the following facts:

```
is_more_important(HostilePresence, Zone).
is_more_important('Unit', 'special forces',
                          '$all').
```

4. CONCLUSION

In this paper we have shown how to resolve run-time conflicts using artificial intelligence in the form of automated logical reasoning, with an algorithm that uses priorities based on sensitivity assessments defined for each policy/rule attribute and its associated values. Our approach uses a relative relationship and thus there is no need for numerical weights. This approach is closer to human reasoning, which reacts to overall sensitivity factors rather than scales of values. We also determined that compile time conflict detection algorithms are very useful for testing purposes. They can determine which requests to a PDP produce these conflicts, and thus enable the policy administrator to verify offline that the conflict resolution algorithms are performing as expected.

5. ACKNOWLEDGMENTS

The authors acknowledge the support of the Natural Sciences and Engineering Research Council of Canada.

6. REFERENCES

[1] OASIS, *XACML Version 2.0*, 2004, docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

[2] OASIS, *XACML Version 3.0*, 2013, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[3] C.D.P.K. Ramli, H. R. Nielson, F. Nielson, The Logic of XACML, in proceedings of FACS 2011 pp 205-222.

[4] K. Jayaraman, V. Ganesh, M. Tripunitara, M. Rinard, and S. Chapin, "Automatic error finding in access-control policies," in *18th ACM Conference on Computer and Communications Security*, 2011, pp. 163–174.

[5] H. Hu, G.-J.Ahn and K. Kulkarni, Anomaly Discovery and Resolution in Web Access Control policies in SACMAT'11 proceedings.

[6] B. Stepien, S. Matwin, and A. Felty, "Strategies for reducing risks of inconsistencies in access control policies," in *5th International Conference on Availability, Reliability, and Security*. IEEE Computer Society, 2010, pp. 140–147.

[7] I. Matteucci, P. Mori, and M. Petrocchi, "Prioritized execution of privacy policies," in *International Workshop on Data Privacy Management and Autonomous Spontaneous Security*, ser. Lecture Notes in Computer Science, vol. 7731. Springer, 2013, pp. 133–145.

[8] M. Aqib and R. A. Shaikh, Analysis and comparison of access control policies validation mechanisms, *International Journal of Computer Network and Information Security*, vol. 7, no. 1, pp. 54–69, 2015.

[9] N. Li, Q. Wang, P. Rao, D. Lin, E. Bertino, and J. Lobo, A formal language for specifying policy combining algorithms in access control, CERIAS, Tech. Rep. 2008-9, 2008, http://core.ac.uk/download/pdf/21173941.pdf.

[10] K. Fatema and D. Chadwick, "Resolving policy conflicts—integrating policies from multiple authors," in *Advanced Information Systems Engineering Workshops*, ser. Lecture Notes in Business Information Processing, vol. 178. Springer, 2014, pp. 310–321.

[11] M. Hall-May and T. P. Kelly, "Towards conflict detection and resolution of safety policies," in *24th International System Safety Conference*, 2006.

[12] B.Stepien, A. Felty, S.Matwin, Challenges of Composing XACML Policies in 2014 Ninth International Conference on Availability, Reliability and Security.

[13] N. Li, Q. Wang, W.Qardaji, E.bertino, P. Rao, Access Control Policy Compiling: Theory Meets Practice in SACMAT 09 proceedings pages 135-144.

[14] A.J. Rashidi, A. Rezakhani, a new method to ranking Attributes in Attribute Based Access Control using decision fusion in Natural Computing Applications Forum 2016, Springer Verlag.

[15] B. Stepien and A. Felty, Using Expert Systems to Statically Detect "Dynamic" Conflicts in XACML in ARES 2016 proceedings, pp 127-136.

Discovering Knowledge of ASD from CCC-2: Ensemble Learning Approach for Analysis of ASD

Hirokazu Shimauchi
Corresponding Author
Tokyo Institute of Technology
2-12-1 Ookayama, Meguro
Tokyo, Japan
hirokazu.shimauchi@gmail.com

Naotake Tsukidate
Yamanashi Eiwa College
888 Yokone, Kofu
Yamanashi, Japan
n.tsukidate@yamanashi-eiwa.ac.jp

Kan Hishiyama
The University of Tokyo
7-3-1 Hongo, Bunkyo
Tokyo, Japan
k.hishiyama1030@gmail.com

Manabu Oi
Kanazawa University
Kakuma, Kanazawa
Ishikawa, Japan
oimanabu@ed.kanazawa-u.ac.jp

Yuko Yoshimura
Kanazawa University
Kakuma, Kanazawa
Ishikawa, Japan
yukuchen@staff.kanazawa-u.ac.jp

Mitsuru Kikuchi
Kanazawa University
Kakuma, Kanazawa
Ishikawa, Japan
mitsuruk@med.kanazawa-u.ac.jp

Chiaki Hasegawa
Kanazawa University
Kakuma, Kanazawa
Ishikawa, Japan
hasegawachiaki1014@gmail.com

ABSTRACT
In this paper, we constructed an ASD classifier by random forest with responses of CCC-2 and the diagnosis results obtained from ADOS. Further the importance of features in CCC-2 for the classification of ASD was analyzed. The hyperparameters of the random forest were adjusted on the training dataset with the cross-validation, and the generalization performance was evaluated on the test dataset. Since the sample size was not so large, we validated the effect of random shuffling for the classification performance with additional 4 shuffle pattern. The all constructed classifiers not only had a highly classification performance, but also the result was stable with respect to random shuffling. It is also remarkable result that two items, which related to pragmatic impairments, were consistently determined to be the first, second important feature respectively. The items that reflect these pragmatic impairments were emphasized over the I and J domains in CCC-2, which reflect the main behavioral characteristics of ASD. It shed light on new aspects of ASD assessment for children.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03...$15.00
https://doi.org/10.1145/3388176.3388192

CCS Concepts
• Human-centered computing→Social engineering (social sciences) • **Information systems→Data mining** • **Computing methodologies→Ensemble methods.**

Keywords
ASD; ADOS; CCC-2; Ensemble learnings.

1. INTRODUCTION
The present research suggested that pragmatic assessment might be an alterative to primary screening tools to support a diagnosis of Autism Spectrum Disorder (ASD). In addition, it was suggested that two items of this pragmatic assessment consistently provide greater precision of classifying ASD.

1.1 Background
In recent it is reported that the overall prevalence of ASD is one in 59 among children aged 8 years (reported by ADDM Network; [1]). From Health care professional to the public, a large number of people are interested in ASD as a highly prevalent developmental disorder. According to diagnostic criteria of DSM-5, the traits are depicted as deficits in social communication and social interaction, the presence of restricted and repetitive patterns of behavior, interests, or activities.

As expressed in terms of “spectrum”, another trait of ASD is broad clinical picture on the symptom. On the other words, it is a diagnostic concept which exist a continuum among patients termed as “spectrum”, ranging from a type of person who has moderate autistic trait and social adaptability to who has severe autistic trait.

Two standardized assessment tools are mentioned as gold standard for the diagnosis of children who were suspected of having autism. One is the Autism Diagnostic Interview-Revised (ADI-R; [14]) and the other is the Autism Diagnostic Observation Schedule ([10], cf. [5] about several versions of ADOS). ADI-R is a semi-structured investigator-based interview for parents, focusing on past features of their child, and it's required time is 90-150 min. ADOS is direct observation of social behavior, communication, and repetitive behaviors, focusing on current features, and it's required time is 40-90 min. Particularly ADOS gives diagnostic classification of "autism", "non-autism ASD" and "non-spectrum". These two assessments are conducted individually by qualified personnel.

The CCC-2 (The Children's Communication Checklist-2; [2]) is a screening test for children who likely to have a language impairment and, to especially identify pragmatic language impairment. According to Bishop [2], the pragmatic impairment is defined as some difficulties in selection of the appropriate message or interpretation in relation to the communicative context. The CCC-2 is a parent rating scale (an adult who has observed the child over time in natural social settings can rate them) consisted of 70 multiple choice items and it is intended for children with 4-16 years-old. Items are divided into 10 scales, each with 7 items. The detail of each scale are A: speech, B: syntax, C: semantics, D: coherence, E: inappropriate initiation, F: stereotyped language, G: use of context, H: nonverbal communication, I: social relations, J: interest (see Table 1). The four scales from A to D represent aspects of language structure, vocabulary and discourse. The next four scales from E to H cover pragmatic aspects of communication. The last I and J scales represent behaviors that are usually impaired in case of autistic disorder.

Table 1. Construction of CCC-2

Category	Subscale
structural aspect of language	speech syntax semantics coherence
pragmatic aspects of communication	inappropriate initiation stereotyped language use of context nonverbal communication
characteristic of ASD	social relations interests

1.2 Motivation

Although, above mentioned, I and J scales assess behaviors that are impaired in autistic disorder, the test manual of CCC-2 [2] emphasizes that it cannot be used to diagnose autistic disorder. However, in consideration that social communication impairment is defined as the core symptom of ASD, it is not difficult to imagine that there is a relationship between ASD and the manner of communication measured by CCC-2. Although it is well known that M-CAHT [13] or SCQ [15] as the preliminary screening test of ASD among practice and research experts, appropriate combination of each 70 items covering several aspects of child's communication might provide more accurate diagnosis of ASD rather than previous screening tests.

It should make an important contribution to composing simplified, parent rating screening test which can complete with relatively short time, comparing to individual diagnosis which require substantial time and procedure.

1.3 Contribution

Based on 70 items of CCC-2 the 112 children with ASD or TD (Typical Development) label were classified by Random Forest Analysis. After the random shuffling of dataset, we adjust the hyperparameters of our model on the dataset of 80% (training dataset) by 5-hold cross-validation, and then evaluated the generalization performance on the remaining 20% (test dataset). Considering the small sample size, we made 4 patterns of training and test dataset additionally, and then evaluate the effect of random shuffling to the performance and structure of constructed classifiers by random forest with same hyperparameters. As a result, scores of the classification indicated average of 86.0% accuracy on all pattern of datasets. Furthermore, the average score for the classification was 88.7% (above 82.6% in all patterns) and the 0.97 in AUC score based on ROC curve showed sufficient performance of the classification (above 0.95).

It is possible, therefore, that CCC-2 which is parent rating scale functions well as an indicator to classify ASD. In addition, according to the model established by Random Forest, two items (item 5 in E: inappropriate initiation and item 28 in G: use of context) were consistently suggested as most important item to classify ASD. Both items represent pragmatic aspects of communication and this finding correspond to a premise that the core symptom of ASD is social communication impairment.

Therefore, the appropriate combination of CCC-2 items showed sufficient accuracy for ASD classification and items belong to pragmatic aspect serve an important role. What is curious about this finding was that pragmatic aspect functioned well as an indicator of the classification rather than items belong to I and J scales which represent behaviors that are usually impaired in case of autistic disorder.

2. DATA AND METHOD

2.1 Data

The following data was provided by Oi's research [12]. Forty-eight children with ASD (37 boys and 11 girls ranging from 3.33 to 9.25 years) and 64 children with TD (44 boys and 20 girls ranging from 3.17 to 10.17 years) were subject to analysis. A speech therapist and a psychiatrist assessed children suspected of ASD. The Autism Diagnostic Observation Schedule–Generic (ADOS–G; [9]) was conducted by the speech therapist, who has more than 5 years of experience in ASD treatment and is well trained and certified in assessment using ADOS. In consideration for the result of Diagnostic Interview for Social and Communication Disorders (DISCO; [16]), the psychiatrist, who has more than 10 years of experience in ASD, made definitive diagnosis of ASD. In accordance with the ADOS–G twenty-four children were classified as "autism" and another 24 were classified "non-autism ASD". The intellectual ability on children in each ASD and TD group was measured by Kaufman Assessment Battery for Children (K-ABC). Children in the ASD group ranged in score from 58 to 144. In the same manner, children in the TD group ranged in score from 86 to 139. Therefore, there was no noticeable difference between ASD and TD group in intellectual level based on cognitive processing. In addition, all children were rated by parents using Japanese version of CCC-2 [11][12].

2.2 Method

We defined labels of ASD/TD as the response variable and classified them by 70 items of CCC-2 according to random forest classifier. In contrast to neural network and support vector

machine which construct one classifier from training dataset, ensemble methods construct a set of classifiers and combine them. According to how the base classifiers are generated, there are two paradigms of ensemble methods. Sequential ensemble methods, e.g. AdaBoost [6] and Gradient boosting tree [7], generate the base classifiers sequentially. In contrast, parallel ensemble methods, e.g. Bagging [3] and Random forest [4], generate the base classifiers in parallel. Exploiting the independence between the base classifiers, parallel ensemble methods reduced error dramatically by combining independent base classifiers. Random Forest is a representative of the parallel ensemble methods: that randomly selects a subset of features firstly, and then carries out the conventional split selection procedure within the selected feature subset. Although regression tree is difficult to keep generalization performance, Random forest has improved this weakness by way that decorrelates the trees, using random sampling of bootstrapped splits on the decision tree.

Random forest is nonparametric nonlinear model and has higher generalization performance in ensemble methods (see e.g. [17]). It can be considered that nonparametric nonlinear model is more appropriate to classify ASD than model-based parametric method because the diagnostic criterion of ASD is not single and the symptom of ASD is premised on spectrum. In addition, Tree-based methods has an advantage that evaluation of importance of features for the classification is available, compared to other nonlinear method such as neural network or SVM. By identifying which item of CCC-2 are closely related to the diagnosis of ASD, it would be available to select items for composing a simpler primary screening test. In addition, it would lead to clarifying where the characteristics of difficulties of children with ASD appears most from the viewpoints of parents who share their life.

Evaluating the performance of our classifier was conducted by following procedure. First, the dataset was randomly shuffled and ordered, then take the first 80% as training dataset and the remaining 20% as test dataset. Second, according to the result of cross-validation, the hyperparameter was tuned on training dataset, and then the generalization performance was evaluated based on test dataset which was not used in the training. In this regard, however it was also evaluated how much the model was affected by the random shuffling of the dataset because of concern that test dataset might be biased due to small sample size. Specifically, five random shuffled patterns were prepared to evaluate the uncertainty of random shuffling. Above procedure was implemented in Python 3.6 with Scikit-learn.

3. EMPIRICAL ANALYSIS

We split the dataset in a training set and a test set after randomly shuffling. The 80% of the available dataset was allocated as training dataset, and the remaining 20% was used for test. We adjusted the hyper parameters on training dataset by 5-hold cross validation (see the case Random seed equal to 0 in Table 2). The adjusted hyperparameters were the number of trees in the forest, the function to measure the quality of a split, the number of features to consider when looking for the best split: these are particularly important parameters for random forest classifier.

3.1 Scores of Classifier

The accuracy of constructed model with adjusted hyperparameter was 86.7% in the 5-hold cross-validation on training dataset, 91.3% in the test on test dataset, respectively. Both precision and recall on test dataset were 92.3%. The area under the receiver operating characteristic curve was 0.96. Considering these scores in the test dataset, the constructed classifier has high classification performance.

However, the training dataset and test dataset might be biased, because the sample was not so large as we mentioned in Section 2. For observing the uncertainty of randomly shuffling, we made additional 4 dataset with different random seed in the same manner, and then construct the classification model by Random forest with same adjusted hyperparameters in the first case (Random seed equal to 0). The table 2 shows the scores on each dataset. The average of accuracy in the 5-hold cross-validation on the training dataset was 86.2%. The average of accuracy, recall, precision, ROC AUC were 88.7%, 90.1%, 85.7%, 96.6% respectively. The score which less than 80% was that the recall of the case random seed 2 only. In this case samples of ASD in test dataset might be biased by random shuffling. Actually, the positive example was 39% in the test dataset: this was 4% smaller than other cases.

Table 2. Scores of constructed classifiers on test dataset

Random seed	0	1	2	3	4	Mean
Accuracy	91.3	87.0	82.6	95.7	87.0	88.7
Precision	92.3	81.8	85.7	92.3	90.9	88.6
Recall	92.3	90.0	66.7	96.0	83.3	85.7
ROC(AUC)	0.96	0.95	0.95	0.98	0.99	0.97

Overall, the highly classification performance of our classifiers can be viewed as a strong correlation (possibly non-linear) between ASD and items of the CCC-2.

3.2 Analysis of Feature Importance

As we showed in section 3.1, random forest construct high-performance classifiers on each dataset. It can be viewed that the performance was not affected strongly by random shuffling. Here we evaluate the magnitude of the effect of the random shuffling to the structure of model. For checking the difference of the constructed models, we calculated the feature importance of each models. Figures 1, 2, 3, 4, 5 shows the feature importance of each random forest classifiers.

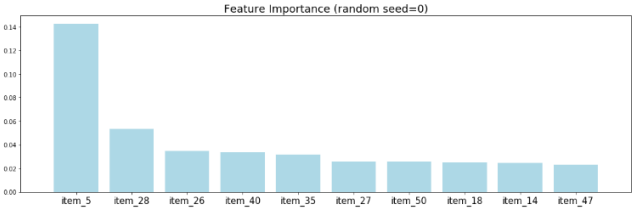


Figure 1. Top 10 items of feature importance of the constructed model with random seed 0.

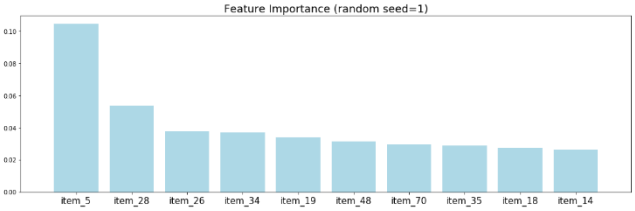


Figure 2. Top 10 items of feature importance of the constructed model with random seed 1.

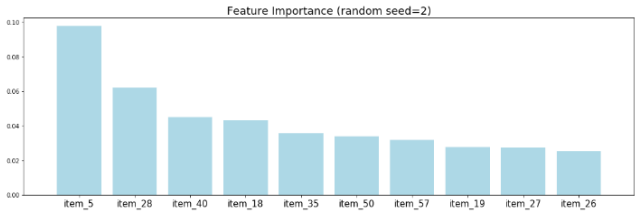


Figure 3. Top 10 items of feature importance of the constructed model with random seed 2.

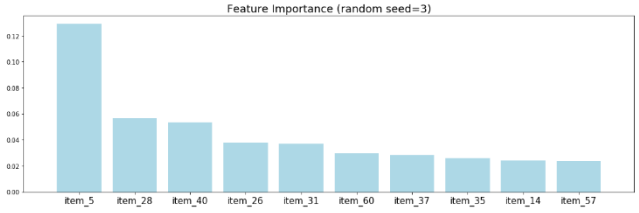


Figure 4. Top 10 items of feature importance of the constructed model with random seed 3.

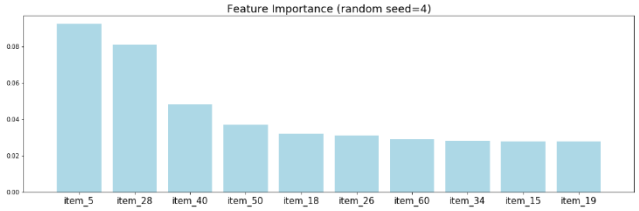


Figure 5. Top 10 items of feature importance of the constructed model with random seed 4.

We found that some items were included commonly on each model as important features. In particular, it should be noted that the item 5, 28 were consistently determined to be the first, second important feature respectively. It can be regarded that the constructed models by random forest is not affected strongly by the random shuffling of dataset.

Both items 5 and 28 reflect pragmatic impairments: these are labeled as social communication disabilities, which is a core symptom of ASD. The items that represent these pragmatic impairments were emphasized over the I and J domains, which reflect the main behavioral characteristics of ASD. It shed light on new aspects of ASD assessment for children.

3.3 Discussion

In this study, the strong correlation with ASD of the two question items in CCC-2 was found: pragmatic assessment might be useful for assisting the diagnosis of ASD. In our dataset, ADOS diagnosis results are used to determine ASD, and the accuracy of the diagnosis results in the dataset can be assumed precise. Since the samples were composed of parents' children who offered to cooperate in the research activity of the university in Japan, we should careful consideration of the population: we need additional information based on appropriate sampling for generalization of our result. Furthermore, the causal relationship between the two items that reflect pragmatic impairment and ASD is unclear, therefore it would be required to clarify this relationship by an experimental approach.

However, the result is not so unnatural for researchers and practitioners of autism such as psychologist, speech therapist, psychiatrist and so on. Because the definition of ASD closely relates with social communication disorder, it is reasonable that two items representing pragmatic impairments relate the classification of ASD. However, despite that pragmatic aspect of CCC-2 consists of four domains (or in some cases five domains to which "coherence" is added), "inappropriate initiation" and "use of context" is more distinct as characteristic of ASD than remaining domains. In other words, it is curious that same pragmatic aspects have each different degree of contribution to the classification of ASD. In this study the data set of CCC-2 is rated by parents. For parents who live with the child over time in natural social setting, the above two domains might be more perceptible, that is, interesting expressions in their child, than typical autistic behavior and the other pragmatic aspects. One of the future works form this study would be how children with ASD is reflected in the eyes of parents. In addition, in consideration that more than one items from the single domain did not contribute to the ASD classification, future research might not only examine the association with ASD at the level of pragmatic aspects, but the association with ASD at the level of items. It might be also necessary to focus on the meaning of the item itself for better assessment.

4. CONCLUSION

In this paper, we constructed an ASD classifier by responses of CCC-2 and the diagnosis results obtained by ADOS. CCC-2 was used as features, and ADOS as a label of ASD. The dataset was randomly shuffled and divided into training dataset and test dataset. The hyperparameters of the Random forest were adjusted on the training dataset with the cross-validation, and the generalization performance was evaluated on the test dataset. Since the sample size was small, the result might be biased by random shuffling of dataset. We validated the effect of random shuffling with additional 4 shuffle pattern. The constructed classifier not only had a highly classification performance on test dataset. Further the result was stable with respect to random shuffling.

Also it is remarkable result that two items, which related to pragmatic impairments, were consistently determined to be the first, second important feature respectively. The items that represent these pragmatic impairments were emphasized over the I and J domains, which reflect the main behavioral characteristics of ASD. It might be revealing noticeable feature useful for assessment on ASD by examining the relationship between these items and ASD. For the generalization of the result, we will consider to collecting additional sample over extended. Further we consider tackling the analysis of the causal relation between two items and ASD.

5. ACKNOWLEDGMENTS

We would like to thank the corresponding author of [12] for giving us the permission of reanalysis to a part of data in the article. The authors are also grateful to the reviewers for their careful reading of our manuscript.

This work was supported by JSPS KAKENHI Grant Number JP17H06382.

6. REFERENCES

[1] Baio, J., Wiggins, L., Christensen, D.L., Maenner, M.J., Daniels, J., Warren, Z., et al. 2018. Prevalence of autism spectrum disorder among children aged 8 years - autism and developmental disabilities monitoring network, 11 sites, United States, 2014. *MMWR Surveillance Summary*, 67, 1–23.

[2] Bishop, D. V. M. 2003. *The Children's Communication Checklist (2nd ed)*. London: Harcourt Assessment.

[3] Breiman, L. 1996. Bagging predictors. *Machine learning*, 24(2), 123-140.

[4] Breiman, L. 2001. Random forests. *Machine learning*, 45(1), 5-32.

[5] Dorlack, T. P., Myers, O. B., & Kodituwakku, P. W. 2018. A Comparative Analysis of the ADOS-G and ADOS-2 Algorithms: Preliminary Findings. *Journal of Autism and Developmental Disorders*, 48, 2078-2089.

[6] Freund, Y., & Schapire, R. E. 1997. A decision-theoretic generalization of on-line learning and an application to boosting. *Journal of computer and system sciences*, 55(1), 119-139.

[7] Friedman, J. H. 2001. Greedy function approximation: a gradient boosting machine. *Annals of statistics*, 1189-1232.

[8] Hastie, T., Tibshirani, R., & Friedman, J. 2009. *The elements of statistical learning (2nd edition)*. New York: Springer series in statistics.

[9] Lord, C., Risi, S., Lambrecht, L., Cook, E.H., Jr, Leventhal, B.L., et al. 2000. The Autism Diagnostic Observation Schedule–Generic: A Standard Measure of Social and Communication Deficits Associated with the Spectrum of Autism. *Journal of Autism and Developmental Disorders*, 30, 205-223.

[10] Lord, C., Rutter, M., DiLavore, P.C. et al. 2012. *Autism Diagnostic Observation Schedule-Second Edition. Los Angeles*, CA: Western Psychological Services.

[11] Oi, M., Fujino, H., Tsukidate, N., Kamio, Y., Gondou, K., & Matsui, T. 2016. *Japanese version of Children's Communication Checklist-2*. Tokyo: Nihon Bunka Kagakusha.

[12] Oi, M., Fujino, H., Tsukidate, N., Kamino, Y., Yoshimura, Y., Kikuchi, M., et al. 2017. Quantitative aspects of communicative impairment ascertained in a large national survey of Japanese children. *Journal of Autism and Developmental Disorders*, 47, 3040–3048.

[13] Robins D.L., Casagrande K., Barton, M., et al. 2014 Validation of the Modified Checklist for Autism in Toddlers, revised with follow-up (M-CHAT-R/F). *Pediatrics*, 133, 37–45.

[14] Rutter, M., Le Couteur, A. & Lord, C. 2003. *Autism Diagnostic interview-Revised*. Los Angeles, CA: Western Psychological Services.

[15] Rutter, M., Bailey, A. & Lord, C. 2003. *The Social Communication Questionnaire*. Los Angeles, CA: Western Psychological Services.

[16] Wing, L., Leekam, S. R., Libby, S. J., Gould, J., & Larcombe, M. 2002. The diagnostic interview for social and communication disorders: Background, inter-rater reliability and clinical use. *Journal of Child Psychology & Psychiatry*, 43, 307–325.

[17] Zhou, Z. H. 2012. *Ensemble methods: foundations and algorithms*. Chapman and Hall/CRC.

Role Identification of Domain Name Server Using Machine Learning based on DNS Response Features

Hailing Li
Institute of Information Engineering, Chinese Academy of Sciences
School of Cyber Security, University of Chinese Academy of Sciences
CNCERT/CC
Beijing, China
lihailing@iie.ac.cn

Hui Zhang*
Corresponding author
Institute of Information Engineering, Chinese Academy of Sciences
School of Cyber Security, University of Chinese Academy of Sciences
CNCERT/CC
Beijing, China
zhanghui@iie.ac.cn

Longtao He*
Corresponding author
Institute of Information Engineering, Chinese Academy of Sciences
CNCERT/CC
Beijing, China
hlt@cert.org.cn

Kai Zhang
CNCERT/CC
Beijing, China
zhangkai@cert.org.cn

Chenghai He
CNCERT/CC
Beijing, China
hechenghai@cert.org.cn

Bingjie Wei
CNCERT/CC
Beijing, China
weibingjie@isc.org.cn

ABSTRACT

The Domain Name System (DNS) plays an important role in the Internet by mapping domains to IP addresses. Numerous authoritative name servers and recursive resolvers form the DNS service infrastructure. Accurate identifying the role of the DNS server is of great importance for understanding the DNS infrastructure and performing security analysis. Previous research has proposed some methods for DNS server identification. Most of them are active methods which bring additional bandwidth and security risks; the non-negligible complex configuration of DNS servers in the actual network makes the results of passive approach using the DNS message header fields "AA" and "RA" unsatisfactory. This paper proposes a machine learning method to classify the typical role of the DNS server in a passive manner. Classifiers are trained by three categories of features extracted solely from passive DNS response records (removing the user information) and the experiment results show that the proposed method can achieve high accurate and low false positive rate.

CCS Concepts

• Networks→Naming and addressing • Computing methodologies→Supervised learning by classification.

Keywords

Domain name server identification; machine learning; DNS response features.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03 …$15.00.
https:// doi.org/10.1145/3388176.3388205

1. INTRODUCTION

DNS servers play an important role in completing the domain resolution process. A typical scenario of domain resolution is illustrated in Figure 1. End-users send DNS queries via the DNS client (also called stub resolver) software to the pre-configured recursive resolver. The recursive resolver will check its cache or recursively ask the authoritative name servers from root to the more specific name server until it get the answer and finally return the result to the DNS client of the end-users.

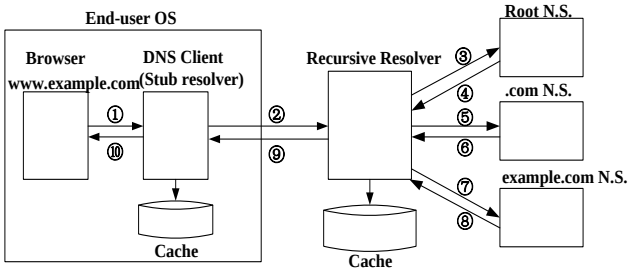


Figure 1. A typical domain resolution procedure.

Accuracy identification of DNS server is essential to understand the overall network structure of the DNS and performing security analysis on DNS. For example, open recursive resolvers can be a component of DNS amplification attacks, and the software defeat in different roles of DNS server will result in different degrees of security impact [2] [3].

The existing methods for identifying DNS servers are mainly in active mode. DNSauth [4], an active measuring tool, was used to obtain the authoritative name server of the specified domain name. Brute force probing method is widely used for large scale open recursive resolver detection [5]. A Zmap-based tool [6] was developed to obtain the open recursive server candidates which were verified later by the self-built authoritative server. Active method is effective in collecting a large list in a short time while the shortcomings are unnecessary traffic on the Internet and security risks to the receivers. Moreover, non-open DNS server will not response.

There are also passive methods based on DNS traffic. The passive data can give more comprehensive information of an IP. A recursive resolver online identification method was proposed by analyzing the connectivity attributes of the source IP [7]. If the number of destination IPs and the number of different domains associated to the source IP in the collected traffic exceed their thresholds respectively, this source IP is considered as a recursive server. This online method was simple and efficient but the connectivity threshold is not easy to set and errors will occur when dealing with large name servers with high connectivity attributes. Another method using a multilayer perceptron model [8] was proposed to identify and classify the recursive server based on the two-direction DNS traffic. Multidimensional features such as traffic direction, traffic statistics features and protocol field features were used for the multi-classification. It gives a high accuracy, low false positive rate and considers a finer-grained partitioning of recursive servers. However, this method requires recording all directions of IP traffic, which is not trivial in practice and may cause privacy concern.

The problem that this article focuses on is the role identification of the DNS server in the case of using only DNS response data (removing the receiver IP). The proposed method is based on the DNS protocol standards and the configuration practice of DNS server with different roles. Leveraging three categories of features extracted from the DNS response records, a machine learning classifier is trained on a labeled dataset and then applied to identify the role of the DNS server. Four popular machine learning algorithms are used in the experiment with k-fold cross validation, among them the random forest algorithm shows the best performance, achieving 99.28% accuracy with an approximately 0.7% false positive rate.

The rest of this paper is organized as follows. The following section describes the background knowledge. Section 3 presents the methodology, including an analysis of the two DNS header flags previously used for DNS role identification and a detailed description of the extracted features. Section 4 discusses the experiment and the evaluation. Finally we conclude in Section 5.

2. BACKGROUND

2.1 DNS Message and Format

Communications inside the domain protocol are carried in a single format called a message [9]. DNS message consists of a 12-byte header and four variable-length fields, namely the question, the answer, the authority and the additional.

The query and response message follow the same header format. There are thirteen fields in the header [9], of which twelve fields are used to indicate relevant information in the communication. Specifically, ID is the 16-bit identifier of the message. QR specifies the direction of the message, TC indicates whether the message is truncated, AA tells whether the answer is from an authoritative server, RD tells whether the query requires recursive resolution, and RA indicates whether the responder supports recursive function. These fields have two values (0 or 1). QDCOUNT is the number of query entries in the question part while ANCOUNT, NSCOUNT and ARCOUNT are the number of resource records (RRs) in the answer, authority and additional part respectively. OPCODE and RCODE specify the query type and response status, both of them have multiple values.

RR is the basic information unit of DNS. The same top-level format is used to describe RR and it consists of six different parts, namely name, type, class, time to live (TTL), RDLENGTH and RDATA. Among them the TTL indicates how long the RR can be cached and the RDATA is a variable length string that describes the resource.

2.2 The Role of DNS Server

Two main service categories are provided by domain name servers, i.e., authoritative service and recursive service.

A name server is authorized to provide authoritative service, responsible for maintaining and answering the RRs in a section of the namespace (called zone) [9] without having to query other servers. Normally a name server is open to any nodes as it is designed to inform the RR data of the managed domains. The main types of the name server's answer are authoritative data, a referral to other name server, an authoritative empty answer which means no RR exists for the existing requested name, and an authoritative NXDOMAIN [10] [11].

A recursive resolver answers client requests for domain names in any zone by repeatedly asking other name servers. Typically, a cache is attached to the recursive resolver to store the received results for a specified period of time (TTL), and subsequent requests during this time period will get instant answers from cache hit, thereby reducing network traffic and server load. In general, legacy recursive resolver only responses to a limited IP range considering the resource cost and security risk. Situation changed since open recursive resolvers came out, which are operated by Internet big players like Google who has enough recourses and technical strength to handle all difficulties in serving to the public. It's noted by ISC [11] that recursive resolvers are not authoritative for any zones in most cases other than the standard minimal ones and the recommended empty zones [12]. Generally, the types of the recursive resolver's response are non-authoritative data from cache, data recursively retrieved from other authoritative name servers, and the authoritative data (if any).

Technically, a single server could be configured to do both. For example, Berkeley Internet Name Domain (BIND) [13], a popular domain name resolution service software, can be deployed to provide either authoritative or recursive service or both. However, due to the different requirements of cache and the population of clients, it is recommended for a business to set up the two on separate servers. Furthermore, the name server is suggested to turn off the recursive function. With recursive function enabled, a server is more vulnerable to hijacking and compromising.

Based on the above analysis, a DNS server may plays multiple roles at the same time. But in practice only one role dominates, especially for the large DNS servers. Therefore, the typical role of a DNS server during the observation time is studied in this paper.

3. METHODOLOGY

3.1 DNS Response Analysis

The connection mode of network nodes can reflect their role. Our insights is that the responses sent by different DNS server roles present different characteristics. In specific, the semantic of most response messages such as DNS header setting and the RR information presents different states. Therefore we study the DNS response message to find more features to distinguish the roles.

According to section 2, the name server can be detected by setting the AA field in the response, and the RA field is useful for identifying recursive resolver [8]. We have made an analysis of them on our dataset (§4.1). The percentage of responses with AA=1 and RA=1 to the total are plotted in Figure 2 and Figure 3

with respect to the top 200 name servers and recursive resolvers ordered by number of responses respectively.

The results are not so satisfying. (1) Cases for recursive resolvers. 4 of the 200 recursive servers, whose ratio of RA=1 is lower than 50%. Moreover, a non-negligible proportion (31 out of 200) of recursive resolvers have a ratio of AA=1 larger than 50%. (2) Cases for name servers. There exists 74 name servers with a ratio of AA = 1 lower than 50% while 78 name servers have a ratio of RA=1 larger than 50% among the 200. We conjecture that some administrator may forget to close or deliberate to open the recursive function of their name server.

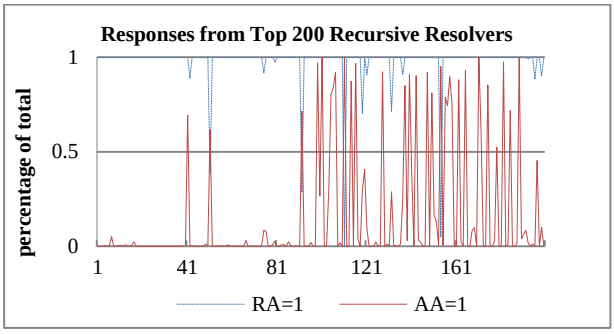


Figure 2. The proportion of RA and AA setting in the responses from top 200 recursive resolvers.

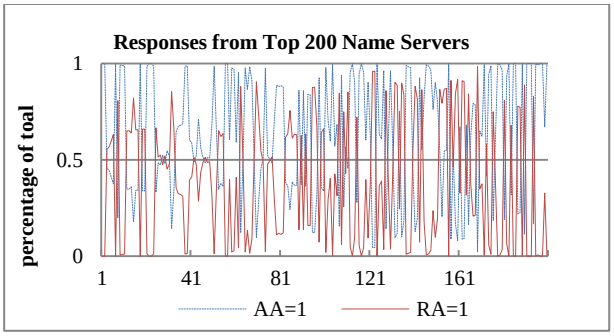


Figure 3. The proportion of RA and AA setting in the responses from top 200 name servers.

The results imply that using these two flags in the response header to identify the role of DNS server (e.g. AA0RA1 for recursive resolver and AA1RA0 for authoritative name server) does not meet expectations in real scenarios, especially for the name server. In the next subsection we will look for more features from the DNS response to bring positive effect.

3.2 Feature Extraction from DNS Responses

Through the observation and analysis, we propose three categories of features obtained from DNS response and give a detailed explanation. Each category has one or more features. Among them the RD ratio, RCODE ratio and the TTL diversity have not been studied in the context of DNS server identification before.

Category 1 (C1): response rate. Since recursive service facing the challenge of influx of name quires initiated by the clients, a recursive resolver has to handle a large number of responses per unit of time. This is particularly the case when it comes to open recursive resolvers. Benefiting from the widely deploy of cache, the traffic is significantly smaller for name servers. It is noted that one unknown recursive resolver may have lower response rate than a famous name server during the observation period, but the combination with other features can further distinguish them.

Category 2 (C2): features of the DNS header. We focus on three types of message header fields of the responses: (1) the field that shows different values due to the functional configuration difference in two roles. (2) the field which copies the value from the request message. (3) the field that shows different statistical values over time due to the diversity of situations faced by DNS servers. Firstly, the recursive resolver works like a proxy to fetch the answer from name servers or its cache instead of the end-users. It forms its own DNS answers after receiving the reply from name servers, always with AA=0 and RA=1 in the message header. Name servers serve multiple objects such as the end-user, recursive resolvers and other name servers with authoritative answers and non-authoritative referrals. The values of AA and RA are various on different level of name servers. Secondly, depending on the purpose of the requester, the fields in the query message header may have different values. Although RD is only valid in the request message, the originator of the response copies the value from the request. Recursive resolvers always receive DNS query with recursive desire by clients. For name servers, non-recursive queries are what they intended to answer while recursive queries will be refused or could be answered with referrals [14] [15]. What's more, referrals received must be followed resulting in further iterative queries to other name servers [14]. Thirdly, the name server returns non-zero RCODE when it encounters problems. For a recursive resolver, in addition to passing the error code from different authoritative name servers to end users, it also sends its own error information.

Category 3 (C3): features of the DNS resource record. Name server is authorized to manage the RRs in its zone. Names in the same zone share a common suffix section. We count the number of domain names with one or two levels of suffix domains to measure the concentration of the resolved names. TTLs in the authoritative RRs show consistency in multiple responses for the same name while recursive resolvers will decrease the value over time. Multiple RR types are defined in standards and drafts of the DNS community among which some types are mainly used by name servers, such as AXFR (zone transfer) and IXFR (incremental zone transfer).

In this paper, E is the set of DNS records in duration T and S is the IP set of the DNS servers, $< \mathrm{h}, \mathrm{w}, \mathrm{t}, \mathrm{p} >$ is set as the message header, resolved domain name, RR TTL and RR type of the answer part in a response respectively. The response records set belongs to an IP_x is denotes as $R = \{r \mid IP_x \in S, < \mathrm{h}, \mathrm{w}, \mathrm{t}, \mathrm{p} > \in E\}$. For IP_x in set S :

- Response rate is expressed by the number of the responses per second. Denote v is the response rate of IP_x, and T is the observation time in second.

$$v = |R|/T \quad (1)$$

- Header flags ratio is calculated by dividing the number of records with the flag set at a particular value by the total responses. The ratio of AA, RA, RD and RCODE with particular value are denoted as R_{AAi}, R_{RAj}, R_{RDk}, and R_{Rcode0}.

$$R_{AAi} = |L_i|/|R|, where\ L_i = \{r|\ AA = i, r \in R\}, \mathrm{i} = 0 \text{ or } 1. \quad (2)$$

$$R_{RAj} = |M_j|/|R|, where\ M_j = \{r|\ RA = j, r \in R\}, \mathrm{j} = 0 \text{ or } 1. \quad (3)$$

$$R_{RDk} = |N_k|/|R|, where\ N_k = \{r|\ RD = k, r \in R\}, \mathrm{k} = 0 \text{ or } 1. \quad (4)$$

$$R_{Rcode0} = |O|/|R|, where\ O = \{r|\ Rcode = 0, r \in R\}. \quad (5)$$

- Name concentration is defined by two values: the number of resolved domain names with the same top-level domain and the second-level domain, denoted as $NC1$, and $NC2$.

$$NC1 = |tld(w)|, w \in R. \quad (6)$$

$$NC2 = |sld(w)|, w \in R. \quad (7)$$

- TTL diversity is defined by the number of different TTL values for RRs in the answer part of all responses, denoted as D_{TTL}.

$$D_{TTL} = |t|, t \in R. \quad (8)$$

- Type diversity is expressed by the number of different RR types in the answer part of all responses, denoted as D_{type}.

$$D_{type} = |p|, p \in R. \quad (9)$$

4. EXPERIMENT AND EVALUATION

The following subsection explains the construction of the dataset and the work flow of our experiment, which is shown in Figure 4.

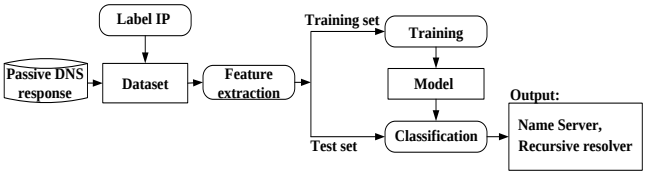


Figure 4. The workflow of the experiment.

Passive DNS response records (removing user information) are used to generate the dataset. Feature vector is further extracted for each labeled IP. Then the training data set are fed to the classifier to build the classification model. Finally, the performance of different models are tested by the test set and discussed later.

4.1 Dataset and Ground Truth

Table 1. The dataset details of the experiment

Label	IP count	Response count
Name server	1,200	1,928,488
Recursive server	1,218	2,620,038
Total	2,418	4,548,526

The experiment uses one-day passive DNS response traffic accessed from China science and technology network (CSTNET). Considering privacy protection, the destination IP of the response packet is anonymized. We extract the following information from the DNS traffic: the source IP address, four flags of the header (AA, RA, RD, RCODE) and the RR in the answer parts (take the first RR if there are multiple RRs). Then we get about 140 million records from Nov. 28th to Nov. 29th, 2019 in total.

As the proposed method is based on supervised learning classifiers, we have to find out the ground truth of the name server and recursive server IPs. Inspired by the NS type RR, we randomly select 1200 name server IPs in the NS type answers from the DNS records. Only one IP address is kept when one name server is mapped to multiple IPs. Secondly, we search in Internet and obtain 1250 IP addresses of the open resolvers and ISP resolvers manually. In addition, each IP is verified to work properly. After that, we get a DNS server IP list with the role labeled. Thirdly, we filter the DNS records by source IP and aggregate the result together for each IP in the list. IP addresses with no corresponding result are dropped. After that we have created our dataset, and the details are listed in Table 1.

4.2 Experiment Setting and Metric

The experiment is performed on a physical machine with Windows 10 (64-bit) operation system, Intel i7-10710U CPU and 16G memory. Python language and the scikit-learn machine learning library [16] are used to implement our model. Four popular supervised machine learning algorithms are adopted in our experiment, i.e., SVM, logistic regression, decision tree and random forest.

Accuracy, recall, F1, accuracy (ACC), false positive rate (FPR) and area under curve (AUC) value which are commonly used in classification algorithms are selected as the evaluation metrics in this paper. Moreover, the effect of different input features for classification are also tested in the experiment. To obtain the best error estimate, the standard k-fold cross validation method is used in the training and testing stage.

4.3 Experiment Results

4.3.1 K-fold Validation

To select the best value of k, we test different values of k in our experiment. The AUC curve plot of different k values with decision tree algorithm are shown in Figure 5. The x-axis is the FPR and the y-axis is the true-positive rate (TPR). We observe that the AUC area does not differ much when k is between 3 and 9, and k with value of 8 and 9 get the largest area. We choose k=8.

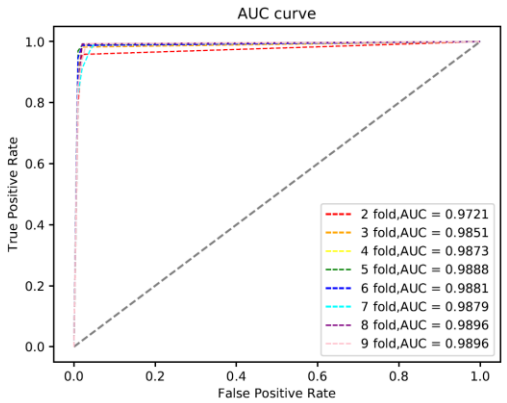


Figure 5. The ROC curves of different k-folds.

4.3.2 Comparison of Different Classifiers

Table 2 shows the performance values of four different classifiers with default parameter setting. We observe that random forest works best, all of the metrics achieving excellent values: precision, recall, F1, ACC and AUC are all higher than 99%, and FPR is 0.7%. Next is the decision tree model, whose metrics are all around 98% except FPR is 1.3%. The left two, SVM and logistic regression classifiers have similar performance, with less promising precision, recall, F1, ACC and FRP, but with good F1 higher than 95%. Random forest is a collective-learning algorithm of multiple decision trees thus it works better than a single tree.

Since few features are used in our method and the feature extraction is not complex from the passive DNS records, the processing time of our method mainly depends on the training time. The training time of each classifier with about 2000 samples are also listed in Table 2. Except for SVM, the consuming time of the other three are very small, all around 0.01 second.

Table 2. The performance of the classifiers

Classifier	SVM	Logistic Regression	Decision Tree	Random Forest
Precision	0.7450	0.7711	0.9845	**0.9940**
Recall	0.9844	0.9533	0.9793	**0.9905**
F1	0.8480	0.8524	0.9858	**0.9922**
ACC	0.8368	0.8475	0.9868	**0.9928**
FPR	0.2901	0.2433	0.0134	**0.0007**
AUC	0.8472	0.8550	0.9860	**0.9993**
Time (s)	0.0618	0.0129	**0.0080**	0.0199

4.3.3 The Importance of Each Feature

Random forest method based on information gain is used in our experiment to assess the importance of the feature, shown in Figure 6. Based on the ranks, we can conclude that the features of RA (value of 0), AA (value of 1), TTL diversity, domain concentration and RD (value of 0) play importance roles in the classification, which comply with our analysis in section 3. On the opposite, type diversion, response rate, RD (value of 1), RCODE (value of 0) and AA (value of 0) have less effect on the work. We suspect that there may be two reasons why these features differ slightly between different roles. The first is the use of cache reduces the chance of errors for recursive resolvers and the other is the low incidence of special types of responses during the observation time, which will be further studied in the future.

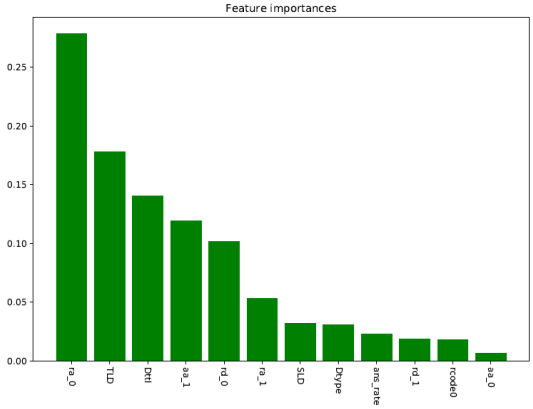


Figure 6. The importance of each feature.

4.3.4 Comparison with Other Method

Compared with the existing method FCDR [8], our experiment result is similar to its related indicators: its precision, recall and F1 are all over 99%. However, the input vector of our model has fewer dimensions. Furthermore, we only use the response records without the source IP, avoiding the risk of user privacy exposure. The FCDR method needs to obtain and analyze the record of all directions of DNS traffic, which is not trivial in practice.

5. CONCLUSION

We investigate the difference between the response behavior of name servers and recursive resolvers and extract three categories of features for DNS server role classification. We evaluate the proposed method on a real-world passive DNS response records, use four popular supervised machine learning algorithms to classify and choose the random forest classifier as the best model. The experiment results show that our method has an excellent classification performance.

6. ACKNOWLEDGMENTS

This work is supported by the National Key Research and Development Program of China with Grant No. 2016QY05X1003.

7. REFERENCES

[1] Mockapetris, P. 1987. Domain names - concepts and facilities. RFC 1034. Nov. 1987.

[2] CISA. 2015. *DNS Zone Transfer AXFR Requests May Leak Domain Information*. National Cyber Awareness System Alert (TA15-103A). CISA. Washington. USA.

[3] NIST. 2002. Buffer overflow vulnerable in named in BIND. Last accessed on Nov.18, 2019. URL https://nvd.nist.gov/vuln/detail/CVE-2002-1219.

[4] Wang, Y. , et al. Research on DNS authoritative server's performance and security. *Journal on Communications.* Vol.27, 2 (Feb. 2006), 147-152. DOI= https://doi.org/10.3321/j.issn:1000-436X.2006.02.023.

[5] Open Resolver Project. Last accessed on Nov.18, 2019. URL http://www.openresolverproject.org/.

[6] Bing, R. L. 2016. *Active measurement and analysis of open recursive DNS server*. Master Thesis. Harbin Institute of Technology.

[7] Sun, Y., Huang, C. Y., Liu, X. M. et al. 2016. Online identification method for recursive domain name server based on connection degree estimation. Patent. CN 201610144111. IIE, CAS. Beijing, China.

[8] Gao, C. L., Xun, X. C., et al. 2019. MFRdnsI: A DNS Recursive Server Identification and Classification Method Based on Deep Learning. *In Proceedings of the 2019 2nd International Conference on Information Science and Systems (ICISS 2019).* ACM, New York, NY, USA, 27-32. DOI= https://doi.org/10.1145/3322645.3322675.

[9] Mockapetris, P. 1987. Domain names - implementation and specification. RFC 1035, Nov. 1987.

[10] Albitz, P. and Liu, C. 1998. DNS and BIND. O'Reilly and Associates, Cambridge, USA.

[11] Suzanne, G., Michael, M. 2018. *Nameserver Basics: What is an Authoritative Server? What is a Recursive Server*. ISC Release Notes. ISC.

[12] Rekhter, Y. 1996. Address Allocation for Private Internets. RFC 1918, Feb. 1996.

[13] Douglas, B., Mark, P., et al. 1984. *The Berkeley Internet Domain Name server*. Technical Report. No. UCB/CSD-84-182. University of California, Berkeley.

[14] Richard, J.A. 2016. System Programming: Designing and Developing Distributed Applications.1st edition. Morgan Kaufmann, Greenwich, UK. DOI=https://doi.org/10.1016/B978-0-12-800729-7.00006-6.

[15] Zheng, W. 2013. Analysis of DNS Cache Effects on Query Distribution. *The Scientific World Journal*. Volume 2013 (2013), 1-8.Article ID 938418. DOI = http://dx.doi.org/10.1155/2013/938418.

[16] Pedregosa, G., Varoquaux, A., et al. 2011. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, Volume12 (2011) , 2825–2830, 2011. DOI= https://doi.org/10.1524/auto.2011.0951

Mapping and Generating Adaptive Ontology of Decision Experiences

Yuan Zhou
Blekinge Institute of Technology
Valhallavägen 1, 371 41 Karlskrona
+46 734 02 86 20
yuan.zhou@bth.se

Siamak Khatibi
Blekinge Institute of Technology
Valhallavägen 1, 371 41 Karlskrona
+46 455 38 55 91
siamak.khatibi@bth.se

ABSTRACT
Decision-making is shared by many disciplines. In computer science decision-making systems aim to substitute or support people for making decisions. The systems generally need to acquire as many as possible data to provide possible options for any decision-making. The possible options are usually obtained by modeling situations data. However, situation data is becoming tremendous along with daily life changes and it is becoming more and more difficult to model and restore those situation data. However as human, when the situation data is lacking, we still can make appropriate decisions based on our "decision experiences". To learn how decisions are made adaptively by humans, this paper propose a method to characterize a decision-making process for a finite number of people only based on individual's actions without modeling any situation data. Then the characterization problem is formulated as a one-dimensional decision-making process and experimented as a number guessing game. The experimental results show the feasibility of the proposed method in mapping and generation of an adaptive ontology structure of decision experiences for experimental participants.

CCS Concepts
• Computing methodologies→Knowledge representation and reasoning.

Keywords
Decision; Decision-making; Representation of uncertainty; Ontology.

1. INTRODUCTION
Decision-making is shared by many disciplines, from mathematics and computer science, through economics and political science, to sociology and psychology [1]. There are three major approaches working with decision-making: psychological, normative and cognitive. The psychological approach [2-4] can be traced to the essay that Daniel Bernoulli published in 1738 [5] in which he attempted to explain why people are generally dislike to risk and why risk disclination decreases with increasing wealth. In this approach individual decisions are examined in the context of a set of needs, preferences and values that the individual has or seeks.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388200

In the normative approach [6,7] the logic of decision-making and its consequence as an invariant choice is considered. The cognitive approach [8,9] regards the decision-making as a continuous process which is integrated in the interaction with the environment.

Figure 1. Example of a situation.

When decision making in computer science is discussed, AI is one of the first things which comes to mind [10–12]. In the field of AI, the aim is to make "intelligent" systems, i.e., computer programs and machines, which are able to make autonomous decisions by themselves [13,14]. With this aspect decision making in computer science is related to diagnosis and prediction processes. Generally, the diagnosis process includes the reconstruction of the situations data by modeling [15], model storage and classification based on comparison of the current model of situation with stored models. Diagnosis process results in possible options for decision-making and further action or optimizing possible options for decision-making and further action by outcome prediction. Both processes of diagnosis and prediction are heavily related to the situation data. The generation of autonomous decisions by this way are heavily dependent on models and situation data in relation to any situations. However everyday life is dynamic with tremendous number of situations. Figure 1[1] shows a simple countryside road. Let us imagine for a moment an autonomous car is driving in this road. For any road position the situation data should be collected and consequently a decision should be made for further action. However, a human driver can drive the whole road safely without knowing every detail on the road, no matter it is a straight or turning. As long as the driver knows the direction of final point, he or she is able to make "right" decisions and actions. One of important reasons of making right decisions is that we make decisions based on our "decision experiences" and each such experience is adaptively updated along with any new decisions

[1]Figure 1: https://pixabay.com/sv/photos/berg-v%C3%A4g-motorcykel-tur-3470062/

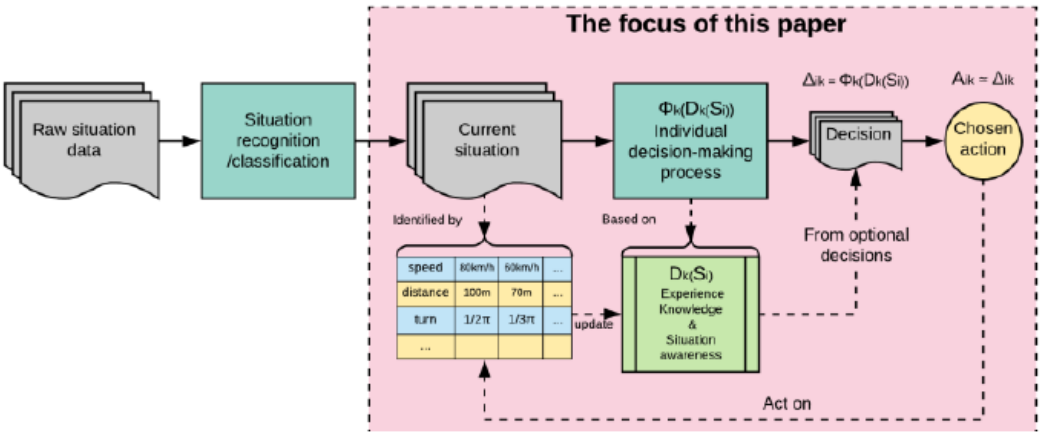


Figure 2. Involvement of decision-making process.

related to the same situations or close situations. In another word, decision experiences can be considered as human decision models in response to a range of close situations. In this paper, we are interested in modeling an autonomous decision-making process instead of model or reconstruction of situation data for making decisions in many everyday events.

To learn how decisions are made adaptively by humans, this paper investigates a method to characterize a decision-making process for a finite number of people only based on individual's actions without modeling any situation data. The characterization does not necessarily reflect an optimized pathway for making decisions in a situation, but it reflects all participants' decision experiences which are represented by an ontology structure. The ontology structure is adaptive and is changed by characterizing different group of individuals' decision-making process. The ontology structure provides a mean to generate autonomous decision-making.

This paper is organized as following: in Section2, the proposed method to characterize a decision-making process is explained. In Section 3 the characterization problem is elaborated in one-dimension and design of an experimental game in this relation is explained. The steps of experimental data processing are presented in section 4. The experimental results and analysis are presented and discussed in Section 5. Finally, the conclusion is coming in Section 6.

2. CHARACTERIZATION OF A DECISION-MAKING PROCESS

To characterize decision-making process, firstly we discuss how each individual's decision-making process is involved with other processes and how the process can be modeled. Figure 2 shows the involvement of each individual's decision-making process with other processes. Raw situation data in the figure represents the result of sampling process from one or multi sensors. Situation recognition/classification in the figure represents the modeling of situation data or diagnosis process. In the figure the current situation represents the current state/moment of decision options (DP). In this relation the DP includes a list of possible options in conjunction to each situation parameter which in their turn they define dimensionality of the situation. In the figure a multidimensional DP is shown as a matrix where each row is a list of options for a parameter or dimension (e.g. driving speed, distance to middle of road or turn mode). The columns are the possible values of each parameter (e.g. 80km/h, 0.5m, $1/2\pi$). Generally, DP is seen as a result of situation data as it was mentioned in introduction section and it is shown in the figure by connection of situation recognition to current situation. However, it is not necessary to generate DP by situation data; intensively or at all. DPs can be result of parameter reduction or casual use of situation data or using logical/fuzzy-logical functions. In a decision-making process, a DP is generated by taking to account for each individual's experience (denoted by D_k) and the situation awareness (denoted by S_i); here situation awareness is considered to be obtained by application of logical or fuzzy-logical functions. Let's denote the DP generation process by function of $D_k(S_i)$ where k and i stand for different individuals and different situations (situation states) respectively. $D_k(S_i)$ is based on each individual's decision experience with outcome of DP which is updated upon awareness of new situation. The function $D_k(S_i)$ gives adaptiveness to the whole decision-making process. Then a decision is made by $\Delta_{ik}=\Phi_k(D_k(S_i))$ where Φ is decision strategy function, k is index of individuals, i is index of situation states. The decision strategy function is varied subjectively, since it depends on individual's knowledge, preference, expectations, experiences and other background factors such as cultural [11]. For example, if we go back to our example in Figure 1, we certainly will find variation in driving among drivers who attempt to drive the same road in almost the same conditions. New decision of Δ_{ik} is expected to be executed by action of A_{ik}. We assume $A_{ik} \approx \Delta_{ik}$ i.e. the action is the physical reflection of a decision. The situation matrix is changed in consequence of any action which has a chain impact of changes in parameter data, S_i and DP. Consequently, a new decision is decided which in its turn executes a new action.

3. CHARACTERIZATION OF A ONE-DIMENSIONAL DECISION-MAKING PROCESS

An experiment is designed to elaborate the method which was discussed in Section 2. The problem is formulated as a one-dimensional decision-making process as a number guessing game; i.e. to choose a number between 1 to 100. In the experiment N number of subjects are asked to find a random integer number which is predefined from 1 to 100. Each subject tries to achieve the goal in several attempts where the number of attempts is not limited. In each attempt there are two questions of 1)- "Is this targeted number bigger than my chosen number?" and 2)- "Is this

targeted number equal to my chosen number?" which the subject needs to choose one of them. Then the subject decides a number. The program is answering the subject by "Yes" or "No" and then the range of targeted numbers is changed according to the subject's chosen question and number. The steps of each attempt in the guessing number game are shown in Figure 3. In the figure type 1 or type 2 refer to the two game questions. The game ends if the targeted number is identified in the attempt. Otherwise the subject is proceeding to a new attempt.

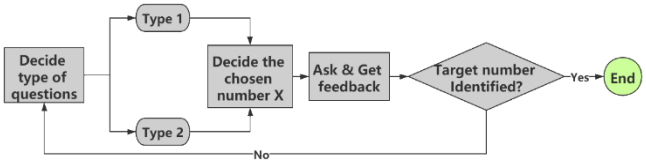


Figure 3. Experiment execution.

4. EXPERIMENT

In this section the data collection, processing and analysis related to the designed game in Section 3 are presented.

4.1 Data Collection

A web-based application (http://123.207.167.171/Guess/) was developed for collecting experimental data. Through visiting the website, 33 subjects were participated in the experiment. During the experiment, the data of subject's choices (i.e. choose of a number and a question) in each attempt were collected as action data. In addition, each subject's demographic information (i.e. gender, residence, age and education level) was collected for further analysis of data.

4.2 Data Processing

The action data was processed in six stages: data normalization, data clustering, generation of fuzzy-cluster, data association, and mapping and ontology structure. We explain these stages in following sub-sections.

4.2.1 Data Normalization

Before normalization, a preprocessing on the collected data was conducted. The chosen numbers in the type 1 question (i.e. "Is this targeted number bigger than my chosen number?") were used as the related action data during decision-making process. The chosen numbers in the type 2 question (i.e. "Is this targeted number equal to my chosen number?") were seen as they introduced another dimension into the characterization of decision-making process; i.e. the data could represent "wild guessing" and its usage frequency or time of occurrence could be used as another dimension. For each subject, there were a sequence of actions; $A_k = \{X_{ik}\}$, where X was the chosen number, k was the index of subjects and i was the index of attempt.

After the preprocessing, each subject's action data A_k was normalized in relation to the targeted range to obtain a value between 0 and 1 in each attempt of i. The sequence of actions of each subject were used to obtain decisions; $\Delta_k = \{P_{ik}\}$, where P_{ik} is the percentage ratio of new range of DP (caused by the action) to old rang of DP for subject k in the attempt i. This is demonstrated in Figure 4 where either the left or the right range to the chosen number was dividing to the old range. The choice of left or right range was determined by position of chosen number in the next attempt due to subject's intention to delimit the search range.

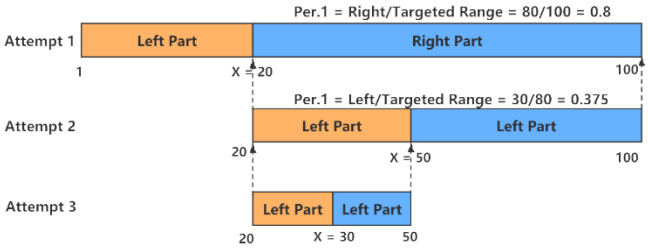


Figure 4. Relation of decision to action in sequence of attempts.

4.2.2 Data Clustering

The sequence of decisions of each subject; Δ_k, was classified by clustering in three steps:

- *Clustering Each Subject's Decisions.*

K-means clustering method was used to cluster each subject's decisions. The number of clusters was identified by increasing the number of clusters in one-steps manner until any one-element cluster was occurred; each cluster included decision elements. Thus one-element cluster had only one decision. The clustering algorithm is shown in Figure 5(c).

- Cluster *Merging*

The merging possibility of one-element-clusters to multi-element-clusters (i.e. having more than one element) of each subject was examined by using t-test with 95% confidence. Each one-element cluster was checked with the nearest multi-element-cluster using t-test. If the null hypothesis was not rejected, the one-element-cluster was merged to the nearest cluster; i.e. the decision element of one-element-cluster merged to the multi-element-cluster.

- Ensemble *of Remaining One-element-clusters From All Subjects and Re-clustering.*

Those one-element-clusters which were not merged with other clusters of each subject were collected from all subjects. Their collection was seen as a new sequence of decisions from a virtual subject which were processed by steps of 1 and 2.

(a) Association Algorithm

```
Input:
fuzzyCluster_dist = {fdi}, i = 1,2,...,n; set of n fuzzy-cluster distributions with
normalized amplitude
dist_amp = {ampi}, i = 1,2,...,n; set of each distribution's amplitude
weight = [Wi, Wj]; weights of each two fuzzy clusters

Output:
two_association = 0; the assocation of each two fuzzy clusters

for i = 1:n
    for j = 1:n
        if (i ~= j)
            Wi = ampi/ampi + ampj;
            Wj = 1 - Wi;
            two_association = Wi * fdi + Wj * fdj;
        endif
    endfor
endfor
```

(b) Ranking Algorithm

```
Input:
association_of_n; an association of n fuzzy-clusters
decision_clusters = {dci}, i = 1,2,...,n; the set of decision clusters for each subject
number_of_decisions = {ni}; the set of number of decisions in each decision cluster
decision_positions = {dpij}, j < i; the set of decision positions in dci

Output:
sum_amp = {spi}, i = 1,2,...,n; the set of amplitude accumulation for each cluster
rank_index = {i}, i = 1,2,...,n; the set of each cluster's ranking index

sum_amp = accumulate(association_of_n, dpij); the function accumulating the
amplitude of dpij in assocation of n distribution

rank_index = rank(sum_amp); the function assigns ranking index to each cluster
based on the values of sum_amp
```

(c) Clustering Algorithm

```
Input:
FDmk = {Pik}, i = 1,2,...,m; the sequence of decisions of subject k
n = 1; the number of clusters

Output:
cluster_index = {Pj}, j = 1,2,...,n; j is the cluster index of each percentage value

While(1)

    if (there is a one-element cluster or n == m)
        break;
    else
        cluster_index = kmeans(FDmk, n);
        n = n + 1;
    endif

endwhile
```

Figure 5. Algorithms.

4.2.3 Generation of Fuzzy-cluster

Every multi-element-cluster of all subjects was modelled by using t-distribution due to general limitation in number of elements and better performance of t-distribution in comparison to Gaussian distribution when the number of elements is less than 30. This was achieved by using a modeling function[2] in Matlab [16]. The mean and sigma values of the modelled t-distribution were used to generate t-distributed clusters. The amplitudes of these clusters were normalized to values between 0 to 1. Then a weighted factor was multiplied to the amplitude of each fuzzy-cluster. The weighted factor was the number of elements which contributed to generation of t-distributed cluster. The clusters were generated by this way were called fuzzy-cluster.

4.2.4 Data Association

The association relation between each two fuzzy-clusters was defined as $C_a = W_1C_1 + W_2C_2$ where $W_1 = C_{amp1} / (C_{amp1} + C_{amp2})$, $W_2 = 1\text{-}W_2$, C_a is the associated-cluster, C_1 and C_2 are the first and second fuzzy-cluster respectively, W_1 and W_2 are the first and second associated-weights in relation to first and second fuzzy-cluster and C_{amp1} and C_{amp2} are the amplitude of first and second fuzzy- cluster. The association algorithm is shown in Figure 5 (a).

4.2.5 Mapping

The mapping was defined as $\Phi_{est} = \sum_i^M C_{ai}$ where C_{ai} is the associated-cluster between each two fuzzy-clusters, M=n(n-1)/2 where M is the number of associated-clusters, n is the number of fuzzy-clusters and Φ_{est} is the estimation of decision strategy function.

4.2.6 Ontology Structure

The clusters of all subjects were used in a ranking process. In the process, for each cluster the values of Φ_{est} for the position of elements were calculated and then they were accumulated. The ranking algorithm is shown in Figure 5(b).

5. RESULTS AND ANALYSIS

The conducted game experiment is used to obtain the results which are in relation to the decision-making process; as shown in Figure 2. The experimental results and their analysis are discussed in this section. Firstly, each subject's sequence of action data was collected as reflections of subject's sequence of decisions in the experiment. The actions were interpreted as decisions based on the targeted range (i.e. current situation) which provided a set of possible targeted numbers (i.e. the options) for each subject. After each decision and consequent action, possible targeted numbers were reduced as result of the targeted range partitioning which in its turn increased the probability of identifying the targeted number. The essence of major subject's decisions was to reduce the number of options for the targeted number. In the experiment, decisions were made in the one-dimensional situation. However, the implemented core idea of decision-making process can be used in the multi-dimensional situation where new DPs are obtained from the matrix in Figure 2.

Subjects' decision-makings are influenced at each deciding event (i.e. attempt) by subjective factors such as knowledge, preference, expectations, experiences, and other background factors such as cultural. However, the decisions are made according to one or several decision strategy(ies). By identifying such limited decision strategy(ies) for each subject in the experiment it became possible to collect/record the subjective decision/experience. For instance, in Figure 6 (a), the subject's decisions were around 0.5 which means her or his decision strategy was according to partitioning the targeted ranges at around middle points in each attempt. To find decision strategies from all subjects, each subject's sequence of decisions was collected at different events (i.e. attempts) and clustered according to Section 4.2.2. The typical results of clustering are shown in Figure 6(a-c, f). However, each cluster is just a preliminary representation of the subject's decision strategy which only included limited decision-making attempts in a sequence of events (i.e. during the experiment). The preliminary representation lacks to show the relation among initial decisions and variation possibility of them. To overcome this lack an ambiguity function is introduced, and initial decisions are used to generate fuzzy-clusters, see Section 4.2.3.

A fuzzy-cluster includes not only initial decisions but also fuzzy decisions (i.e. variation possibility of initial decisions). Two example results of fuzzy-clusters are shown in Figure 6(d). The representation of decision strategy was enhanced by generation of fuzzy-cluster by including broader possibilities. The modeling of ambiguity function was based on the initial decisions in this paper. However, such modeling can be influenced by other factors such as subject's preference, expectation to the related decision strategy. The fuzzy cluster showed relations among decisions by their positions and probabilities (i.e. revealed by amplitudes) in one decision strategy. Thus, as long as the fuzzy-cluster was identified, each subject's initial decisions became a set of samples belonging to one decision strategy. As well, this sampling idea was used in characterization of decision-making process which is discussed in following. Note, t-distribution was used for modeling decision strategy, but it is not the only choice. The choice of model depends on the naturality of initial data set [17] and defined factors/parameters which can influence a decision.

The characterization of subjects' decision-making process was revealed by how the decision strategies were related to each other. Before characterizing all decision strategies of all subjects, the relationship between each two decision strategies was considered by associating their fuzzy-cluster distributions. The algorithm of association was addressed in section 4.2.4. As the Figure 6 (d) shows, their commonness and difference are reflected by amplitude of the associated distribution. The over lapping part of two distributions (i.e. where the commonness between two decision strategies) has higher amplitude after association. While the difference is reflected by lower amplitude. In addition, the weight of each fuzzy-cluster also has impact on the amplitude, the more weighting, the more initial decision was sampled in the fuzzy-cluster; i.e. there are more certainty about modeling of ambiguity function. After associating each two fuzzy-clusters, the whole group's decision strategy was estimated by accumulating all their associated distributions, the algorithm was shown in section 4.2.5. The result in Figure 6(e) shows a distribution of all decision strategies which is the characterization of subjects' decision-making process.

At last, the ontology structure of all decision strategies was built by mapping their initial decisions positions back to the distribution Φ_{est} and ranking the accumulations of amplitudes at the corresponding positions. In Figure 6(g), the table shows a 1-D ontology structure of decision strategies. The higher layer in the ontology means the higher rank of this decision strategy which share more commonness with other cluster. The ontology structure gives us a likelihood that each decision strategy could be used by a group of subjects in a given situation. This likelihood is

[2] fitdist (x, 'tLocationScale'): https://se.mathworks.com/help/stats/fitdist.html

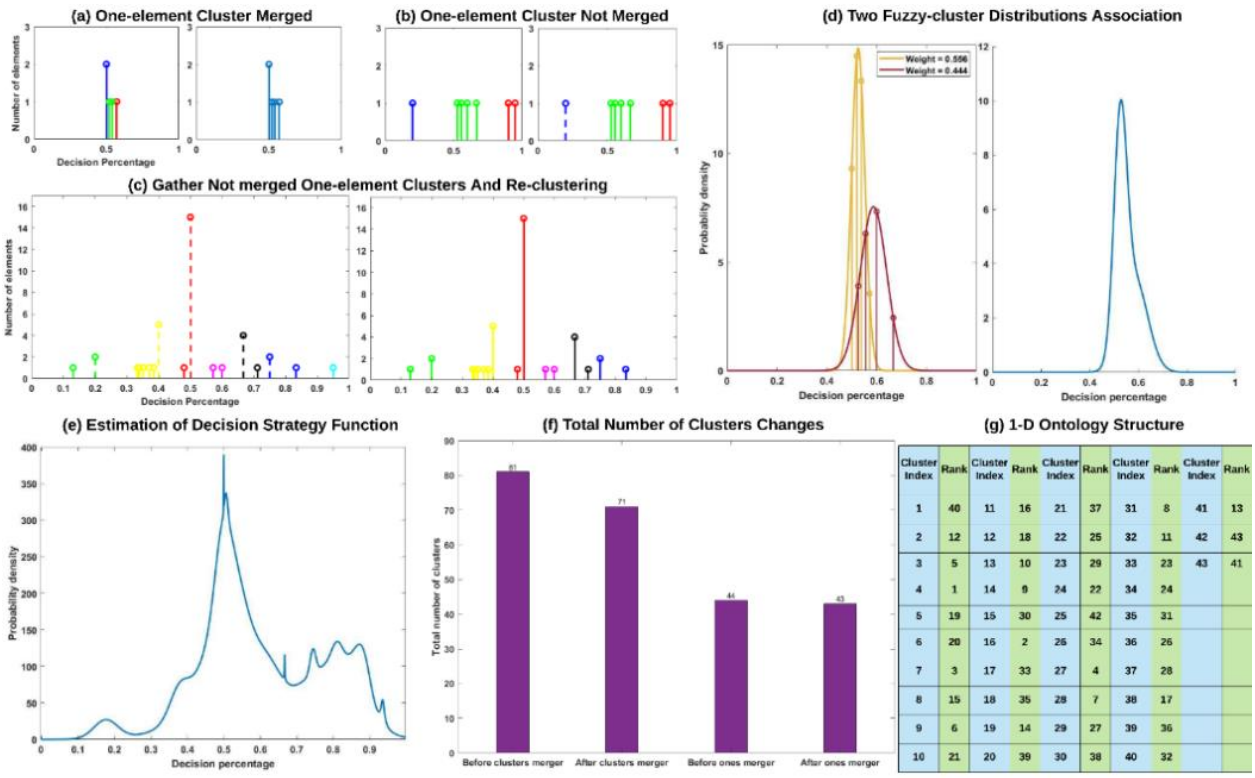


Figure 6. Results.

regarded as a decision experience of this group. In addition, this ontology structure is not rigid, it can be updated if a new group's decision-making process is characterized and this new characterization will lead to a new mapping between each decision strategy and the distribution of all decision strategies.

6. CONCLUSION

In this paper, a decision-making process is characterized and a decision experience is represented by a new proposed method with following steps: 1) sampling a group of subjects' decisions from their actions in a given state/moment of situation; 2) clustering each subject's decisions; 3) modeling each decision cluster and consequently generating a fuzzy-cluster; 4) finding the association between each two fuzzy-clusters as a new associated-cluster; 5) characterization of a decision-making process by estimation of the decision strategy function; 6) generating an ontology structure of decision experience by ranking decision clusters. The result shows a feasible way to represent decision experience without modeling of situation data, which provides a new angel to investigate autonomous decision-making process by learning the decision experiences. In addition, it is shown by the results that the ontology structure of decision experience can be generated adaptively by characterizing different groups' decision-making process. This provides a way to optimize the decision-making process when the actions of a group of experts, i.e. optimal decision makers, are collected in a given situation. In future work, we will investigate the ontology structure of decision experiences in conjunction of their orders in the sequence of decisions.

7. REFERENCES

[1] D. Kahneman and A. Tversky, "Choices, Values, and Frames," in *Handbook of the Fundamentals of Financial Decision Making*, vol. Volume 4, 0 vols., WORLD SCIENTIFIC, 2012, pp. 269–278.

[2] C. J. D. Patten, A. Kircher, J. Östlund, L. Nilsson, and O. Svenson, "Driver experience and cognitive workload in different traffic environments," Accid. Anal. Prev., vol. 38, no. 5, pp. 887–894, Sep. 2006.

[3] O. Svenson, "Decisions among time saving options: When intuition is strong and wrong," *Acta Psychol. (Amst.)*, vol. 127, no. 2, pp. 501–509, Feb. 2008.

[4] A. K. Debnath, N. Haworth, and A. Rakotonirainy, "Driver beliefs regarding the benefits of reduced speeds," *J. Transp. Saf. Secur.*, vol. 9, no. 4, pp. 470–488, Oct. 2017.

[5] D. Bernoulli, "Exposition of a new theory on the measurement of risk," in *The Kelly Capital Growth Investment Criterion*, vol. Volume 3, 0 vols., WORLD SCIENTIFIC, 2011, pp. 11–24.

[6] V. H. Vroom, "Leadership and the decision-making process," *Organ. Dyn.*, vol. 28, no. 4, pp. 82–94, Mar. 2000.

[7] R. Ayman and K. Korabik, "Leadership: Why gender and culture matter," *Am. Psychol.*, vol. 65, no. 3, pp. 157–170, 2010.

[8] Y. Wang and G. Ruhe, "The Cognitive Process of Decision Making," *Int. J. Cogn. Inform. Nat. Intell. IJCINI*, vol. 1, no. 2, pp. 73–85, Apr. 2007.

[9] G. Phillips-Wren, D. J. Power, and M. Mora, "Cognitive bias, decision styles, and risk attitudes in decision making and DSS," *J. Decis. Syst.*, vol. 28, no. 2, pp. 63–66, Apr. 2019.

[10] W. D. Holford, “Emphasizing Mètis Within the Digital Organization,” *J. Glob. Bus. Technol.*, vol. 15, no. 1, pp. 58–66, Spring 2019.

[11] P. Tang, H. Wang, C. Qi, and J. Wang, “Anytime heuristic search in temporal HTN planning for developing incident action plans,” *AI Commun.*, vol. 25, no. 4, pp. 321–342, Jan. 2012.

[12] A. Osório and A. Pinto, “Information, uncertainty and the manipulability of artificial intelligence autonomous vehicles systems,” *Int. J. Hum.-Comput. Stud.*, vol. 130, pp. 40–46, 2019.

[13] M. Bohanec, “Decision Making: A Computer-Science and Information-Technology Viewpoint,” *Interdiscip. Descr. Complex Syst. INDECS*, vol. 7, no. 2, pp. 22–37, Dec. 2009.

[14] K. Parry, M. Cohen, and S. Bhattacharya, “Rise of the Machines: A Critical Consideration of Automated Leadership Decision Making in Organizations,” *Group Organ. Manag.*, Apr. 2016.

[15] B. Rousso, D. Dickman, M. Nagler, and S. Vallabhajosula, “Multi-dimensional image reconstruction and analysis for expert-system diagnosis,” US7872235B2, 18-Jan-2011.

[16] S. Hurst, “The characteristic function of the Student t distribution,” *Res. Rep. Stat. Res. ReportCentre Math. Its Appl. Canberra*, 1995.

[17] P. Cintula, P. Hájek, and C. Noguera, *Studies in Logic, Mathematical Logic and Foundations*. London: College Publications, 2011.

CDN-hosted Domain Detection with Supervised Machine Learning through DNS Records

Hailing Li
Institute of Information Engineering, Chinese Academy of Sciences
School of Cyber Security, University of Chinese Academy of Sciences
CNCERT/CC
Beijing, China
lihailing@iie.ac.cn

Longtao He*
Corresponding author
Institute of Information Engineering, Chinese Academy of Sciences
CNCERT/CC
Beijing, China
hlt@cert.org.cn

Hui Zhang*
Corresponding author
Institute of Information Engineering, Chinese Academy of Sciences
School of Cyber Security, University of Chinese Academy of Sciences
CNCERT/CC
Beijing, China
zhanghui@iie.ac.cn

Kai Zhang
CNCERT/CC
Beijing, China
zhangkai@cert.org.cn

Xiaoqian Li
CNCERT/CC
Beijing, China
lxc@cert.org.cn

Chenghai He
CNCERT/CC
Beijing, China
hechenghai@cert.org.cn

ABSTRACT
Content delivery network (CDN) has become a critical infrastructure in the Internet and DNS-based request routing mechanism is widely used in CDNs. The current methods of CDN detection mainly use information such as hostname keywords, keywords in HTTP error message, PTR records and the public posted IP ranges. However, the application scope of these methods is limited. Considering the fact that CDN-hosted sites show some characteristics during the domain name resolution process, a novel machine learning algorithm for CDN-hosted site detection is proposed in this paper and three categories of features related to IPs, domains and TTLs are extracted from the DNS records. Machine learning classifiers are trained on a labeled dataset and the experimental results show that the method can achieve good precision and F1 score. Based on the feature evaluation, the IP and TTL related features are found to be more useful.

CCS Concepts
• **Computing methodologies** → **Feature selection**
• **Networks** → **Network measurement.**

Keywords
CDN-hosted domain detection; request routing; DNS records; machine learning algorithm.

1. INTRODUCTION

With the rapid growth of the Internet and the abundance of web content, the ever-growing number of access requests from decentralized clients poses great challenges to Internet content providers (ICPs). Content delivery network (CDN), an intelligent virtual network built on top of the existing network, was introduced to address this urgent need. CDN can duplicate content from the original web servers and response the requests from end-users with good scalability, reliability and availability by exploiting advanced technologies and placing surrogate servers deep into Internet service providers (ISPs) [1] or on the edge networks [2] all over the world.

Domain name system (DNS), which was invented to translate the human recognizable domain names to computer-processable IP addresses, has become a fundamental component of the Internet today. With the help of DNS, domain name becomes the actual entry for end-users to access the Internet. Due to the nature of ubiquity and robustness, DNS is now widely used in the field of traffic control in addition to its original usage. A typical application case is DNS-based request routing technology, which uses DNS-based method to take over the resolution of the customer domain to CDN's facilities and offer transparent and agile control for the end-user's requests. The advantage of making minor changes to customers makes it adopted by a significant proportion of CDN vendors such as Akamai and Limelight.

The measurement of CDN is important for understanding the architecture, service performance and technological evolution of CDN, among which CDN detection is the most critical step. Several methods were proposed to discover or verify the CDN network footprints in previous studies. Huang [3] and Guo [4] used HTTP error message returned by the server to discover the CDN nodes. Adhikari [5] identified CDN by the keywords in the canonical names. Timm [6] and Oliver [7] guessed the naming convention of CDN edge servers to construct the host name, and performed DNS probes to get more node IPs. Xue [8] used the public published IP ranges of CDN to verify the collected IP addresses. These methods, although simple and effective in collecting one or some CDN's resources to measure the CDN's scale and performance, their application is very limited. PTR [9] records and WHIOS information [3] are also used to look for the

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom.

ACM ISBN 978-1-4503-7725-6/20/03 …$15.00.
https://doi.org/10.1145/3388176.3388206

CDN IPs. These methods can be generalized to other CDNs, but the effects are not good because CDN vendors do not always set PTR records for their IPs. Li [9] discussed the characteristics of the CDN domains and fast-flux domains and proposed a deep learning method mainly for fast-flux domain detection.

In this paper, we focus on one important means by which CDN vendors adopt to provide services: DNS-based request routing technology and propose a novel approach to detect the CDN-hosted domain (hereinafter called CDNized domain) through the complete DNS resolution records of the domain. Our observation is that under the role of DNS-based request routing mechanism, CDNized domains will show some rules during the domain resolution process. Therefore, three categories of features related to IP addresses, domains and TTLs are analyzed and extracted from the DNS records. A machine learning classifier is trained on a labeled dataset. Logistic regression and random forest are adopted in the experiment with k-fold cross validation, both of them have a good performance, and the better one can achieve the precision of about 96% and the F1 score of approximately 94%. Based on the feature importance assessment, the IP and TTL related features are shown to be more helpful for detection.

The paper is organized as follows. Section 2 gives the background and related work. Section 3 describes the framework of the methodology and the extraction of the features. Section 4 summarizes the generation of the label dataset. Section 5 presents the experiment setting and results. Finally we make our conclusion in section 6.

2. BACKGROUND

2.1 Time to Live

A resource record (RR) is the basic data unit in the DNS that defines the components that support a domain. There are multiple types of RR and the most popular three types are A, NS and CNAME [10]. Each RR is associated with a time to live (TTL) value indicating how long the RR is valid. The TTL value is assigned at the authoritative name server of the zone. When the RR is cached by the recursive resolvers, responses to the clients will get gradually decreased TTL value over time until the RR expires and a new query will be issued to the authoritative server.

Larger TTL value means the record cache will live longer and end-user will get faster response from higher cache hit rates, ultimately reducing the DNS traffic in the network. Therefore, the TTL value could be set at a relative large value to maximize the cache efficiency of DNS. However, on the other hand, large TTL value makes any change of the RR take a long time to update or even cause some serious problems like service failure. Small TTL value provides a service provider more agility in mapping and directing traffic [11]. But small TTL value will reduce the caching effect and push query pressure on the name server. In summary, the setting of the TTL is a complex engineering problem to balance the tradeoff with the efficiency and flexibility.

In practice, for records that rarely change, it is best to keep the TTL value between an hour (3600s) and a day (86400s) [12]. It suggested by RFC 1035 that when it is expected to make changes to the records, the domain owner can lower the TTL value in prior of the change to ensure that the changes will propagate quickly. Under some circumstances, the mapping IP needs to quickly change over time to adapt with the current network environment, such as the traffic engineering and replica selection, the TTL will be configured at a small value on the order of few minutes [13]. By means of this, the authoritative name servers can response the optimal RR dynamically to the requester.

2.2 DNS-based Request Routing Technique

The aim of request routing technique is redirecting client requests to appropriate surrogate servers based on specify metrics and policies. There are different levels of request routing mechanisms including DNS request-routing, transport-layer request-routing, and application-layer request-routing [14]. According to a recent empirical analysis [15], the most popular solution is based on DNS. In this paper we only consider DNS-based request-routing. There are two consecutive steps in DNS-based request-routing: customer domain delegation and surrogate server selection [15].

In the first step, CDN providers obtain the domain resolution delegation from the customer. This step requires the customer involvement to establish a link between the CDN vendor and itself. After delegation, subsequent requests for the customer's domain are redirected to the CDN. Common methods for domain delegation are NS hosting and CNAME redirection.

a) NS hosting. The customer changes its authoritative name server to a CDN vendor-designated name server by modifying the NS record. After the record takes effect, the CDN name server will become the new authoritative server for the customer's domain, and the RRs of the customer's domain space will be taken over by the CDN. Figure 1 gives an example of NS hosting.

b) CNAME redirection. Customers set up a new CNAME record to a domain following the name conversion method specified by the CDN vendor. For example, Cloudflare instructs their customer to set the original domain in front of the given suffix domain to form a new domain, while Akamai combines a numbered user identifier with the specified suffix domain. Figure 2 gives an example of ordinary CNAME redirection. It is noted that CDNs may use multiple CNAME records (called CNAME chain) to provide the same customer with different kinds of services [15]. Figure 3 gives an example of CNAME chain redirection. The first CNAME record is used for binding the customer with the CDN, the next CNAME redirection is used for service selection.

```
root:~$ dig NS zellwk.com
zellwk.com 21599 IN NS ivy.ns.cloudflare.com
zellwk.com 21599 IN NS will.ns.cloudflare.com
root~$ dig zellwk.com
zellwk.com 299 IN A 104.28.17.31
zellwk.com 299 IN A 104.28.16.31
```

Figure 1. NS hosting mechanism.

```
root:~$ dig www.lifo.gr
www.lifo.gr  1828  IN  CNAME www.lifo.gr.cdn.cloudflare.com
www.lifo.gr.cdn.cloudflare.com  299  IN  A  104.16.169.82
www.lifo.gr.cdn.cloudflare.com  299  IN  A  104.16.170.82
```

Figure 2. CNAME redirection mechanism.

```
root:~$ dig www.dell.com
www.dell.com  3265  IN  CNAME  www1.dell-cidr.akadns.net
www1.dell-cidr.akadns.net 3599  IN CNAME  cdn-www.dell.com.edgekey.net
cdn-www.dell.com.edgekey.net 16091 IN CNAME cdn-www.dell.com.edgekey.net.globalredir.akadns.net
cdn-www.dell.com.edgekey.net.globalredir.akadns.net 3599 IN CNAME e28.ca2.s.t188.net
e28.ca2.s.t188.net 19 IN A  60.221.216.38
```

Figure 3. CNAME chain redirection mechanism.

In surrogate selection step, all the work is done under the control of the CDN. Anycast or DNS hierarchy are adopted by CDNs to complete server selection. The former simply assigns anycast IP addresses to globally distributed surrogates and select the closest edge server by BGP routing protocol. The disadvantage of this method is being unaware of network performance and server load,

resulting in suboptimal results. The latter uses DNS hierarchy to give the RR of the best surrogate based on calculating complex metrics such as geographical or topology proximity, current network performance, server load, etc. The last three lines of resolution records (content under the dotted line) in Figure 3 show the process of DNS-based surrogate selection.

2.3 Other Services using DNS Magic

CDN vendors provide multiple forms of services to their customers. Customers can use the delivery service that fully replicate the sites or the one that dynamically replicate the object to CDN surrogates. Alternatively, customers with own replicated sites could just outsource the CDN's server selection technology [13], which is usually called server load balance. In addition to CDN, there are several other cases which also use the DNS-related methods.

a) Website management practice. CNAME is commonly used to redirect the sub-domains to the domain. Although multiple sub-domains are provided to users to visit, the content is ultimately served by only one or a few servers. An example is shown in Figure 4. Moreover, the two domains always exist in the same zone and have limited IPs.

```
root:~$ dig www.list-manage.com
www.list-manage.com 21599 IN CNAME list-manage.com
list-manage.com 3599 IN A 205.201.132.96
```

Figure 4. An example for website management practice.

b) Web hosting. Modern ICPs tend to rent physical or virtual servers with independent IPs from Internet datacenters (IDCs) or cloud service vendors. ICP may use the same method as domain delegation in CDN to map the website domain to the leased resources. Other than that, they are no different from ordinary website management.

c) Fast-Flux. Fast Flux is a DNS technique used by botnet to hide the malicious activities, behind a dynamic network of compromised machines acting as proxies [16]. The adversary quickly changes the IP address mapping to a domain name at high frequency, by means of setting short TTL values in the DNS record. And the mapping IP addresses are very messy in terms of C-class segment and AS.

Since these services are easily confused with the CDN in DNS records, they should be carefully distinguished when researching the detection method.

3. METHODOLOGY

3.1 DNS Records Feature Analysis

3.1.1 IP-related Features

Leveraging the globally distributed CDN infrastructure, a CDNized domain is resolved to different IP addresses close to the location of end-users or local resolvers. This means the IP addresses of a CDNized domain are geographically dynamic. Furthermore, multiple IP addresses show certain dispersion in network segments and ASes in consistent with the deployment scope of the CDN surrogates. In one geographic area of the CDN, surrogates are usually configured into a group or cluster [13]. Therefore, although it may change with time, the IP address resolved from the same location will be in the same cluster. For fast flux domain names, the IPs show great time variability, but there is no geographical variability in a single measurement. For ordinary website domains, no matter hosting on self-built or rented resources, the number of the mapping IPs is small.

Three features related to IP address, i.e., N_{IP}, N_{IPC}, N_{AS} are denoted as follows.

- N_{IP}: Number of different resolved IP addresses in resolution records from different locations.
- N_{IPC}: Number of different 24-bit C-class segments for the resolved addresses in resolution records from different locations.
- N_{AS}: Number of different AS for the resolved addresses in resolution records from different locations.

3.1.2 Domains-related Features

For the sake of clarity, we define the following terms to describe the features related to domains.

User entry. The original domain name requested by the end-user.

CDN entry. The first CNAMEd domain in the domain delegation stage, which means that the resolution enters into the CDN's infrastructure.

Surrogate name. The domain name in the A record, which is the name of the selected surrogate server.

CNAMEd name set. The set of all CNAMEd domains in a complete DNS resolution.

3.1.2.1 Similarity between the Client Entry and the CDN Entry's Hostname Part

In the domain delegation phase, customers want to use their site-related keywords to built the CDN entry so that their assets are tightly bound to the domain, which is better in terms of CDN SEO. Therefore, similarity exists to some extent between the strings in the user entry and the CDN entry. Figure 2 show an example. At the same time, it should be carefully differentiated from the situation of the same second level domain (SLD) which indicates that it is could be a website management practice. So we only use the hostname part of the CDN entry to compare.

It is noted that not all the CDN allow the customer to contain their keywords in the CDN entry, therefore the similarity will not exist, but the combination of other features can further distinguish.

We denote $\mathrm{Sim_{UC}}$ as the similarity between the user entry and the host part of the CDN entry. It is calculated by simply comparing the effective SLD of the user entry and the hostname part of the CDN entry. If they are the same, we will assign it to 1, otherwise -1. More sophisticated methods for string similarity can also be applied to get a specific value.

- $\mathrm{Sim_{UC}}$: Similarity between the client entry and the host part of the CDN entry in a resolution record.

3.1.2.2 Difference between the SLD of the User Entry and the SLDs of the CNAMEd Name Set

User entry is the customer's asset, which is usually located in different domain zones from the CDN. Considering that a CDN customer's user entry may have a CNAME redirection to another own domain name (usually the parent domain located in the same zone), we compare the SLD of the user entry with the SLDs of each domain in the CNAMEd name set, instead of the SLD of the first CNAMEd name.

We denote $\mathrm{Diff_{UC}}$ and calculate it as follows. If any CNAMEd domain has different SLD from the user entry, we assign it to 1, otherwise -1.

- $Diff_{UC}$: Difference between the SLD of the user entry and the SLDs of the CNAMEd name set.

It should be noted that private CDN may use the same name space as the user entry, and the combination of IP features can further distinguish.

3.1.2.3 Features of the Surrogate Name

CDNs maintain a large number of surrogate servers. For convenience, their server administrators usually serialize the hostname and mix it with some specific information about the server, such as the server's location, cluster, and service type [6] [7]. Therefore, the surrogate servers of the CDN show different characteristics from the ordinary domain name in the domain name composition, whose hostname part contains more digits, dots and hyphens.

Therefore, three features, i.e, N_{dot}, N_{digit} and N_{hyphen} are defined as follows.

- N_{dot} : Number of dots in the surrogate name.
- N_{digit} : Number of digits in the surrogate name.
- N_{hyphen} : Number of hyphens in the surrogate name.

3.1.3 TTL-related Features

Customers and CDNs hope to build long-term relationship. Therefore, the RR in the domain delegation stage will be rarely changed, and the TTL value can be set at a relative large number. In contrast, the RR of the surrogate server has a small TTL value to support the CDN with sufficient agility to dynamically adjust the mapping result according to the network situation. Table 1 shows the TTL value for the RR of surrogate server in some popular CDNs.

Table 1. TTL values for the RR of surrogate in some CDNs

CDN Vendor	TTL Value / second
Akamai	20
Fastly	30
Limelight	300
Amazonaws	60
Alicdn	60
Baiduyun	300, 60

For the results of one resolution, and the results of multiple resolutions at different locations, we denote six features as follows.

- maxATTL : The maximum TTL value of A record in resolution records from different locations.
- meanATTL : The average TTL value of A record in resolution records from different locations.
- maxCTTL: The maximum TTL value of the CDN entry record in resolution records from different locations.
- meanCTTL: The average value of the CDN entry record in resolution records from different locations.
- ATTL : The TTL value of the A record in a resolution.
- CTTL : The TTL value of the CDN entry record in a resolution.

3.2 Detection Framework

Using the DNS records features of domain name analyzed in the previous subsection, this paper proposes a CDNized domain name detection method based on supervised machine learning model, called the CDD method. The structure of the method is depicted in Figure 5.

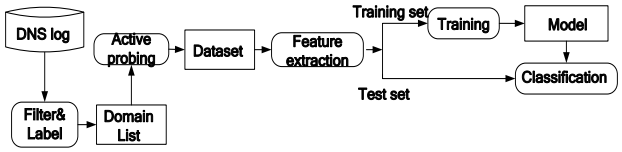


Figure 5. The framework of the CDD method.

Passive DNS logs are used to generate the domain list. An active DNS probe is performed from multiple locations to obtain the resolution records and construct the dataset. Feature vector is further extracted from the samples and the training part split from the whole dataset is fed to the classifier to build the classification model. Finally the model is applied to the test dataset to evaluate the performance.

4. EXPERIMENT PREPARATION

4.1 Domain List Generation and Labeling

Based on the DNS logs from recursive servers, we pick domains with the hostname "www" for that they are very likely to be websites. Considering the fact that about 50% of the popular sites are deployed behind a CDN [17], we select the top 30k domains with "www" prefix sorted by the number of resolution from eight-hour DNS logs of a network service provider as our bootstrap domain list. Then we try to fetch the landing page of each domain to ensure that the site could be accessible. If error occurs or no landing page exists, the domain name will be filtered out. After that, 5320 domain names are discarded.

As our method is based on supervised learning classifier, we need to construct the labeled dataset from the remaining 24680 domains. We use a heuristic approach and a manual check for ground truth classification. For CDNized domain, with the help of previous work, we use IP ranges, name conventions posted publicly by CDNs to identify. Once confirmed, the domain is taken from the list into a CDNized domain list. For non-CDNized domains, we check the domain manually from the remaining domain list. We also use WHOIS information to check the ownership of the domain and IP address. If we feel confused about the class of a domain, it will be put aside to be determined. Eventually we conservatively find out 4200 CDNized domains and 4200 ordinary domains without CDN supported to the next step. Among the non-CDNized domains, there are 2508 website management practices, 1670 web hosting and 22 fast flux. The count of the labeled samples are listed in Table 2.

Table 2. The description of the dataset

Label	Domain Name Count
CDNized domains	4,200
Non-CDNized domains	4,200
Total	8,400

4.2 Dataset Construction

To extract the features for experiment, we actively initiate DNS requests for the 8400 domain names from 33 vantage points lying

in China cities and abroad. It is noted that the recursive server of each vantage points is set up following the recommendation of the local operator. The details of 33 vantage points are depicted in Table 3. We repeat the probing work three times in three separate days. Nearly one hundred DNS records received from different vantage points are gathered and aggregated for each domain name. Subsequently statistical work is done based on the results and features are extracted for the labeled samples, and the construction of the dataset is finished.

Table 3. The description of the vantage points

Location	Details	Number
CHINA	2 operators in 15 provinces: BJ, SH, AH, ZJ, LN, SD,SX, GZ, JS, HA,GX, GD, CQ, XJ, GS	30
ABROAD	the USA, Singapore, Japan	3
Total		**33**

5. EXPERIMENT AND EVALUATION

5.1 Experiment Setting

Python language is used to process data and train models in the experiment. Logistic regression and random forest are two popular supervised machine learning algorithms in the classification field. And logistic regress is widely used in industry as a baseline method. We use the popular scikit-learn machine learning library [18] to implement the detection model.

The configuration of our experiment machine is as follows: a physical server with Windows 10 (64-bit) operation system, Intel i7-10710U CPU and 16G memory.

5.2 Evaluation Metrics

To evaluate the experimental results, four metrics, i.e. precision, recall, F1 score and the area under curve (AUC) value, which are widely used in the classification algorithms are utilized in this paper. As we only have a relative small dataset, standard k-fold cross validation method is adopted to achieve a better error estimate. The final results of the metric are calculated by the average results of multiple cross validation.

In addition, the importance of each input features for the classification are also evaluated in the experiment.

5.3 Experiment Results

5.3.1 Results of Two Classifiers

Table 4. The performance of two classifiers

Classifier	Logistic Regression	Random Forest
Precision	0.9821	0.9643
Recall	0.8579	0.9202
F1	0.9157	0.9417
AUC	0.9565	0.9658
Time/second	0.0625	0.0793

Logistic regression and random forest algorithms are tested in the experiment with 10-fold cross validation using scikit-learn machine learning library. The random forest algorithm uses 10 trees and entropy-based criterion, and the other parameters are set by default. The logistic regression uses liblinear algorithm for optimization.

The values of the performance metrics of the two classifiers are listed in Table 4. It is observed that both classifiers achieved good performance in term of the metrics: the precision, F1 and AUC are all higher than 90%. The precision of the logistic regression classifier is about 0.018 higher than the random forest classifier, but the recall rate of 85.79% is 0.062 lower than the random forest classifier. From the perspective of F1 and AUC, the random forest classifier performs better.

Considering the dimension of the feature vector is small, the consuming time of our method is mainly focused on the training. We recorded the time it takes for two classifiers to train approximately 7500 samples, which is also listed in Table 4. There is not much difference in the time consuming of the two, both are quite small.

5.3.2 Evaluation of the Feature Importance

The feature vector is constructed by features described in section 3 in forms of { N_{IP}, N_{IPC}, N_{AS}, maxATTL,meanATT, meanCTTL, maxCTTL, Sim_{UC},$Diff_{UC}$, N_{hyphen}, N_{dot}, N_{digit}, ATTL , CTTL }. We use a gain-based random forest algorithm to evaluate the importance of the features and depict the result in Figure 6. The values from 1 to 14 in x-axis represent the index of each feature in the feature vector. The value of y-axis demonstrates the importance of each feature.

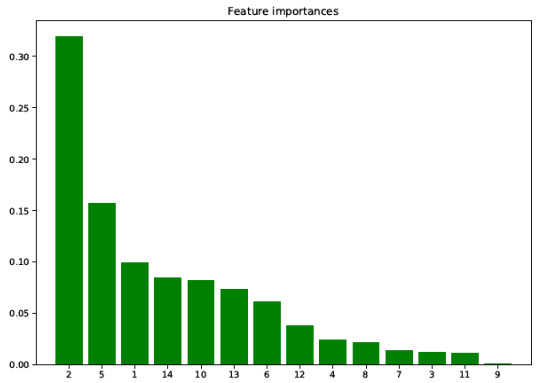


Figure 6. The importance of the features.

From the ranks, we can conclude that the IP related features contribute most to classification, including the number of C-class segments and the number of IPs with the tags of 2 and 1. On the contrary, the number of AS (tagged with 3) has little effect. We guess that AS is a big range for the CDN surrogate cluster, so the number of C-class segments and IPs show good diversity.

Next are the TTL-related features, tagged with 5, 14, 13 and 6. With respect to TTL, we have two findings. The first one is that the average value is better than the maximum value in recognition. We conjecture that compared with the non-CDNized domain names (TTL value is relative large), the difference between the average value is greater than the difference between the maximum value, which makes the average value win. The second finding is that the TTL value of the A record performs better than the TTL value of the CDN entry record in classification. We looked at the data and found that the former was always small while the latter has no such obvious pattern.

In comparison with the other two categories of features, the contribution of the domain-related feature (including 8, 9, 10 ,11 and 12) is the lowest. Only the features of the surrogate name be of help, the influence of the hyphen number, the dot number and the digit number is gradually reduced. We think the reason is that ordinary domain names (especially for small sites) are also named with dots, numbers and hyphens, and their probability decreases in turn. Moreover, the similarity and difference between the user entry and the CDN entry are not as effective as we imagine. The complexity of the actual operation makes the difference in these two features between CDNized domains and non-CDNized domains not obvious enough.

6. CONCLUTION

The CDD method proposed in the paper is an attempt to identify CDNs by using domain resolution records and machine learning algorithms. We studied the DNS-based request routing technique in CDN and extracted three categories of features from DNS records for CDNized domain detection. The classifier performs well in a labeled dataset which is constructed from the active DNS probe results of a domain lists picked from real-world DNS logs. From the results of the feature importance assessment, the IP and TTL related features are found to be more useful.

7. ACKNOWLEDGMENTS

This work is funded by the National Key Research and Development Program of China under grant 2016QY05X1003.

8. REFERENCES

[1] Frank, B., Poese, I., Lin, Y., et al. 2013. Pushing CDN-ISP collaboration to the limit. *J.ACM SIGCOMM Computer Communication Review*. 43, 3 (2013), 34. DOI= https://doi.org/10.1145/2500098.2500103.

[2] Zheng, W., J. Huang, and S. Rose. 2018. Evolution and challenges of DNS-Based CDNs. *J. Digital Communications and Networks*. 4, 4 (2018), 235-243. DOI= https://doi.org/10.1016/j.dcan.2017.07.005.

[3] Cheng, H., Angela, W., et al. 2008. Measuring and evaluating large-scale CDNs. *In Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*. (Greece, October 20 - 22, 2008) ACM, New York, NY, USA, 1–4. DOI= https://doi.org/10.1145/1452520.1455517.

[4] Guo, R., Chen, J.J., Liu, B.J., et al. 2018. Abusing CDNs for fun and profit: Security issues in CDNs' origin validation. *In 2018 IEEE 37th Symposium on Reliable Distributed Systems* (Salvador, Brazil, Oct. 2-5, 2018). Volume 1 (2018), 1-10. DOI= https://doi.org/10.1109/SRDS.2018.00011.

[5] Adhikari, V. K., Guo, Y., Hao, F., et al. 2014. Measurement study of netflix, hulu, and a tale of three cdns. *In IEEE/ACM Transactions on Networking*. 23, 6 (Dec. 2015), 1984-1997. DOI= https://doi.org/10.1109/tnet.2014.2354262.

[6] Bottger, T., Cuadrado, F., Tyson, G., et al. 2018. Open Connect Everywhere: A Glimpse at the Internet Ecosystem Through the Lens of the Netflix CDN. *J.ACM SIGCOMM Computer Communications Review (CCR)*. 48,1 (April 2018), 28-34. DOI= https://doi.org/10.1145/3211852.3211857.

[7] Hohlfeld, O., Rüth, J., Wolsing, K., Zimmermann, T. 2018. Characterizing a Meta-CDN. *In International Conference on Passive and Active Network Measurement 2018. Lecture Notes in Computer Science*. vol 10771 (March 2018), 114-128. Springer, Cham. DOI= http://doi. org/10.1007/978-3-319-76481-8_9.

[8] Xue., J. A., Choffnes, D., Wang, J. 2017. CDNs Meet CN An Empirical Study of CDN Deployments in China. *In IEEE Access*. vol. 5(2017), 5292-5305. DOI= http://doi. org/10.1109/ACCESS.2017.2682190.

[9] Chen, X.X., Li, G.C., Zhang, Y.Z, et al. 2019. A deep learning based fast-flux and CDN domain names recognition method. *In Proceedings of the 2019 2nd International Conference on Information Science and Systems*. Part F1483 (March 2019), 54–59. DOI= https://doi.org/10.1145/3322645.3322679.

[10] Mockapetris, P. 1987. Domain names - implementation and specification. RFC 1035, Nov. 1987.

[11] Callahan, T., Allman, M., Rabinovich, M. 2013. On modern DNS behavior and properties. *J.ACM SIGCOMM Computer Communication Review*. 43,3(2013), 7-12. DOI= https://doi.org/10.1145/2500098.2500100.

[12] NS1. Last accessed on Jan.18, 2020. URL https://ns1.com/resources/understanding-ttl-values-in-dns-records.

[13] Jiaping, P., Hou,Y.T, Bo, L. 2003. An overview of DNS-based server selections in content distribution networks. *J.Computer Networks*. 43,6 (2003), 695–711. DOI= https://doi.org/10.1016/S1389-1286(03)00293-7.

[14] Barbir, A., Cain, B., Nair, R., Spatscheck, O. 2015. Known Content Network (CN) Request-Routing Mechanisms. RFC 3568, Oct. 2015.

[15] Hao, S., Zhang,Y.B.,Wang, H.N. 2018. End-Users Get Maneuvered: Empirical Analysis of Redirection Hijacking in Content Delivery Networks. In 27th USENIX Security Symposium (Baltimore, US, August 15-17, 2018). pp 1129–1145. DOI= https://doi.org/10.5555/3277203.3277287.

[16] Malhotra, A., Toorop, W., Overeinder, B., Dolmans, R., & Goldberg, S. 2019. The Impact of Time on DNS Security. IACR Cryptology ePrint Archive. 788(2019). DOI= https://doi.org/10.1109/Eco-friendly.2014.53.

[17] Builtwith. Content Delivery Network Usage Statistics. Last accessed on Jan.19, 2019. URL. https://trends.builtwith.com/CDN/Content-Delivery-Network.

[18] Pedregosa, G., Varoquaux, A., et al. 2011. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*. Volume12 (2011), 2825–2830. DOI= https://doi.org/10.1524/auto.2011.0951.

Chapter 4

Internet of Things and Mobile Communication Technology

IoT as an Enabler for Successful CSR Practices: The Case of Spanish Firms

Marina Mattera
Universidad Europea
C/Tajo S/N
28670 – Madrid - Spain
+34912115086
marina.mattera@universidadeuropea.es

ABSTRACT
Firms have been increasing their efforts towards sustainable manufacturing and service provision from pollution prevention to integrated approaches. With Internet's expansion, the degree of possibilities has been broadened exponentially. Considering its recent implementation, there is still a lack of understanding regarding the role that technology, specifically Internet of Things (IoT), plays in the implementation of Corporate Social Responsibility (CSR) strategies. The present study provides insights on how firms could leverage on IoT technology to succeed in the implementation of their CSR policies and presents empirical tools being implemented by companies.

CCS Concepts
• Social and professional topics → Sustainability.

Keywords
Business Processes; Internet of Things, Sustainability; Social Responsibility.

1. INTRODUCTION
Technology has been the driver of business strategies, increasing productivity, enabling the standardization of processes, augmenting the number of possible products or services offered, fostering larger communication networks, among many other benefits. This, together with social changes, has greatly impacted in the global economic context over the past centuries, modifying completely the way in which business carry out their activities.

Furthermore, during the 20th century, several studies revealed that at various stages of global supply chain were contributing to the endangerment of the environment, which together with the natural changes in climate, could significantly endanger the continuity of all species. Consequently, firms have rapidly changed their approach, acknowledging their social responsibility. This has led to Corporate Social Responsibility (CSR) strategies.

By conducting CSR actions, firms not only address socio-environmental issues, they also create new business opportunities, and get a better understanding of the market in which they operate. In spite of the fact that technology and firm's acknowledgement of their social responsibility have been the two major elements that changed the way in business is conducted, there is still a lack of understanding regarding technology's impact, specifically IoT, in the implementation of CSR strategies.

The present paper directly tackled this matter through an in-depth study of the 16 most renowned brands in Spain, assessing the role that IoT plays in the fulfillment of their CSR strategies. This will be our contribution. In the following subsections, a literature review will be outlined, followed by a detailed study of the firms and discussion. Finally, conclusions are drawn from the analysis, and future avenues of research are identified.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388177

2. LITERATURE REVIEW
There has been a change evidenced in technology's role in society, from a tangent role in which it would be only a set of tools to carry out tasks, to a more central role. For instance, technology can be in it of itself the basis of the new products and services offered by firms, the overall production process, management systems, and this would lead to becoming the core element of a firm's business model (Haller et al., 2008;O 'Reilly and Battelle, 2009).

Furthermore, it has gained relevance from the moment in which corporations expanded beyond borders and their traditional economic activities. Through this, it has enabled the creation of new industries, new segments, new services and products, and thus companies becoming international operators whose marketplace is not focused in one geographic region or industry, but on a transnational and trans sectorial framework, which continues to expand (Proffitt, 2013).

2.1 Sustainable business models
A business model has been defined as a framework to understand and interrelate customer relations and business processes. Hence, it can be determined how a firm creates goods or services and delivers value to its consumers, correlating (through cost analysis, investment valuation and profits) the use of resources with the how much value is offered to a single consumer with every product or service.

Moreover, Teece (2010) identified that the elements that contribute to value creation, are: (i) choosing technologies and features to be incorporated in the product or service, (ii) determining which are the benefits that the consumer will obtain with the purchase, (iii) identifying the market segments that will be targeted with the product or service offering, (iv) ratify

available revenue streams, and (v) establish mechanisms to capture value. Depending on the business model that the firm adopts, these elements will be combined in different ways.

Considering the profitability of the entity and the adequation of product/service offering, it becomes necessary to consider how the company will derive value in terms of two elements: people and profit. A firm's operations would be obstructed if such company fails to fulfil its major stakeholders' demands. Consequently, there should be an optimal combination of these facts, outlining technology and CSR, in order to have an effective and efficient business model that will lead the firm to economic growth and fulfillment of their social commitment.

However, firms operate in physical contexts and they need to ensure the long-term operations to ensure not only value will be provided to its consumers (and society at large) as well as their investors, but also not over exploiting resources so that they can be used for future operations. Because of the abovementioned, three elements are essential to a sustainable business model: people, profit and planet, or the three Ps.

This is known as the triple bottom line theory where the optimization of these three elements can ensure business success in the long run. It is by including the social and environmental aspects into the elements that firms are able to take these issues into account and have a measurement that portrays the overall performance of the company. Additionally, several authors have found TBL elements necessary to achieve sustainable development and ensure the company's sustainable stream of revenues in the long run (Norman and MacDonald, 2004; Hacking and Guthrie, 2007; Venkatesh, 2010).

Complementary to the influence of technology and TBL in the firm's strategy and business model, Osterwalder (2010) was able to identify the stereotypical elements that are commonly included, regardless of the organization and interaction within the business model. The concepts identified are: infrastructure, including key activities, resources and partner network; offering, comprising quantitative (price and efficiency) and qualitative (client's overall experience and outcome) value propositions; customers (mass and niche markets and segments, together with multi-sided platforms and diversification); channels to deliver products and services; customer relationship (personal assistance, self-service, automated services, communities, co-creations, etc.); and finance (cost structure and revenue streams). This, combined with the five elements identified by Teece (2010) creates the basis for understanding the key aspects of sustainable business model design.

2.2 Internet of Things

As it was previously mentioned, technology plays a significant role in the creation of new products/services, entire industries, improvement of production processes, increasing efficiency in management, among other great advantages. Its advancements currently have a key role in the evolution of business management and particularly in business models' design, especially the Information and Communication Technologies (ICT). Among the most recent innovations in the field of ICT is Internet of Things (IoT), which consists of elements that are interconnected with each other through wireless communications.

IoT **started through** Radio Frequency Identification (RFID) tags as to indicate and identify elements in supply chain management (European Commission, 2009), where the communication between "things" simplified processes. These identification tags were connected to Internet databases that organized and allowed to follow up these objects. After the success of RFID, researchers realized the potential for further applications.

The essence remains the same: establishing links in order for "things" to autonomously connect elements in the physical world events according to a predetermined premise, independently of human intervention (European Commission, 2013). Nowadays several other technologies arose since RFID irrupted in the market, such as QR codes, Bluetooth, UWB or Zigbee. All of these enable the existence of interconnected objects, and consist of specific radiofrequency technologies that permits radio transmission of information between objects (European Commission, 2013).

Consequently, IoT creates a dynamic global network infrastructure through which communication could be standardized and interoperable, adding self-configuring capacities to "things". In this new framework, there are endless possibilities to connect physical and virtual elements by using intelligent interfaces which integrate information (European IoT Council, 2013), and whose objective is to have "things" which actively participate in business, information and social processes, interacting and communicating between each other and with the environment.

This is achieved through data exchange, whether facts each element "knows" or data they "sense" about the environment. Furthermore, IoT allows for elements to react autonomously to physical world events according to a predetermined premise, independently of human intervention (European Commission, 2013).

2.3 Sustainable Business Models and the Impact of Technology

When integrated into the business strategy, it is determined that the firm can implement IoT in many areas of business management, being the main applications logistics, environment monitoring, market research, procurement, customer management (Mattera and Ureña, 2014). In doing so, it is allowing for the creation of new products or services, as well as expanding connectivity and enabling higher effectiveness and efficiency both internally and externally. This implies modifying the firm's interaction with consumers, in the services or products it offers, in their own corporate infrastructure (management, process, production, communication, etc.) and as part of the elements used for maintenance, whether of its internal processes, the production process or other elements that may require it.

It is understood that there will be a revolution in the near and far future as the current IoT available is only a small portion of its true potential (Serbanati et al., 2011), especially in the business area as there will be an increased possibilities in terms of product/service creation, production, delivery, which are currently under research. The real applications, together with the futuristic ones, are only a small part of the true extension of IoT.

Midori Oishi Nemoto et al. (2018) evaluated the perception managers had of IoT and its applicability, in the specific context of Brazil. The authors concluded the new technologies could lead to an improvement in the company's corporate reputation, as well as producing innovative elements that could lead to a competitive advantage.

Considering the possibilities derived from using embedded sensors and actuators in the environment, there could be a significant impact on the way in which CSR is implemented and

businesses are managed in order to effectively consider TBL. However, there is still a lack of evidence regarding how IoT influences firm's CSR and whether there could be an interrelation that contributes to a more efficient business model. The present paper directly tackled this matter through an exploratory study, assessing the role that IoT plays in service sector firms in terms of the fulfillment of their CSR strategies.

3. Spanish Firms Using IoT to Successfully Implement CSR Practices

The present exploratory study assesses the role that IoT plays in the fulfillment and implementation of Spanish service sector firm's CSR strategies. The paper considers the information that each of the 16 companies has disclosed in their Annual Statements, corporate websites, environmental reports and media.

Firms were selected from the service sector as the industries comprised in this sector are largely influenced by stakeholders and therefore should have a higher esteem for their CSR strategy and integrating it into the business model. Furthermore, in some cases such as energy service provision, the environmental impact of their production process deems it necessary to have strong policies and strategies in order to properly manage their operations within TBL framework.

Taking as a standpoint that CSR has a high impact in society at large, it was deemed relevant to consider the firms with highest reputation and brand awareness as they would be the ones with the best performance within TBL criteria. Thus, based on the study contucted by the Foro de Marcas Renombradas Españolas (FMRE), firms with highest brand awareness in the service sector were selected. In order to provide conclusive evidence for firms providing services, firms from a wide variety of economic activities were incorporated.

Consequently, the resulting database consisted of firms in travel services (Renfe and Iberia), entertainment and leisure (Meliá Group, NH), financial services (BSCH, La Caixa, Banco Sabadell, BBVA), retailers (El Corte Inglés), private security (Prosegur), insurance (Mafre), and energy providers (Gras Natural, Unión Fenosa, Iberdrola, Endesa, and Repsol). Table 1 summarizes the information herein analyzed.

All of the companies included in this study have high CSR commitments, participating with international organizations, designing services that are aligned with social and environmental matters (such as clean energy provision, an eco-friendly lodging experience, traveling with low CO2 emissions, etc.). In addition, several implement ISO 26.000, or Global Reporting Initiative.

After evaluating the firms with the highest brand awareness and representing a variety of sectors, it was evaluated the technological development and application of IoT within each of these firms and whether it served as a basis for CSR policies or not. For that purpose, the main IoT technologies that the firm is or has used were analyzed, to contrast whether IoT enables the firm to achieve their objectives in a highly efficient way.

It should be noted that in this context, the improvement of a CSR initiative's efficiency should not only impact the people and planet aspects, but also reduce costs, increase effectiveness and this positively affect profit. Therefore, the TBL is being impacted in full, creating win-win situations for society and the company.

Table 1. CSR implementation through IoT in Spain

Sector	Co.	CSR implementation through IoT Corp. Infrastructure
Airline	Iberia	Internal control systems (acoustics emissions and air quality); Monitoring/reporting of CO2 emissions; Multifunction equipment
Train transportation	Renfe	CO2 Emissions control; Integrated Security Systems; Integrated communication with civil services (police, firemen, etc.)
Hotel	Meliá	Integrated control, communiations and knowledge systems; Energy measurement; Smart buildings
Hotel	NH	Integrated control systems; Energy measurement; Smart buildings; Communication and integrated knowledge systems
Banking	BBVA	Integrated knowledge systems
Banking	Banco Santander	Integrated knowledge systems
Insurance	Mapfre	Integrated knowledge systems
Banking	La Caixa	Integrated knowledge systems
Banking	Sabadell	Integrated knowledge systems
Petrol	Repsol	Integrated knowledge systems
Electric	Endesa	INTEGRIS - Smart Cities
Gas supplier	Gas Natural	Advanced Metering Management and Advanced Metering Infrastructure; PSE 2025 REDES FUTURED
Electric	Iberdrola	Environmental Management Systems; Integrated knowledge systems
Electric	Unión Fenosa	Advanced Metering Management and Advanced Metering Infrastructure; PSE 2025 REDES FUTURED
Warehouse	El Corte Inglés	Integrated Logistics Management
Private security	Prosegur	Integrated System Analysis (Customer interaction and service provision)

4. DISCUSSION

Among the practices and technologies that are being implemented by nearly all the firms herein included, is the development of Smartphone applications. By having a specific application downloaded in their smartphones, customers can access the services provided by any of the abovementioned companies from anywhere and at any time.

In the case of travel services (Renfe and Iberia), entertainment and leisure (Meliá Group, NH) and financial services (BSCH, La Caixa, Banco Sabadell, BBVA), this allows customers to carry out transactions, hire services or modify existing services, without using any paper, which contributes to an environmentally-friendly service provision. In addition, it contributes to a faster service and a more transparent interaction, which increases the consumers' satisfaction and reduces costs in the long run for the firm.

This is true even for the case of travel services or entertainment and leisure, where customers previously had to carry a voucher or other documents which would confirm their transaction and with the mobile app they can have all the information in a single QR code. In the case of issues, they can report them directly from the app, and the firm can track the number of times a particular problem arose in order to develop policies and procedures that will help solve it or entirely avoiding it happening again in the future. This proves IoT simplifies the process, creates a more direct and transparent interaction with consumers and contributes to CSR actions.

Additionally, retailers (El Corte Inglés), airlines (Iberia), private security (Prosegur), insurance (Mafre), and energy providers (Gras Natural, Unión Fenosa, Iberdrola, Endesa, and Repsol), have a steady approach towards environmental protection as well as contributing to the improvement of social welfare. As an example, MAPFRE provides an app that enables people who have hired their insurance services can learn how to make a more efficient use of energy, improve car maintenance, declare any issues they have had (such as an accident with their vehicles), among many other features.

Finally, it should be noted that firms in the service sector are creating collaborations in the advancement of IoT technologies that will enable the achievement of common objectives. Such is the case of Endesa, the Spanish electric company that is playing a significantly important role in the European project INTEGRIS which consists of a telecommunications system, running parallel to the current electric network existent in each city.

This system will allow to have live information regarding distribution of medium and low tension, allowing for a better management of electricity and also opening a new possibility for real-time data exchange. The initiative has been so far been successful in Barcelona (Spain); Brescia (Italy and Tampere (Finland) and it is expected to continue to be implemented in other European cities.

5. CONCLUSIONS

It has herein been detailed that technology is currently integrated into the business management as a set of tools that will enable an increasing level of productivity, standardizing processes, augmenting the number of possible products or services offered, fostering larger communication networks, among many other benefits.

Meanwhile, firms have also been incorporating managerial actions directly tackling their corporate social responsibility, in an attempt to improve the relationship between a corporation and the community, minimizing social and environmental impacts. However, it has been argued that IoT and firm's acknowledgement of their social responsibility have not yet been linked together. Specifically, in terms of understanding regarding the role that technology, specifically IoT plays in the implementation of Corporate Social Responsibility (CSR) strategies.

The results from the present exploratory analysis provide new insights for practitioners, in two main streams. Firstly, by implementing IoT, as it was mentioned before, managers can not only create more effective and efficient work environments but also contribute to CSR actions. This ensures the firm's achievement of CSR objectives and creates synergies between managerial and socio-environmental objectives, with the same resources and efforts.

Secondly, the areas of application of IoT can be larger than initially thought when technical and social objectives are combined. Hence, the possible applications under a unified Business Strategy can range from automatizing processes to community involvement. Figure 3 depicts some of the possible applications if firms were to create a unified Business Strategy that combines IoT and CSR objectives and initiatives.

However, this study has certain limitations that need to be dealt with by future research. Firstly, the present study focuses on a single country (Spain) and a specific sector (service). It would be valuable for a future research to analyze companies from other nations and sectors of activity different from service-oriented companies to test whether it is possible to generalize the results obtained in this manuscript.

Secondly, conceptually and empirically more work is necessary to refine the model designed to portray the relation between IoT and CSR. Lastly, it would be of interest to learn the impact of IoT in improving the people-profit-planet outline considering the lessening of harmful effects, as well as creating positive virtuous cycles.

6. REFERENCES

[1] European Comission (2013) Division of Information Society and Media. Information available in html format at: http://www.iot-visitthefuture.eu/

[2] Hacking, T. and Guthrie, P. (2007) A framework for clarifying the meaning of Triple Bottom- Line, integrated and sustainability assessment; *Environmental Impact Assessment Review*; 28 (2-3), 73-89.

[3] Haller, S.; Karnouskos, S. and Schroth, C. (2008) The Internet of Things in an Enterprise Context, IN Domingue, J.; Fensel, D. and Traverso, P. (Eds.) *Future Internet – First Future Internet Symposium.* Vienna: Springer.

[4] Mattera, M. And Ureña, R. (2014) Internet of things: merging technological advancements with corporate social responsibility. POMS Annual Conference Meeting 2014, May 1-5 Atlanta, USA.

[5] Midori Oishi Nemoto, M. C., Vieira Santos, G. Z. And Contreras Pinochet, L. H. (2018) Adoçao de inovaçao: internet das coisas para melhoria de desempenho de sistentabilidade na Klabin. Revista Gestao & Tecnologia, 18 (1), 197-224.

[6] Norman, W. and MacDonald, C. (2004) Getting to the bottom of "Triple bottom line", *Business Ethics Quarterly*; 14, 2,

[7] O'Reilly, T. and Battelle, J. (2009) Web 2.0 Five Years On. O'Reilly Media Inc. Information available in html format at: http://gossgrove.com/sites/default/files/web2009_websquared-whitepaper.pdf

[8] Osterwalder, A.; Pigneur, Y.; and Smith, A. (Eds.) (2010) *Business Model Generation*. Wiley.

[9] Proffitt, B. (2013) Cisco Hearts Internet of Things, *ReadWrite*, February 14th 2013. Information available in html format at: http://readwrite.com/2013/02/14/cisco-hearts-internet-of-things#awesm=~ojepiFVydclycG

[10] Serbanati, A.; Medaglia, C. M. and Ceipidor, U. B. (2011) Building blocks of the internet of things: State of the Art and Beyond in Ed. Turcu, C. (2011) *Developing RFID Challenges, Solutions and Open Issues*. pp. 351-366.

[11] Teece, D. J. (2010) Business Models, Business Strategy and Innovation. *Long Range Planning*, 43, 172-194.

[12] Venkatesh, G. (2010) Triple Bottom line approach to individual and global sustainability; *Problems of Sustainable Development*; 5 (2), 29-37.

Development of Portable Air Quality Index (AQI) and Emergency Vehicles Preemption Prototype Based on Internet of Mobile Things (IoMT)

Shaik Shabana Anjum
Faculty of Computer Science and Information Technology
University of Malaya
50603 Kuala Lumpur, MALAYSIA
Email: shabana@um.edu.my

Rafidah Md Noor
Faculty of Computer Science and Information Technology
University of Malaya
50603 Kuala Lumpur, MALAYSIA
Email: fidah@um.edu.my

Ismail Ahmedy
Faculty of Computer Science and Information Technology
University of Malaya
50603 Kuala Lumpur, MALAYSIA
Email: ismailahmedy@um.edu.my

Norazlina Binti Khamis
Faculty of Computing and Informatics
Universiti Malaysia Sabah
Kota Kinabalu, Sabah, Malaysia
Email: norazlina@ums.edu.my

Mohammad Hossein Anisi
School of Computer Science and Electronic Engineering
University of Essex
Colchester, United Kingdom
Email: m.anisi@essex.ac.uk

ABSTRACT

The technological advancements of the Internet of Things (IoT) in the recent past have facilitated immense progress towards mitigation of environmental pollution through smart transportation systems and solutions. In particular, communication to the commuters about the traffic ahead or occurrences of congestion has been envisioned to play a major role in outsmarting traffic through mobile applications giving rise to the emergence of the Internet of Mobile Things (IoMT). However, the existing mobile applications that serve as traffic reporting solutions still face major issues such as fixed route suggestions, longer delays during busy hours or emergencies, inefficient prompting of road accidents and heavy traffic en route to a particular destination. This research aims at providing solutions for notifying the commuters with updates on the traffic based upon the Air Quality Index (AQI) of the routes towards the destination and also about the approach of emergency vehicles. The cross-platform mobile application in this way enables the user to opt for a route with good air quality so that the more congested routes are avoided thereby mitigating the air pollution induced by road traffic. The experimental testing and validation of the proposed methodology are applied for areas belonging to Greater Kuala Lumpur. The various timings divided according to peak and non-peak hours are experimentally tested for analyzing the parameters of traffic usage and pattern through the mobile application. The outcome of the experiments has showed that when traffic flow is modelled and governed through vehicular emissions and concentrations of air pollutants, nearly 75% of the congested traffic is reduced thereby, giving rise to pollution-free environment as well as mitigation of urban heat island (UHI) effect that is formed through vehicular heat generation and difference in temperatures. On the other hand, the approach of emergency vehicles also prompts the commuters to avoid panic.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388194

CCS Concepts

• **Hardware→Emerging tools and methodologies.**

Keywords

Air quality index; Air pollution; Road transportation; Internet of Things and traffic congestion.

1. INTRODUCTION

In the past few decades, the population of vehicles has been on higher demand. This huge demand for vehicles results in heavy traffic congestion, accidents, pollution and costs millions of dollars for annual fuel consumption. Such drawbacks have led researchers to look for effective solutions to mitigate vehicular traffic congestion. The vehicular network environment is dynamic in nature due to the frequently changing topologies and network configurations. Though there are numerous existing Intelligent Transportation Systems (ITS) techniques comprising of Internet of Things (IoT) and Vehicular Adhoc Networks (VANETs), which enables the users to keep well-informed and well-updated about smarter ways to deal and handle utilization of transport networks, seldom do they provide guarantee for considering non-recurring congestion as well as means for mitigation of traffic congestion induced air pollution and fuel consumption.

Moreover, the long waiting hours of vehicles at signals and traffic jams leads to higher air pollution levels and heat generated from vehicular exhausts cause Urban Heat Island (UHI) effect. The developing countries like Malaysia, still face potential drawbacks such as increased air pollution levels, due to higher vehicle usage rate resulting in adverse health hazards such as respiratory diseases and asthma. *In this research, the Air Quality Index (AQI) values obtained using the deployment of real-time AQI measuring*

devices, are validated with existing system's values for performance comparison and traffic management.

The proposed cross-platform mobile application is developed on iOS and Android platform at the application layer for timely updates on the AQI values and is also based on the approach of emergency vehicles to the end users. AQI here refers to the numerical value assigned to the level of air quality in the atmosphere. These values are communicated to the commuters tailored to the traffic pollution levels of various routes towards the destination in a timely manner. This concept is based upon an IoT based protocol and is envisioned as an application of the Internet of Mobile Things (IoMT).

Figure 1. Internet of mobile things (IMoT).

The future of smart transportation relies upon the 5G communication as per the IoT researchers and such applications of IoMT would pave a way for the extensive implications of higher mobility, lower latency and spectral efficiency of 5G networks as depicted in Figure 1.

2. LITERATURE REVIEW

In a timespan of the past few decades, vehicular use and population have been tremendously increasing around the world. The usage of a huge number of vehicles cause heavily congested traffic, increased fuel consumption, higher air pollution and the resultant economic hazards [13]. These reasons are the major contributors to global warming. The fast-growing utilization of vehicles gives rise to environmental threats with regards to harmful CO_2 emissions. A study by [5] suggests that emission levels in Malaysia according to CO_2 projections between the years 2000 to 2020 is estimated to increase by 68.86%. This rapid increase in percentage shows that almost 3 billion tons of harmful CO_2 emissions will be released during the year 2020 if no preventive measures are taken for pollution mitigation systems.

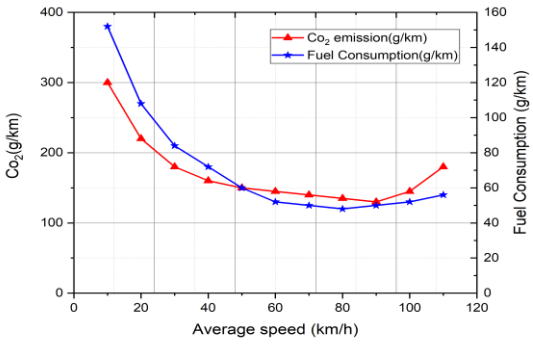


Figure 2. Fuel Consumption vs CO_2.

Over the last years, road traffic congestion and the associated emissions have drawn lots of attention in environmental related research. Based on results contributed by [8] the CO_2 emissions and rate of fuel consumption are directly impacted due to traffic congestion. Therefore, for better solutions to address environmental issues, it is essential to find an optimal relationship between travelling speed of vehicle and rate of fuel consumption along with CO_2 emissions. There is a considerate amount of numerical representations that relate the fuel consumption rate with travelling speed of vehicles and CO_2 emissions in the past few decades.

The representation in Figure 2, depicts such parameters as a function of average travel speed. It clearly shows that there is a 30% average increase in CO_2 emissions and fuel consumption at low average travel speed due to severe vehicular congestion and longer delays at signals (increase in stop-and-drive mode and idle engine extension). Moreover, at relatively higher speeds also there is higher CO_2 emissions and fuel consumption due to the need for more power to the vehicle engine. An average moderate travelling speed that typically ranges from 65 to 85 Km/h produces comparatively lower CO_2 emissions and fuel consumption. Hence, it is essential to mitigate these greenhouse gases and CO_2 emissions by switching towards a fleet that requires lesser stop and drive mode of driving with fewer idle time. Therefore, the solution for effective measures with a reasonable cost for vehicular congestion mitigation and preservation of the environment is essential to reduce the rate of fuel consumption and emission of harmful pollutants [1].

The solution of raising new buildings and highways with higher capacities can be employed to address the above-mentioned issues but can turn out to be cost inefficient, time-consuming and space-limited. Additionally, the research development and innovation on switching towards alternative fuels tend to consume a lot of time and effort to turn to a reality [4,12]. The giant vehicle manufacturers have made significant contributions towards enhancing the design of vehicles and developing the features of cost-effectiveness, environment-friendliness and fuel consumption. The green technology-based solutions have rather given importance to the interior features and technology of the vehicles, for instance, the vehicular companies that focus on research and development to make economical and environment-friendly engines. Few examples of such efforts are fully electric and hybridized vehicles [6,10]. Comparatively, the optimal utilization of the existing streets and roads can mitigate the congestion issue at a reasonable cost in larger metropolitan cities.

Nevertheless, such solutions require exact information about the present status of the streets and roads that turns out to be a challenging risk due to rapid changes in vehicular environments and networks. Intelligent Transportation System (ITS) is defined as a novel emerging platform that combines the electrical technology and network-oriented information with transportation-based technologies [7,11]. This framework covers and addresses a huge variety of methodologies and techniques such as intelligent embedded systems to mitigate the rate of fuel consumption and CO_2 emissions. Such techniques can range from an application-based traffic light signals, traffic routing methodology or even the system for electronic toll collection at highways. These ITS techniques address the mitigation of fuel consumption based on 2 aspects- firstly, to suggest alternate paths with shorter time period rather than shorter distance paths and secondly to mitigate the traffic congestion that maintains optimal vehicle speed [9]. According to [14], the two most promising solutions for

mitigation of CO_2 emissions and fuel consumption rate are – Vehicular traffic routing system (VTRS) and ITS based traffic light signals (ITLS).

Comparatively, the former is considered to be a better solution than the latter due to cost factors and time consumption. Nevertheless, majority of the current VTRS methods have obtained a better outcome for cutting down the travel time or for improved flow of traffic, they can seldom provide assurance for mitigation of fuel consumption, air pollution and noise [2,3]. Therefore, this research aims to develop smart traffic congestion mitigation model based on the values of air quality index (AQI) and prompting of emergency vehicles. This solution is based upon governing the flow of traffic based upon the AQI values, so that the vehicles are routed in the paths with lesser AQI (green paths). The term "green path" here refers to those routes with relatively lesser traffic congestion, reduced fuel consumption and CO_2 emissions.

3. MOBILE APPLICATION FRAMEWORK

The proposed methodology comprises of the data gathering mechanism and distributive path guidance suggestion among vehicles in vehicular networks. These networks are highly dynamic in nature and comprise of unique characteristics such as constrained resource availability and distributed radio channel. They also have issues such as the absence of central coordination, the insecure medium of communication and the hidden terminal problem. The proposed methodology is evaluated in terms of its performance through a cross-platform mobile application called "Go Green Malaysia". The real-time AQI measuring devices are installed in various areas of Greater KL, followed by which extensive simulations run and tests are done to evaluate the proposed approach in comparison to other existing methods. The distinctive scenarios with different sizes of maps, AQI values, vehicular densities, accident and weather conditions are taken into account for comparative analysis between the existing and proposed solutions.

The proposed methodology comprises of an IoT based mobile application and is aimed towards modelling the heavily congested road traffic to mitigate congestion as depicted in Figure 3. The traffic induced air pollution causes the emission of harmful pollutants into the atmosphere ultimately leading to higher AQI. Therefore, prompting the users with notifications of routes having lesser AQI, can considerably mitigate the longer delays, traffic congestion and can also address an increased percentage of harmful emissions into the atmosphere. The parameters for performance evaluation include pollutant emission level, UHI effect and vehicular density ratio.

The comparative analysis with respect to the existing solutions is carried out for the results of performance determination. The application is developed on iOS and Android platforms using Apache Cordova and Ionic framework at the application layer, for timely updates on the AQI. The application shows the different routes with the AQI information wherein the user inputs the current location and destination address as shown in Figure 4, after which the selection of route with lesser AQI is chosen for the commuter to reach the destination through less congested route and also the approach of emergency vehicle, as depicted in Figure 5, ultimately resulting in balance of air pollution levels and mitigation of traffic-induced pollution. The experimental validation and analysis of the proposed methodology are carried out for different areas of greater KL, in Malaysia as part of the extension of the research presented in [15,16]. The various timings of the day (morning, afternoon and evening) are monitored for evaluation and explored for the usage of traffic parameter based on the mobile application.

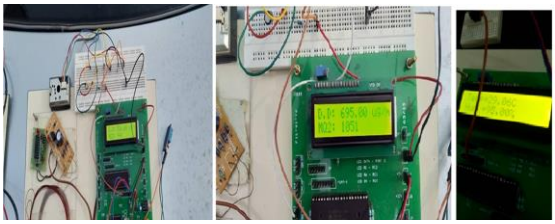


Figure 3. The proposed proof-of-concept (POC) for monitoring of air quality.

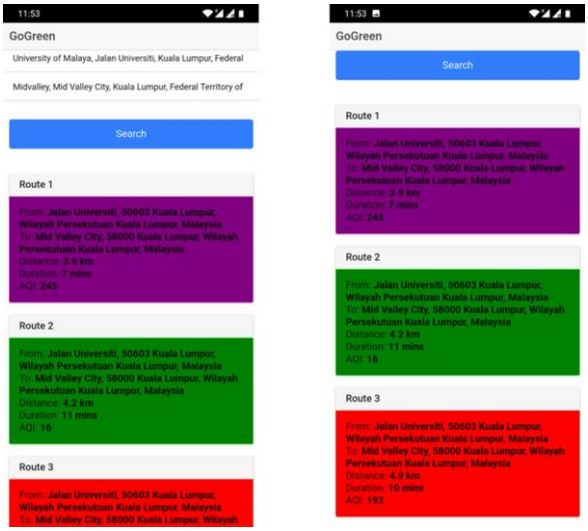


Figure 4. Screenshot of the proposed mobile application showing the route suggestions.

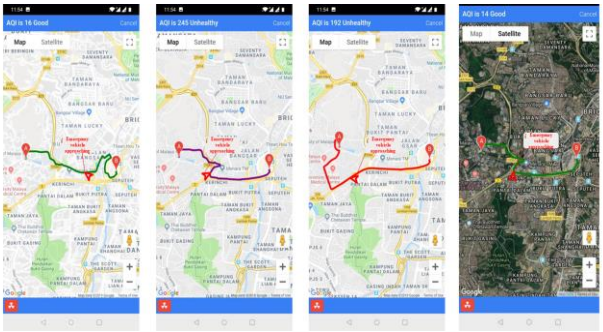


Figure 5. The proposed mobile application showing AQI of the routes with the approach of emergency vehicles.

4. CONCLUSION

The correlation between pollutant emission, the flow of traffic and dispersion of harmful gases into the atmosphere determines the quality of air and enables a broader scope for designing the traffic management methodologies for urban road networks. The proposed methodology has determined that modelling the flow of road traffic based on AQI has consequently mitigated the air pollution level. It can be said that whenever, the traffic flow and vehicular emission are integrated together, the rate of harmful

emissions are estimated to be better for ensuring good air quality of urban transportation. The development of proposed methodology has revealed that the major contributions of air quality are – traffic flow, speed/acceleration of vehicles, vehicular density, an average waiting period of vehicles at junctions/intersections, type of air pollutant and frequency of stop and drive mode in vehicles. The results are experimentally analyzed and quantified for various urban road networks and traffic management scenarios. The experiments have provided an essential perspective for enabling pollutant free atmosphere and also to mitigate the traffic congestion. The proposed traffic-induced air pollution mitigation mechanism proves that nearly three-fourths of the emissions into the atmosphere can be alleviated by reducing the heavy congestion due to long delays and heavier densities of vehicles. The preemption of emergency vehicles on one hand, can save human lives through faster transportation (such as for ambulances) and on the other hand, can alleviate panic caused to the on-road commuters as well.

The future work is focused upon improvising the mobile application for bugs identified and also to include the notifications about the places of interest as per recommendation systems for the route suggestions provided to the user.

5. ACKNOWLEDGMENTS

The authors would like to thank the University of Malaya Post-Doctoral Research Fellowship scheme and University Malaysia Sabah research grant under grant number SDN0062-2019 for the required support provided to carry out this research. The authors would also like to extend their thankful regards to the anonymous reviewers for providing constructive suggestions that aided in improvisation of this manuscript.

6. REFERENCES

[1] Ahmed, M. et al. (2013) Vehicle Adhoc Sensor Network Framework to Provide Green Communication for Urban Operation Rescue, Lecture Notes on Information Theory, 1(2), pp. 7782. DOI: 10.12720/lnit.1.1.77-82

[2] Akcelk, R., Smit, R. and Besley, M. (2012) Calibrating Fuel Consumption and Emission Models for Modern Vehicles, IPENZ Transportation Group Conference. DOI:261363189

[3] Bakhouya, M., Gaber, J. and Lorenz, P. (2011) An adaptive approach for information dissemination in Vehicular Ad hoc Networks, Journal of Network and Computer Applications. Elsevier,34(6), pp. 19711978. doi: 10.1016/j.jnca.2011.06.010.

[4] Barth, A. and Boriboonsomsin, M. (2009) Traffic Congestion and Greenhouse Gases, Access Magazine, 35. Available at: http://www.accessmagazine.org/fall-2009/traffic-congestion-greenhouse-gases/

[5] Demestichas, K. et al. (2011) Intelligent Advanced Driver Assistance System for Electric Vehicles, 2011 IEEE Intelligent Vehicles Symposium (IV), (Iv), pp. 7882. doi:10.1109/IVS.2011.5940409.

[6] Dimitrakopoulos, G. and Demestichas, P. (2010) Intelligent Transportation Systems, IEEE Vehicular Technology Magazine, 5(March 2010), pp. 7784. doi: 10.1109/MVT.2009.935537.

[7] Frey, H. C. et al. (2003) On-road measurement of vehicle tailpipe emissions using a portable instrument, Journal of the Air and Waste Management Association, 53(8), pp. 9921002. doi:10.1080/10473289.2003.10466245.

[8] Jabbarpour, M. R. et al. (2014) Cross-layer congestion control model for urban vehicular environments, Journal of Network and Computer Applications, 44, pp. 116. doi: 10.1016/j.jnca.2014.05.002.

[9] Jianmin Jiang; James Charles; Konstantinos Demestichas (2011) Toward Cooperative and Intelligent Optimization of Travel Planning and Energy Saving for Drivers of Fully Electric Vehicles, (SEPTEMBER), pp. 2226. doi: 10.1109/MVT.2011.941900

[10] Martinez, F.J., Fogue, M., Toh, C.K. et al. (2013) Computer Simulations of VANETs Using Realistic City Topologies Wireless Pers Commun, 69: 639. https://doi.org/10.1007/s11277-012-0594-6

[11] Van Mierlo, J. et al. (2004) Environmental rating of vehicles with different alternative fuels and drive trains: A comparison of two approaches, Transportation Research Part D: Transport and Environment, 9(5), pp. 387399. https://doi.org/10.1016/j.trd.2004.08.005

[12] Narzt, W. et al. (2010) Self-organizing congestion evasion strategies using ant-based pheromones, IET Intelligent Transport Systems, 4(1), pp. 93102. doi: 10.1049/iet-its.2009.0022.

[13] Papadimitratos, P. et al. (2009) Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation, IEEE Communications Magazine, (November), pp. 8495. doi: 10.1109/MCOM.2009.5307471.

[14] Salvi, B. L., Subramanian, K. A. and Panwar, N. L. (2013) Alternative fuels for transportation vehicles: A technical review, Renewable and Sustainable Energy Reviews. Elsevier, 25, pp.404419. https://doi.org/10.1016/j.rser.2013.04.017

[15] Schrank, D., Eisele, B. and Lomax, T. (2012) TTI s 2012 Urban Mobility Report Powered by INRIX Traffic Data TTI s 2012 Urban Mobility Report Powered by INRIX Traffic Data, Report, Texas A&M Transportation Institute. The Texas A&M University System, (December). Acc. no. 01579161

[16] Anjum, S. S., Noor, R. M., Aghamohammadi, N., Ahmedy, I., Kiah, M. L. M., Hussin, N., Qureshi, M. A. (2019). Modeling Traffic Congestion Based on Air Quality for Greener Environment: An Empirical Study. IEEE Access, 7, 1–24. https://doi.org/10.1109/ACCESS.2019.2914672.

[17] Shaik Shabana Anjum, Rafidah Md Noor, Ismail Ahmedy, Mohammad Hossein Anisi, Nasrin Aghamohammadi, Norazlina Binti Khamis and Muhammad Ahsan Qureshi, "Performance evaluation of energy-autonomous sensors for air quality monitoring in Internet of Vehicles", 1st International Workshop on Internet of Autonomous Vehicles (INAVEC) held in conjunction with IEEE 89th Vehicular technology Conference, 28 April- 1 May 2019, Kuala Lumpur, Malaysia. DOI: 10.1109/VTCSpring.2019.8746496.

A Novel Optimized Design of Energy Efficient Lights for Producing Uniform Illumination by Harnessing Photoluminescent Properties of 'Strontium Aluminate'

Vijay A. Kanade
Senior Patent Associate, Intellectual Property Research,
Pune, Maharashtra, India
kanade.science@gmail.com

ABSTRACT

Electrical energy consumed worldwide today amounts to about 22,500 terawatt-hour (TWh). A larger chunk of this electrical energy is used to produce light energy. Excessive production of light energy (termed as 'light pollution') causes a disturbance in the natural environment that living beings live in. The very light energy when produced above a threshold poses certain drawbacks such as disrupting ecosystems, in particular affecting nocturnal wildlife, adverse health effects such as sleep disorders, increased headaches, etc. Hence, there seems to be a stronger need for developing a substitute for electrical form energy used for producing light energy. The research proposal discloses a portable lighting device that harnesses the properties of photoluminescent pigment 'Strontium Aluminate' for producing light energy by utilizing a free source of energy**.** The lighting device uses a portion of 'Strontium aluminate' mixed with freely available 'water' resource to produce light energy in the presence of black light.

CCS Concepts

• Applied computing→Physics.

Keywords

Photoluminescent Properties; Strontium Aluminate; Black Light; Energy Efficient Lighting; Portable Lighting Device; Light Pollution.

1. INTRODUCTION

Lighting forms a major source of electricity consumption on the planet earth. According to a global survey on lighting uses and costs by the International Energy Agency (IEA), about 19% of the global electricity generation is sucked up for lighting. The very percentage is more than what is produced by hydro or nuclear stations, and equivalent to what's produced from natural gas [1].

The electricity generation produces carbon dioxide which equals to 70% of the global CO_2 emissions from passenger vehicles. According the reports, this is three times more than the emissions coming from the aviation sector.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388198

Further, the incandescent bulbs, which were developed a century and a quarter ago by eminent scientists such as T.Edison, J. Swan are still used around the globe in households. The light energy produced by these bulbs amounts to almost half of the light used in homes worldwide. However, it has been experimentally validated that the incandescent bulbs do not seem that efficient, as they only convert about 5% of the energy they receive into light energy.

The bigger player occupying the market is the fluorescent tubes. It has been observed that the corporate building, commercial and public sector buildings use about 43% of the electrical power for lighting purposes. It is noted that such vibrant buildings are fluorescent-centric. Further, the study also points at the fact that the performance efficiency of the tubes varies greatly in the range of 15-60%.

It is further observed that such commonly used electric lighting systems are ranked lowest in terms of efficiency. In addition, these systems develop a by-product in the form of heat which is distributed in the living spaces. Thus, the developed heat energy further needs additional air-conditioning systems for its removal [1].

Another important aspect with respect to lighting is that a significant proportion of the world's population on the planet has no access to electric lighting at all. If we narrow it down to countries, then even today in India 60-70% population lives in rural areas, where there is no sufficient supply of electricity and thus the population is not in a position to avail the benefits of electric lighting. Therefore, the rural population has sorted out an alternative to this and they rely on burning fuel, etc. Such source of energy is expensive, inefficient, produces poor light quality and also contributes to respiratory disease.

Hence, there seems to be a need for an alternative to electric lighting systems that is accessible to all the living beings on this planet. The research proposal discloses a novel solution to the above-discussed problem by providing energy efficient lights that act as an apt substitute for electric lighting system.

2. LUMINESCENCE PRINCIPLE

Luminescence is a phenomenon that results from spontaneous emission of light by a substance that is not heated. It elaborates a type of 'cold-body radiation'. The effect of luminescence can be caused by chemical reactions between substances, electrical energy, subatomic vibrational motion or crystals under stress. This differentiates luminescence from incandescence, wherein incandescence is observed when light is emitted by a substance as a consequence of heating.

2.1 Luminescent Pigments

Luminescent pigments are often termed as glow in the dark powder(s) or phosphor(s). These pigments give the substance ability to self-glow in the dark environment after sufficiently exposing them to natural or artificial light. Such pigments do not mix and dissolve in medium but in fact make suspension in the medium. The stability of the suspension depends on pigment's particle size and medium viscosity.

Luminescent pigments can be charged in natural daylight or artificial light. Unlike UV pigments, luminescent pigments do not need constant light to work. Once the pigments are charged, they can self-glow up to approximately 12 hours or longer. Another important aspect of these pigments is that the pigments can be charged and allowed to glow innumerably. Therefore, the glowing cycle of 'charging > glowing > charging' can be repeated countlessly without significant reduction of luminescence properties.

Strontium aluminate is one of the potent 'glow in the dark pigment'- a phosphor that offers about 10 times better glowing power compared to older generation of pigments that were essentially based on sulphures [6].

2.2 Strontium Aluminate (SrAl2O4)

Photoluminescent strontium aluminate (pigment) is a new type of phosphor which is ecological alkaline earth aluminate. It has non-radioactive properties and therefore is non-toxic by nature. $SrAl_2O_4$ pigment particles are charged (excited) instantaneously by any light spectrum that ranges in visible light region or ultraviolet light region. Post charging, the photo luminescent pigment releases energy in the form of visible light (i.e. glowing in the dark ambience) for a substantial period of about 24 hours, depending on the type of color. $SrAl_2O_4$ pigments provide a duty-cycle operation with high ratio of glow time to required charging time. The luminosity of the pigment and after-glow time of the pigment material is 30 times stronger than the conventional Zinc Sulfide (ZnS) that is commonly distributed in retail store products.

Strontium aluminate is stable compound with a larger lifespan of about >15 years. It has been observed that even after the active lifespan of 15 years, the pigment continues to glow – however, the glowing power may drop to an extent wherein the pigment may no longer be considered as new. Yet, the reduction in glow is not that significant enough in natural scenarios. The amount of glow depends largely on how we use the pigment with a solvent or medium.

Further, Strontium aluminate is unstable in water as it readily hydrolyzes and thus this result in decrease or complete obliteration of its luminescent properties. However, a lot of research has gone into encapsulating strontium aluminate phosphor to enhance water resistance and luminescence [2]. Silica or sol-gel encapsulation is carried out in order to make the pigment particles water stable while preserving their luminescent properties by using Stober process [3].

3. PROPOSED PORTABLE LIGHTING DEVICE

The proposed portable lighting device consists of three important components: water, encapsulated strontium aluminate and black light. 1/3rd portion of the device holds the black light lamp which is turned on while using the device. The black light emits UV light, which is invisible to human eye, since the visual apparatus of humans can perceive light only from the visible region of the light spectrum. Remaining portion of the lighting device is water storage space, wherein encapsulated strontium aluminate phosphor particles are suspended in water.

The device has a panel for pouring in water of the required amount in such a manner that the water can be refilled and changed with time. Further, the disclosed lighting device can be charged during day time by placing the device in sunlight during the day. This allows the device to run its course for about 24 hours. Thus, the device can be used during night time as the phosphor particles are sufficiently charged during the day time. Therefore, device allows reuse by refilling the water and recharging the phosphor particles in real time based on the usage of the device.

3.1 Working

Water is poured in the water storage space (i.e. remaining portion of the device apart from black light region) of the portable lighting device. Encapsulated strontium aluminate is added to the water as per requirement (i.e. depending on the required illumination). Once the phosphor particles are added, black light is turned on in order to produce maximum luminescence. Black light emits UV light. This UV light further hits the strontium aluminate phosphor and excites the electrons in its outermost shell. These electrons remain in the excited state as long as they receive UV light from the black light that energizes them. However, as the light energizing them is cut off, the electrons return to their original lower orbits. While doing so, they give off energy that excited them in the form of visible light. Hence, the observed bright luminescence around the lighting device is a consequence of UV light energy. Therefore, the strontium aluminate phosphor converts the energy in the UV radiation into visible light.

$$SrAl_2O_4 + H_2O \xrightarrow{\text{(black light)}} SrAl_2O_4 \text{ (Photoluminescent glow)}$$

[Suspended particles in water]

[50-100 lumens]

[Chemical reaction]

[Note: Water is used as a medium that provides homogenous distribution of the strontium aluminate powder and therefore produces appropriate brightness depending on the type of application.]

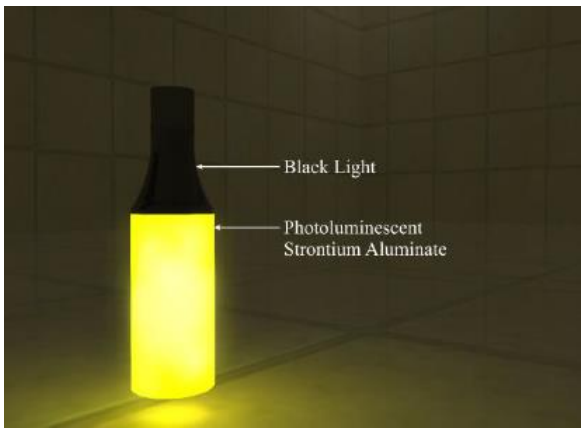


Figure 1. Portable lighting device with photoluminescent properties.

Fig. 1 above discloses the optimized design of the proposed 'Energy Efficient Light' (i.e. Portable Lighting Device) that

produces uniform illumination by harnessing the photoluminescent properties of 'Strontium Aluminate' in the presence of 'Black Light'.

4. EXPERIMENTAL DATA

The experimental data dealing with the usage of strontium aluminate in an application of 'Traffic paint pavement marking' is appropriately discussed by Riches Bacero et.al. [9]. We observed that the collected data elaborates the operational mechanics of strontium aluminate. Therefore, this well-established knowledge and understanding of strontium aluminate, validates our proposition of the 'portable lighting device'.

The data relevant to our research proposal is as tabulated below. The table shows the experimental data collected for the luminance produced by strontium aluminate during the period of September to early of October [9]. Here, sunlight is measured by using the lux meter. The tabulated data discloses four parameters:

- Charging time (15, 30 & 60 minutes) for Strontium Aluminate by exposure to sunlight
- % of Strontium Aluminate
- Lux received (i.e. Amount of sunlight received from the Sun)
- Total luminance produced by Strontium Aluminate after being sufficiently charged [9].

Table 1. Charging time for $SrAl_2O_4$, percent of strontium aluminate, average lux received, and total luminance produced by $SrAl_2O_4$ [9]

Charging Time	% $SrAl_2O_4$	Lux Received (Sunlight)	Total Luminance
15 minutes	15	1139.133	4.9380
	30	1201.667	6.2153
	45	1070.633	8.5736
	60	1036.7	12.6905
	75	1144.733	17.1269
30 minutes	15	827.533	42.1189
	30	788.867	52.7172
	45	771.933	66.8636
	60	800.433	87.5817
	75	792.767	121.1343
60 minutes	15	747.35	380.6322
	30	806.8	616.0843
	45	776.75	914.0636
	60	706.3	1471.9894
	75	701.5	2184.6070

From the above data, it is quite evident that 'Strontium Aluminate' produces sufficient luminance in limited charging time (15, 30 & 60 minutes). Hence, by charging it for a longer duration of time, $SrAl_2O_4$ would produce much greater luminance. Further, it is important to note that such intense luminance is produced merely by charging the strontium aluminate phosphor particles in day light, which is the most natural form of energy.

5. OBSERVATION & RESULTS

The observational data from the literature-surveyed show that encapsulated $SrAl_2O_4$ phosphors can be suspended in water for a period of about 2 weeks without any consequential loss of luminescent properties. As per the prior art literature, Stober process employed for silica encapsulation hydrolytically degrades the phosphors, thereby hampering the luminescent properties of the pigment particles. However, as per the observed results, the encapsulated phosphors do not experience any hydrolytic degradation, although the encapsulated pigment particles are left suspended in water for more than a month [3].

Therefore, based on the above validated results we propose the portable lighting device that could be used in rural areas or areas that lack electricity lighting supply.

The dimensions of the proposed portable lighting device with mini black light are as follows:

- Capacity of lighting device: Approx. 17oz+ water
- Diameter: Base = 2.8in, Lid = 1.4in (top region of black light portion) [in=inch]
- Height = 10.1in, [in=inch]

The structural dimensions of the proposed portable lighting device having a mini black light are as disclosed in the Fig. 2 below.

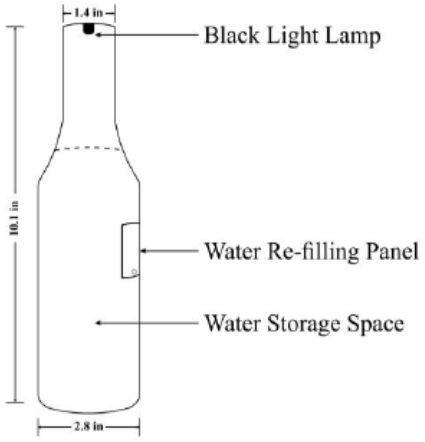


Figure 2. Dimension of proposed portable lighting device.

Further, the standard recommended lumen chart (i.e. luminosity) for various application areas are disclosed in the below table along with the lumen for the proposed lighting device.

Table 2. Lumen chart for various electric lighting systems [4], [5].

Sr. No.	**Light Application / Area**	**Recommended Lumens**
1	Reading	450 lumens
2	Sitting room or Bedroom	10 to 20 lumens per square foot
3	Bathroom or Kitchen	70 to 80 lumens per square foot
4	Security Floodlights	700-1300 lumens
5	Shed Lights	150-300 lumens
6	Lamp Posts	120-180 lumens
7	Landscape Spotlights	120 lumens
8	Outdoor Path Lighting	100 lumens
9	**Proposed Portable Lighting Device**	**50-100 lumens (expected)**

Hence, based on the values tabulated above, we believe that by utilizing a set of portable lighting devices within the household, it could serve the purpose previously served by electric lighting systems. As disclosed, one portable lighting device could offer 50-100 lumens of light producing capacity (i.e. based on the discussed photoluminescent properties of $SrAl_2O_4$), therefore if 'n' number of such portable lighting devices are used within a room or household then the luminosity offered by all the lighting devices could cumulatively sum up to yield significant lumens numerically. This could serve the purpose of a consumer, as the consumer could add or cut down on number of devices to produce bright luminescence based on the requirement. The portable lighting device thus adds flexibility in usage at the consumer end.

The proposed portable lighting device is cost efficient alternative to electric lighting system as once the device is purchased, it could be used for a substantially long period of about >15 years – due to the luminescent properties of strontium aluminate phosphor, which is the basic ingredient of the lighting device . The overall cost of the lighting device designed for the consumer based on the ingredients / components used in the operation of the device is as given below:

- **Component -I**: Water – freely available
- **Component-II**: Encapsulated strontium aluminate phosphor – Range [$5 - $50] / [50grams – 1 kilogram] [7].
- **Component-III**: Black light – Range [$5 - $15] / Black light [8].
- **Component-IV**: Solar energy for charging the lighting device – free source of energy

6. APPLICATIONS

The proposed portable lighting device has following application areas:

- Corporate buildings
- Commercial and public sector buildings such as shopping malls
- Street lighting – as streetlights can be charged during the day through natural sunlight and can be turned on during nighttime.
- Household areas – In living room for reading purposes, in bathrooms, etc.

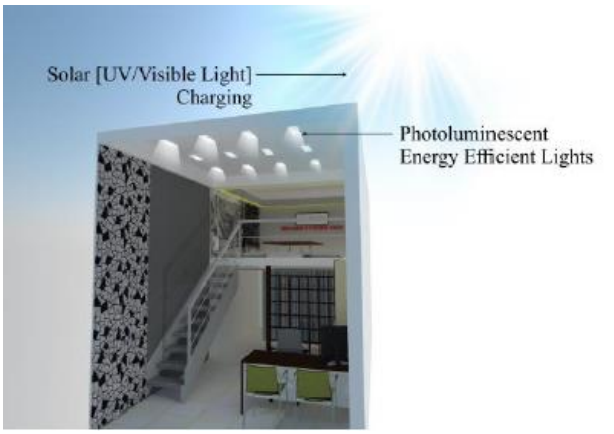


Figure 3. Proposed operational energy efficient lights in a corporate office.

Fig. 3 above illustrates the energy efficient lights that are operational in the corporate office.

7. CONCLUSION

The proposed portable lighting device discloses energy efficient lighting solution for electric lighting systems by harnessing photoluminescent properties of 'strontium aluminate phosphor'. The lighting device is reusable as the phosphor pigments can be charged by using freely available solar energy (i.e. visible or UV light energy). Further, the disclosed lighting device is long lasting as the lifespan of $SrAl_2O_4$ is more than 15 years. In addition, the device permits refilling mechanism, wherein water can be changed or refilled any number of times depending on the usage of the device. Hence, the device can be cycled, run and reused countless number of times.

8. ACKNOWLEDGMENTS

I would like to extend my sincere gratitude to Dr. A. S. Kanade for his relentless support during my research work.

9. REFERENCES

[1] Richard Black**,** "Lighting the key to energy saving", http://news.bbc.co.uk/2/hi/science/nature/5128478.stm.

[2] Yong Zhu, et. al., "Encapsulation of strontium aluminate phosphors to enhance water resistance and luminescence" Applied Surface Science, June, 2009.

[3] Richard Willson, et. al., "Phosphorescent reporters", US20150105284A1, April 16, 2015.

[4] "How to choose a lightbulb - the complete guide", Jan 23, 2018, https://www.pooky.com/inspiration/all-about-lighting/how-to-choose-a-lightbulb-the-complete-guide.

[5] "How Many Lumens Do You Need for Outdoor Lighting?", Solar Outdoor Lighting, November 30, 2015.

[6] "Luminescent pigment S-ZZS380", https://chaostrade.eu/en/luminescent-pigment-S-ZZS380.

[7] Price of strontium aluminate, https://www.alibaba.com/showroom/price-of-strontium-aluminate.html

[8] Handheld UV black lights, https://www.amazon.in/Handheld-Black-Light-Portable-Blacklight/dp/B00EPNW8P8

[9] Riches Bacero et. al., "Evaluation of Strontium Aluminate in Traffic Paint Pavement Markings for Rural and Unilluminated Roads", Journal of the Eastern Asia Society for Transportation Studies, Vol. 11, 2015.

A Verification Method for Security and Safety of IoT Applications Through DSM Language and Lustre

Wentao Tang
Graduate School of Information Science and Electrical Engineering, Kyushu University
tou@f.ait.kyushu-u.ac.jp

Hao Feng
Graduate School of Information Science and Electrical Engineering, Kyushu University
hustfenghao@gmail.com

Kenji Hisazumi
Faculty of Information Science and Electrical Engineering, Kyushu University
nel@f.ait.kyushu-u.ac.jp

Akira Fukuda
Faculty of Information Science and Electrical Engineering, Kyushu University
fukuda@f.ait.kyushu-u.ac.jp

ABSTRACT
Development of Internet of Things (IoT) brings a variety of IoT applications that involve housing, navigation, payment, and healthcare. Since IoT applications play an important role in our lives, security is critical to these applications and must be guaranteed. In order to realize this, the paper proposes a pre-execution verification method for downloaded IoT applications, which meets security and safety requirements of users using model checking. The model checking requires special models for verification, which is difficult to describe for developers. So we introduce a domain-specific modeling language (DSML) to describe IoT application and a generator from the DSML into the model to pre-execution verification and execution. Also, as a case study, we provide a study of our method used in a smart house application, which is one of the most representative examples in IoT applications.

CCS Concepts
• Security and privacy→Domain-specific security and privacy architectures.

Keywords
IoT; DSML; Model-Checking; Code Generating; Lustre; Smart House.

1. INTRODUCTION
At present, the use of Internet of Things is becoming more and more popular. IoT is a communication paradigm, in which the objects of everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet [1].

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388211

With the development of Internet of Things, IoT applications have widely penetrated various areas. Thousands of devices are connected together through the Internet to enable real-time data exchange for IoT applications. While the Internet of Things brings convenience, it also brings many security risks, such as network attacks and malicious applications.

Smart House is a representative manifestation under the development of IoT. Through the technology of IoT, Smart House connects various devices in the home, such as lights, air conditioning, camera, to provide services of lighting control, temperature adjustment, security system, and so on. Usually, there are more than ten devices in one Smart House, which contain plenty of personal information and exist everywhere in the house. When a malicious application is downloaded to the device, there will be risks that personal data is leaked and tampered with. Even devices may be controlled by the malicious application, which may pose a threat to the users' safety.

On the other hand, Model-based design has been advocated as a choice for achieving high quality and guaranteeing properties at a lower cost [2]. Model-based design means that models play an important role in the process of design, which includes building models, checking and assessing the required system properties on the built model, and then deriving the implementation to preserve these properties.

To reduce the risks posed by malicious IoT applications, we hope to provide a method with the help of model-based design to check the IoT application downloaded from the Internet and ensure that it meets our requirements when it runs.

In this paper, we will introduce our method of using DSML to build models for IoT applications and using dataflow programming language Lustre for model checking to ensure the security of IoT applications through a case study of Smart House.

2. BACKGROUND
2.1 Domain-Specific Modeling Language
Model-Driven Engineering (MDE) emerged to allow the development of applications based on the definition of models closer to the problem domain than to the implementation domain. It is usually to use Domain-Specific Modeling Language (DSML) for development to simplify the problem domain and develop on different platforms.

DSML is usually designed with a specific purpose and used to formalize the application structure, behavior, and requirements within particular domains, which allows users to work directly with domain concepts [3]. As graphical diagrams are believed to be more effective than in the communication between end-users or domain practitioners, models used by DSML usually based on graphical representation and are supported by graphical design tools [4].

2.2 Lustre

Lustre based on the synchronous dataflow model, is designed for the description and verification of real-time systems and now in use in many major companies developing embedded software like avionics, transportation, and energy [5]. Lustre program is used to describe the relations between the outputs and inputs of a system by using operators, auxiliary variables, and constants. Each description written in Lustre is built up of a network of nodes that correspond to the functions of the system and allow complex networks to be built by passing parameters [6]. Any variable and expression in Lustre denote a flow, which means a pair made of a possibly infinite sequence of values as well as a clock representing a suite of graduations. As the Lustre formalism is very similar to temporal logics, it can be used to both write programs and express program properties, which results in an original program verification methodology [7]. For verification, using Lustre can not only check the correctness of the program but also check whether the execution order meets users' need or not.

2.3 Middleware

Middleware is a type of software between devices and applications and a key technology to develop IoT applications effectively and safely. In order to achieve resource sharing and system controlling, middleware uses the basic services provided by the device system to connect applications with each other [8]. Besides, middleware provides a high-level interface, which masks the complexity of protocols, and makes it easier for software developers to implement communication and input and output, so they can focus on application-specific issues, where they are most qualified to add value [9]. For IoT middleware, it must be available in the cloud as well as on the edge for supporting all types of IoT applications, better privacy control, and latency.

3. RELATED WORKS

At present, there is three main existing open-source middleware for IoT smart house application: Kaa, openHAB, and Node-red. Also, openHAB and Node-red use DSML.

3.1 Kaa

Kaa is an open-source platform designed for building end-to-end IoT solutions and is administered by KaaIoT Technologies and Cybervision Inc. It is an Apache-based platform that uses a web page graphical UI for data delivery schema creation, endpoint SDK generation, and provides support for multi-tenancy on servers [10]. Kaa can connect and manage IoT devices via the cloud using graphical or REST API and provide varieties of security methods for Kaa communication with devices.

However, data collected from IoT devices by Kaa is stored directly on cloud servers without any processing, which may lead to some security risks.

3.2 OpenHAB

OpenHAB represents a technology agnostic open source automation middleware used DSML for a smart home. OpenHAB is a local system that runs as the center of the smart home on local hardware with a graphical UI dashboard. With the graphical UI dashboard, users can view data collected by sensors and control their devices.

However, the security of openHAB is currently undefined, which means an adversary does not need to explore too much before finding out an apparent vulnerability: the lack of authentication, and therefore, absence of access control [11]. What's more, openHAB also does nothing with data processing.

3.3 Node-RED

Node-RED is a Flow-based programming tool for wiring together hardware devices, APIs, and online services using DSML. Node-RED provides a browser-based flow editor that makes it easy for users to wire devices together and deploy them to the runtime. The security method of Node-RED is Bcryptjs and AES.

However, Node-RED has only a small amount of ready-to-use data processing functions, so that users must thing about the functions connection order and input the code themselves when they need to process data.

3.4 Development Demand

Through the analysis of the above three mainstream open-source IoT middleware for a smart house, we hope to develop an IoT middleware system using DSML to guarantee the security of IoT applications developed by this middleware and also protect the privacy of users. After that, considering that Lustre is convenient for checking, we hope to express the developed applications in Lustre for verification. The system should have the following characteristics:

- Support for building models of applications with graphical UI
- Code generating function
- Varieties privacy and security data processing functions.
- Compatible with as many IoT applications as possible
- Easy to use

4. PROPOSED METHOD

We present an overview of our method in Figure 1.

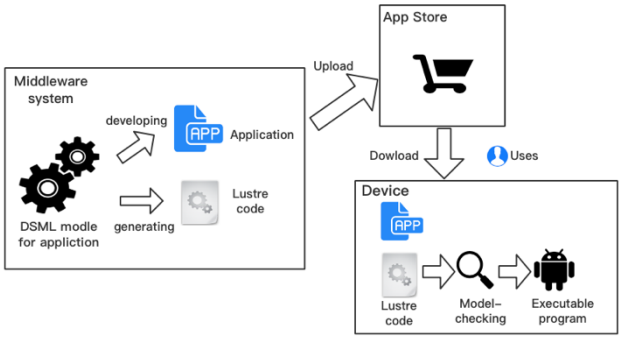


Figure 1. Overview of our method.

First, to develop applications that not only meet user demand but also meet development easily, we develop middleware to build a model of applications. After that, we use the middleware to generate Lustre code from the DSML model of an application that was built before. The generated Lustre code meets all our requirements for the application and can be easily checked. Then

the Lustre code will be packaged in the application as the actual execution part of the application and be uploaded to the App Store.

After the application containing the Lustre part is uploaded to the App Store, users can download the corresponding application to their devices according to their own needs.

Before the downloaded application is executed, a model-checking on the security of the Lustre part will be done to ensure that it can meet the needs of the user without posing a threat to the user's safety. Finally, after passing the model-checking, the Lustre code will be converted into executable code for the device to execute normally, such as C code.

Here we want to introduce a study of our method to develop an application for controlling IoT devices in a smart house and checking the power of these devices. As we mentioned earlier, this study includes building models, translating the DSML model into Lustre code, and model checking.

4.1 Model Building

We used Sirius, which is a graphical DSML Tools in Eclipse to build the model of our study and give an overview of the metamodel in Figure 2.

In this model, IoT devices in Smart House consist of the working mode and sensors. Each device will automatically change its working mode by collecting environmental information of the house through sensors. For example, air condition can automatically adjust its working mode to cool and heat through the information of temperature in the room obtained by the temperature sensor to maintain the temperature within a set range.

In addition, considering that a large number of devices may lead to an increase in energy consumption and even the risk of fire due to overload, we also set an electric sensor in our model to get the power consumption of these devices when working to ensure that they are working under the specified power consumption set by user.

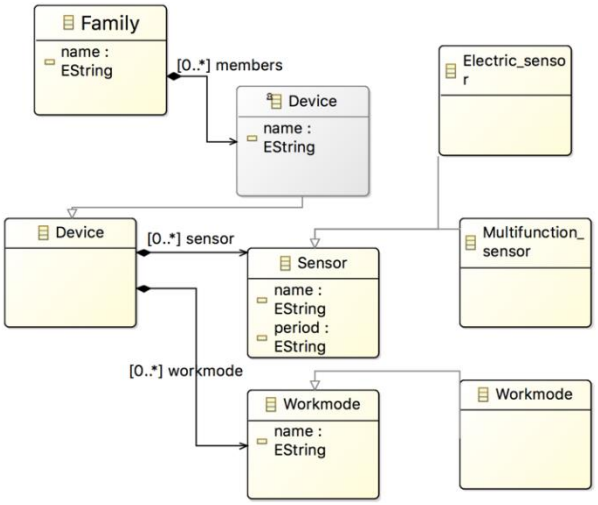


Figure 2. Overview of a metamodel.

Then we converted the metamodel built into a graphical UI on Sirius. On this UI, users can drag the icons of the devices they require and connect them to the Smart House system as the devices in their house to build a Smart House system they want. They also can set the power cap they hope for these devices. And in this process, users do not need to enter any code. We give an overview of the graphical UI in Figure 3.

Finally, with the help of the generation function of Sirius, we converted the information of the model built before into an XML file.

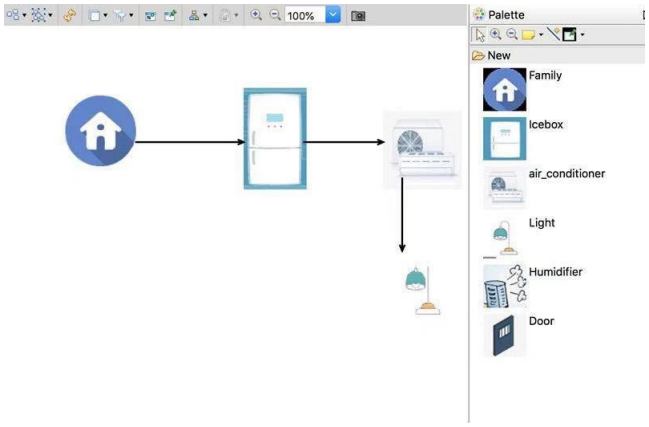


Figure 3. Overview of graphical UI.

4.2 Code Generation

After the model was built, we generated a Lustre code for this model to execute.

We give an overview of our Lustre program in Figure 4. For the Lustre program, we wrote everything in a master node to ensure real-time performance. At the same time, we used two different child nodes in the master node to implement the operation of control and power verification for devices and defined them as the Control Node and Verification Node.

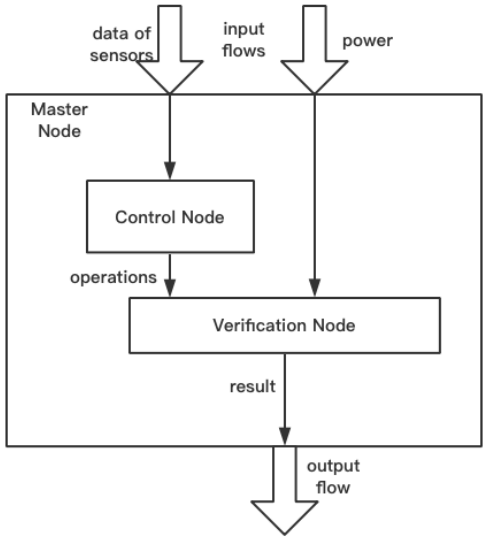
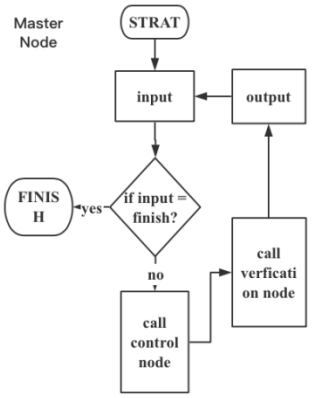


Figure 4. Overview of lustre program.

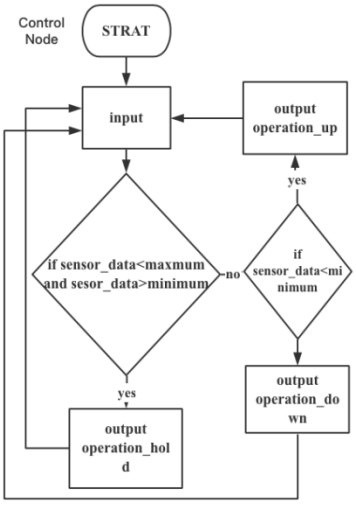
The master node obtained the data of each sensor and the power of each device as input flows. And the Control Node took the data of sensors obtained by the master node as its own input flow and returns the operation to be performed next according to the data of sensors as an output flow to the master node. In addition, the master node passed the power of the operations should be performed next as well as the power consumption for devices now to the Verification Node as input flows for verification. If the power consumption after performing these operations exceeded the requirement, a command to reject these operations would be returned as an output flow to the master node. Finally, the master node would output a warning command to the system if the

verification of power failed, otherwise it would output the command for operation should be performed next. Flow charts and code for each node are shown in Figure 5, Figure 6 and Figure7.



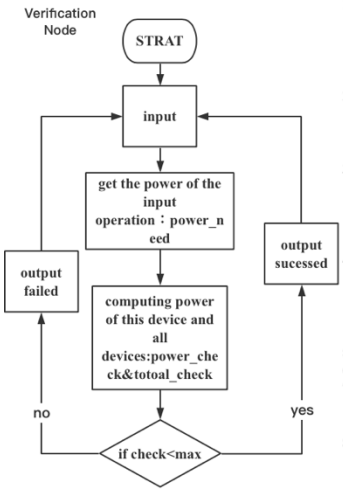

```
1. node master(de:device; sensor_data,
   power:real)
   returns(r_operation:operation;
   warning:bool);
2. var
3. control_output:operation;
4. verification_output:bool;
5. let
6.   control_output=control(de,
     sensor_data);
7.   verification_output=verification(de,
     control_output, power);
8.   r_operation = if verification_output
     then
     control_output
     else operation_hold;
9.   warning = if verification_output then
     false else true;
10. tel
```

Figure 5. Overview of the master node.




```
1. node control(de:device;
   sensor_data: real)
   returns(result:operation);
2. var
3.   max, min:real;
4. let
5.   max= if de = air_condition
then
     air_data_max
     else if de = humidifier then
     humidifier_data_max
     else lights_data_max;
6.   min= if de = air_condition
then
     air_data_min
     else if de = humidifier then
     humidifier_data_min
     else lights_data_min;
7.   result= if sensor_data > max
     then
     operation_down
     else if sensor_data < min then
     operation_up
     else operation_hold;
8.  tel
```

Figure 6. Overview of the control node.




```
1. device_max = if de = air_condition then
   air_condition_safety
   else if de = humidifier then
   humidifier_safety
   else lights_safety;
2. power_up = if de = air_condition then
   air_up_power
   else if de = humidifier then
   humidifier_up_power else lights_up_power;
3. power_down = if de = air_condition then
   air_down_power
   else if de = humidifier then
   humidifier_down_power
   else lights_down_power;
4. power_need = if op = operation_up then
   power_up
   else if op = operation_down then
   power_down
   else 0.0;
5. power_check = power_need + power_used;
6. total_check = total_used + power_need;
7. result = if power_check < device_max and
   total_check < total_safety
   then true else false;
8. total_used = 0.0
      ->(if pre(result) then pre(total_used) +
   pre(power_used) else pre(total_used));
```

Figure 7. Overview of the verification node.

In this way, we can input the data of sensors and the power of devices into the Lustre program at a certain frequency, and the program will give output about the command of operation or a warning for each input in real-time.

4.3 Model Checking

Finally, we did a model-checking for our Lustre code through Kind 2 [12]to verify before the code was executed in order to check whether the logic and execution order meet our needs.

Kind 2 is an automatic model checker for the safety properties of Lustre programs. Kind 2 can take as input a Lustre file annotated with properties to be proven invariant and outputs which of the properties are true for all inputs, as well as an input sequence for those properties that are falsified.

When we got the Lustre program, we wanted to verify whether the program meets our requirements through three different verifications. First, we wanted to verify whether the program can properly transmit the correct command of operations to the device according to the data collected by the sensor, such as whether the Control Node would output a command to increase the temperature when a collected temperature in the house was lower than the minimum set by us. Second, we wanted to verify whether the Verification Node meets the requirement, which means the node should output a rejection instruction when the power consumption exceeded the standard. Finally, we verify the output of the master node to make sure whether it meets the requirement. In other words, we wanted to ensure the warning command and rejection instruction would appear at the same time, and the command to perform operations will not appear at the same time as well as rejection instruction.

After clarifying the content of verification, we completed the verification using Kind 2 through adding appropriate annotation in the body to specify properties to verify in the Lustre program.

5. CASE STUDY

This section describes a case study of our model and verification method. And we show the entire process and tools in Figure 8.

We connected three different devices to the Smart House system in graphical UI including air-conditioning, light, and humidifiers. You can see the model in Figure 9. As mentioned earlier, the air-conditioning would adjust the temperature based on the date from the temperature sensor. And the light will control itself to turn on and turn off through the light sensor. Similarly, the humidifier can adjust the humidity in the house automatically based on the information obtained by its own sensor. In the meantime, a power cap was set. Then we translated the information of the model into an XML file used by the Lustre program.

For the Lustre program, we had written the execution code of many devices in the Lustre program in advance, and then read the information of devices in an XML file to determine which devices should be used this time. The flag of the selected device in the Lustre program would be set to ON state to ensure the corresponding operation can be executed. At the same time, the corresponding parameter in the Lustre program was adjusted according to the power cap in the XML file.

Then we added a lot of annotations like the following in the Lustre program to assist in the three verifications mentioned before and completed verifications with Kind 2.

```
   --%PROPERTY sensor_data>max =>
Control_output=operation_down;
```

```
   --%PROPERTY power_check>max =>
rejection=1;
   --%PROPERTY rejection=1 =>
operation=operation_hold;
```

As a result of Kind 2, it was confirmed that the operation that does not satisafy the power limit will be rejected by program, and the operation can be executed rightly when the limit is satisfied.

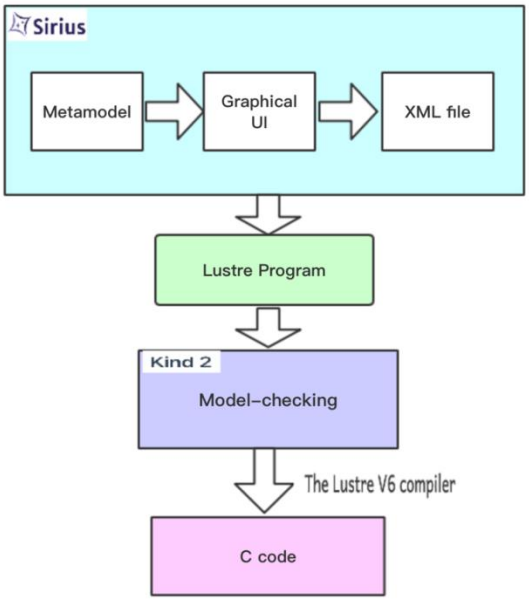


Figure 8. Process and tools.

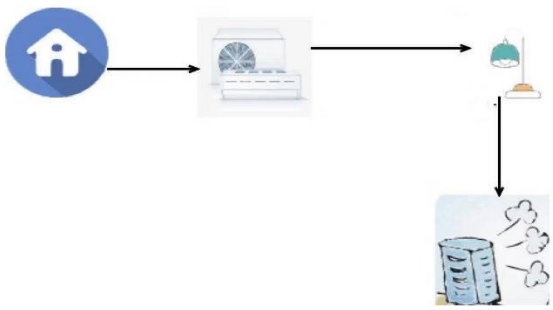


Figure 9. Model for evaluation.

Finally, we converted the Lustre program into an executable C code through the Lustre V6 compiler and manually entered a bunch of data to simulate the environmental data obtained by sensors. As a result, operation could not be executed if the safety property requested by the user was not satisfied.

6. CONCLUSIONS AND FUTURE WORK

We propose a method for using DSML to develop IoT application and translating the model into Lustre code for verification including model building, code generating, and model checking.

In the case study, we used Sirius to build a simple model of Smart House for device control and power checking. Then we generated a Lustre program about this model. After verifying this program through Kind 2, the Lustre program was translated into an executable C code with the help of the Lustre V6 compiler finally.

In future work, we hope to extend our model and verify the Lustre program of the built model for Smart House in a real environment. Then we plan to improve the method about Lustre code generating from the DSML model. At last, we hope our system can realize the function of automatically generating the corresponding Lustre program after the model is built.

7. REFERENCES

[1] Zanella, A., Bui, N., Castellani, C., Vangelista, L., and Zorzi, M. 2014. Internet of things for smart cities. In *IEEE Internet of Things journal*. (2014), 22–32.

[2] Scaife, N., Sofronis, C., Caspi, S., Tripakis, S., and Maraninch, F. 2004. Defining and translating a "safe" subset of Simulink/stateflow into lustre. In *Proceedings of the 4th ACM international conference on Embedded software*. (2004), 259-268.

[3] Viyovic, V., Maksimovic, M., and Perisic, B. 2014. Sirius: A rapid development of DSM graphical editor. In *IEEE 18th International Conference on Intelligent Engineering Systems INES* (2014). 233-238.

[4] Moody, D. 2007. What makes a good diagram? Improving the cognitive effectiveness of diagrams in is development. In *Advances in Information Systems Development*. (2007), 481-492.

[5] Halbwachs, N., Caspi, P., Raymond, P., and Pilaud, D. 1991. The synchronous data flow programming language LUSTRE. In *Proceeding of the IEEE*. (1991), 1305-1320.

[6] Tahier, E., Raymond, P., and Halbwachs, N. 2019. The Lustre V6 Reference Manual. DOI= http://www-vrimag.imag.fr/DIST-TOOL/SYNCHRONE/lustre-v6/doc/lv6-ref-man.pdf.

[7] Halbwachs, N., Caspi, P. Raymond, P., and Pilaud, D. 2000. The synchronous dataflow programming language LUSTRE. (2000).

[8] Agarwal, P., Alam, M. 2018. Investigating IoT Middleware Platforms for Smart Application Development. DOI= https://arxiv.org/abs/1810.12292.

[9] Bernstein, P. 1996. Middleware: a model for distributed system services. In *Communications of the ACM*. (1996), 86-98.

[10] Scott, R., Ostberg, D. 2018. A comparative study of open-source IoT middleware platforms. In *KTH Stockholm*. (2018).

[11] Velazquez, J. 2018. Securing openHAB smart home through user authentication and authorization. In *Institute of Computer Science*. (2018).

[12] About Kind 2. Retrieved from https://kind.cs.uiowa.edu/kind2_user_doc/.

An Enhanced Two-factor Authentication Protocol for V2V Communication in VANETs

Tarak Nandy
Department of Computer System and Technology
Faculty of Computer Science and Information Technology
University of Malaya
Kuala Lumpur, Malaysia
tarak@um.edu.my

Mohd Yamani Idna Bin Idris
Department of Computer System and Technology
Faculty of Computer Science and Information Technology
University of Malaya
Kuala Lumpur, Malaysia
+603 7967 6414
yamani@um.edu.my

Rafidah Md Noor
Department of Computer System and Technology
Faculty of Computer Science and Information Technology
University of Malaya
Kuala Lumpur, Malaysia
+603 7967 6346
fidah@um.edu.my

Ismail Ahmedy
Department of Computer System and Technology
Faculty of Computer Science and Information Technology
University of Malaya
Kuala Lumpur, Malaysia
+603 7967 6440
ismailahmedy@um.edu.my

Sananda Bhattacharyya
Department of Information Technology
Maldives Business School
Male', Maldives
sanada@businessschool.mv

ABSTRACT
The objective of the vehicular ad-hoc network (VANET) is to mobilize transportation systems along with the enhancement of safeguard and efficiency. Security and anonymity are important aspects of VANET too. Vehicle-to-vehicle (V2V) communication fulfills most of the requirements in VANET except the security breaches. Authentication protocols are designed to improve security by validating legitimate users in V2V communication. In this research, we proposed a two-factor authentication protocol using user biometric-based and password-based, which can support minimum or no VANET infrastructure environments. Furthermore, we performed an informal security analysis on the aforesaid protocol and shown the security features of it. We further discussed the future scope of the research in the field of VANET authentication.

CCS Concepts
• **Security and privacy→Multi-factor authentication**.

Keywords
Authentication; vehicle-to-vehicle communication; VANET; DSRC; internet of vehicles; intelligent transport system.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388185

1. INTRODUCTION
In recent years, automobile industries invest to incorporate automation in vehicles. Traditional vehicular systems are molted to become the smart vehicular system, which is also known as the Internet of Vehicles (IoV). IoV is a major part of the revolutionary concept of a smart city. Therefore, industries and researchers are conducting occasions to improve road management to create a robust and responsive transportation system. Vehicle-to-vehicle V2V communication is one of the important aspects of VANET [1]. V2V communication has stolen significant attention to improving traffic safety for the Intelligent Transportation System (ITS) [2]. VANET allows every vehicle to communicate in a short-range, called Dedicated Short Range Communication (DSRC). Vehicles can interchange valuable information such as alert messages, emergencies, route, signal and also communication bandwidth [3] using V2V communication. On the other hand, that increases the probability of attacks [4] on the network or vehicle to either gain access to the system or intends to harm the system including components [5]. For example, an intruder can pretend to be a legitimate vehicle or set of vehicles and communicate using false messages to other vehicles and get its route prediction and pattern of network. Moreover, autonomous vehicles are more prone to attacks, because it needs a little or no intervention of human and depends highly on sensor-based information. The attacker can take advantage of breaches in the network or the protocol to get access to the system to perform their malicious activities.

1.1 Motivation and Contribution
Internet of Things (IoT) always plays a great role to motivate automation systems. Internet of Vehicle (IoV) is one of the important parts of the IoT. Therefore, security issues on autonomous vehicles are a principle reason to conduct this research, because it can drag a total annihilation in the road with the autonomous vehicles if an intruder tries to destroy or malfunction the system. In this study, we concentrate on the

authentication of the vehicle in the V2V network with the DSRC (See Figure 1) of the VANET.

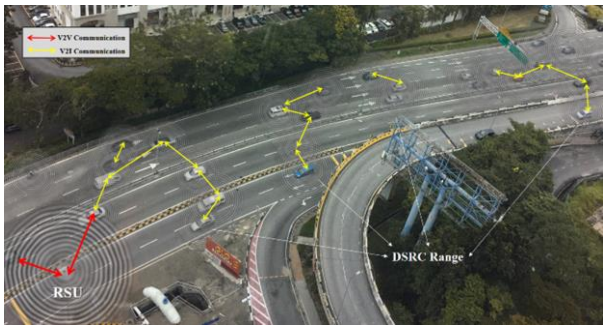


Figure 1.V2V scenario in VANET.

The rest of the paper is organized as per the following manners. Section 2 shows the literature review on the V2V authentication. After that, the proposed authentication protocol has been discussed in section 3 with the system model and assumption. Section 4 represents the informal security analysis of the proposed protocol. Lastly, discussion and future scope are demonstrated in section 5 followed by a conclusion in section 6.

2. RELATED WORK

Security is an alarming issue in VANET due to enormous attacks. Researchers developed a plethora of authentication mechanisms based on the attack model on their proposed schemes. However, pseudonym-based approaches and group-signature based approaches for authentication in VANET are most popular.

Ravi, et al. [6] designed a message authentication scheme based on the Elliptic Curve Digital Signature Algorithm (ECDSA). Yao, et al. [7] proposed biometric-based anonymous authentication in VANET in the data link layer. Then, Hasrouny, et al. [8] invented group-based authentication form V2V communication, in which supports safety message dissemination. After that, Prathima, et al. [9] designed an authentication framework, which supports both V2V and Vehicle to Infrastructure (V2I) communication. However, this framework needs Road Side Unit (RSU) to authenticate vehicles, which is not ideal for the rural or infrastructure-less area. Then, a cloud-assisted protocol has been invented by Rajput, et al. [10]. Again, a group-based authentication has been proposed by Waghmode, et al. [11]. Rekik, et al. [12] invented dual authentication and key management technique to improve the Quality of Service (QoS). Vasudev and Das [13] designed an authentication protocol based on only vehicle id and password, which is vulnerable to attacks. Then, Lim, et al. [14], proposed a Lidar information based protocol to support an infrastructure-less environment, but Lidar sensors are unable to detect an object in a shadowing situation.

By investigating all the drawbacks and loopholes of the existing authentication protocols for V2V, we finalized and proposed a biometric-based authentication protocol for V2V communication in DSRC, which can support the infrastructure-less environment too.

3. PROPOSED AUTHENTICATION PROTOCOL

Communication under centralized control is common in the vehicular network, but V2V communication in the decentralized network like VANET is challenging. The proposed authentication protocol ensures communication between legitimate vehicles and users even in a situation where supporting services unavailable, like RSU, authentication server and so on. The proposed protocol has several phases to fulfill the ultimate communication in the ad-hoc network in V2V, which are the initial setup phase, registration phase, authentication phase, and communication phase. The elaboration of all the phases is described as follows. Notations, which are used in the protocols, are provided in the document (See Figure 2).

Notation	Description
B_a	Biometric information of V_a user
B_b	Biometric information of V_b user
$DE_s(.)$	Decryption function
$EN_s(.)$	Encryption function
$h(.)$	One way hash function
$H(.)$	Bio-hash function
ID_{V_a}	ID of V_a
ID_{V_b}	ID of V_b
ID_{VIS}	ID of VIS
K_{VIS}	Vehicle Information Server(VIS) Key
M_i	Message
n_s	Nonce generated by VIS
n_a	Nonce generated by $V_a$to register with VIS
n_b	Nonce generated by V_b to register with VIS
PW_{V_a}	Password of V_a
PW_{V_b}	Password of V_b
q_a	Nonce generated by V_a to communicate with V_b
Rq	Request for communication
Rp_{EN}	Encrypted reply generated against request Rq
Rp_{DE}	Decrypted form of reply Rp_{EN}
s_a	Nonce generated by VIS to register V_a
s_b	Nonce generated by VIS to register V_b
T, T_i	Time-stamp values
U_i	User
V_a	Vehicle a
V_b	Vehicle b
VIS	Vehicle Information Server
$X \mid\mid Y$	Concatenation operation
$X \oplus Y$	XOR operation

Figure 2. Notation.

3.1 System Model and Assumption

The network model (See Figure 3) of the protocol is in a VANET scenario where two decentralized vehicles can communicate. This model has two layers, namely the server layer, and the vehicle layer. Vehicle Information Server (VIS) is equipped with high storage and computational capabilities, which stores vehicle information. Vehicles, which are registered, can only participate in the communication. Vehicles are equipped with On-Board Unit (OBU), which is protected in a Temper Proof Device (TPD). OBU consists of all important information, stored in the registration phase, to communicate with another vehicle. A new car, as well as an old car, can be registered through VIS by including TPD in the vehicle. Vehicles need to authenticate themselves to process for communication with others.

To achieve the ultimate performance and to make the proposed protocol lightweight, we have chosen simple but powerful mathematical and logical operations like Hash and XOR. All the hash operation of the system are based on SHA2 with the digest size 256. The purpose of choosing the SHA2 over other hashed function is for its performance and security. As the size of the key is large, the cost to break the key is high. On the other hand, XOR computation is extremely fast, especially on the hardware. Additionally, it does not depend on the size of the value. Moreover, using XOR is easy to understand and analyze.

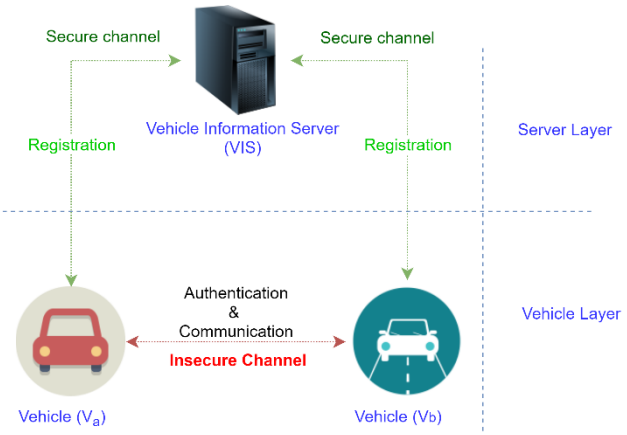


Figure 3. Authentication system model.

3.2 Initial Setup Phase

In the initial set-up, there are several VIS, which has information about the registered vehicles and can register new vehicles in the server. To set up a server, it supplies with a server id, ID_{VIS} and it generates nonce n_s to compute server keyK_{VIS}, by using equation 1.

$$K_{VIS} = h(ID_{VIS} \,||\, n_s) \tag{1}$$

The initial phase is done through a secure channel of communication.

3.3 Registration Phase

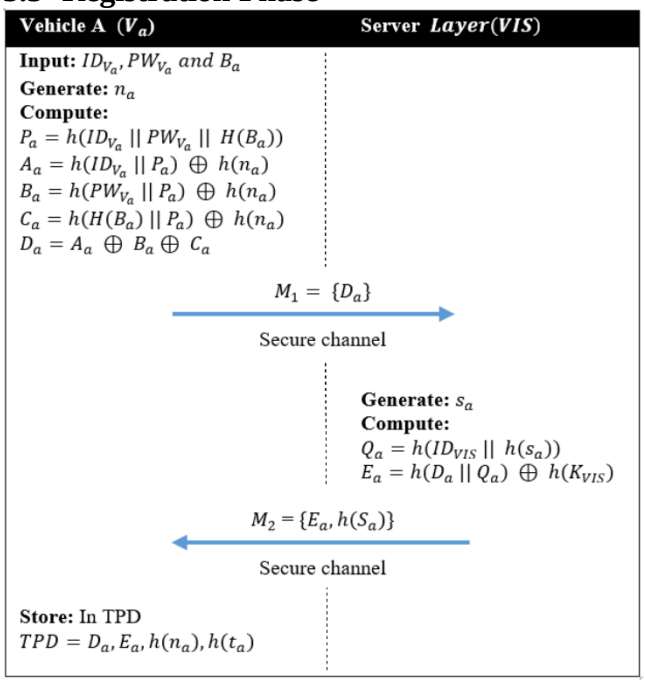


Figure 4. Vehicle registration phase.

In the registration phase, old and new vehicles are registered with the VIS. Vehicles can be registered through the purchase period. However, old cars can also join in the VANET by implementing permanent TPD, which will contain OBU in it. Therefore, when a car is purchased, it communicates with the VIS, and populate vehicular unique identification details and store in a TPD, which is safely placed in the vehicle. TPD information is required for further communication.

The proposed protocol operates in both secure and insecure channels. This phase of the protocol design needs a secure communication channel to register a vehicle into the VIS. Secure communication can be done through the blockchain mechanism [15].

The vehicle registration phase is pictorially presented in the document (See Figure 4).

3.3.1 *Vehicle to Server*

Vehicles are well equipped with biometric equipment to receive biometric information from the user of the vehicle. In this step, users need to provide the vehicle's identification number ID_{V_a}, password , PW_{V_a} and user biometric information B_a through device.

- Vehicle generate a nonce value n_a.
- Vehicle computes P_a using ID_{V_a}, PW_{V_a}, and $H(B_a)$ as equation 2.

$$P_a = h(ID_{V_a} \,||\, PW_{V_a} \,||\, H(B_a)) \tag{2}$$

- Then it computes A_a using vehicle ID ID_{V_a},P_a and hashed value of nonce n_a as equation 3.

$$A_a = h(ID_{V_a} \,||\, P_a) \oplus h(n_a) \tag{3}$$

- After that, car computes B_a using vehicle password PW_{V_a},P_a and hashed value of nonce n_a as equation 4.

$$B_a = h(PW_{V_a} \,||\, P_a) \oplus h(n_a) \tag{4}$$

- Next, it computes C_a using user bio-hashed value of biometric information B_a,P_a and hashed value of nonce n_a as equation 5.

$$C_a = h(H(B_a) \,||\, P_a) \oplus h(n_a) \tag{5}$$

- Then, it computes D_a using A_a, B_a and C_a as equation 5.

$$D_a = A_a \oplus B_a \oplus C_a \tag{6}$$

- Finally, the vehicle sends the computed data D_a as a message M_1 to VIS.

3.3.2 *Server to Vehicle*

- After getting D_a from vehicle V_a, the server generates nonce s_a to register the vehicle V_a.
- After that, the server computes Q_a by using server identification number ID_{VIS} and hashed value of nonce s_a as equation 7.

$$Q_a = h(ID_{VIS} \,||\, h(s_a)) \tag{7}$$

- Furthermore, the server computes E_a by the help of D_a, Q_a and hashed value of server key K_{VIS} as equation 8.

$$E_a = h(D_a \,||\, Q_a) \oplus h(K_{VIS}) \tag{8}$$

- Finally, the server sends the hashed value of nonce S_a and computed value E_a to the vehicle V_a through a secured channel.

3.3.3 *Vehicle Phase*

At the end of the registration phase, vehicle V_a stores $D_a, E_a, h(n_a), h(t_a)$ into OBU, which is in TPD.

The registration phase shows the procedure of registering a vehicle into the system by using its ID, user's password, biometric information, the nonce value of the vehicle, nonce value of server, server ID and server secret key. This stored information will further be used for the rest of the communication in the system.

3.4 Authentication Phase

In the authentication phase, passing information is crosschecked with OBU information in the vehicle. If a vehicle wants to communicate with other vehicles in DSRC in VANET, then both of the vehicles need to prove their authenticity individually. The authentication phase (See Figure 5) is illustrated as follows.

In this phase, the user needs to provide the identification number and password of the vehicle along with his/ her biometric information.

After receiving these values, the car regenerates P_a, A_a, B_a, C_a *and* D_a by using the following equations 9, 10, 11, 12, 13.

$$P'_a = h(ID'_{V_a} \,||\, PW'_{V_a} \,||\, H(B'_a)) \quad (9)$$
$$A'_a = h(ID'_{V_a} \,||\, P'_a) \oplus h(n_a) \quad (10)$$
$$B'_a = h(PW'_{V_a} \,||\, P'_a) \oplus h(n_a) \quad (11)$$
$$C'_a = h(H(B'_a) \,||\, P'_a) \oplus h(n_a) \quad (12)$$
$$D'_a = A'_a \oplus B'_a \oplus C'_a \quad (13)$$

Finally, vehicles check if the stored value of D_a and computed value of D'_a is equal. If they are same then the vehicle is eligible to participate in further communication with other vehicles in DSRC.

However, in this phase, the protocol is unable to detect any malicious vehicle.

Vehicle A (V_a)	Vehicle B (V_b)
Input: ID'_{V_a}, PW'_{V_a} **and** B'_a	**Input:** ID'_{V_b}, PW'_{V_b} *and* B'_b
Compute:	**Compute:**
$P'_a = h(ID'_{V_a} \,||\, PW'_{V_a} \,||\, H(B'_a))$	$P'_b = h(ID'_{V_b} \,||\, PW'_{V_b} \,||\, H(B'_b))$
$A'_a = h(ID'_{V_a} \,||\, P'_a) \oplus h(n_a)$	$A'_b = h(ID'_{V_b} \,||\, P'_b) \oplus h(n_b)$
$B'_a = h(PW'_{V_a} \,||\, P'_a) \oplus h(n_a)$	$B'_b = h(PW'_{V_b} \,||\, P'_b) \oplus h(n_b)$
$C'_a = h(H(B'_a) \,||\, P'_a) \oplus h(n_a)$	$C'_b = h(H(B'_b) \,||\, P'_b) \oplus h(n_b)$
$D'_a = A'_a \oplus B'_a \oplus C'_a$	$D'_b = A'_b \oplus B'_b \oplus C'_b$
Check: $\boldsymbol{D_a = D'_a}$?	***Check***: $D_b = D'_b$?
If yes, registered vehicle and user to communicate in V2V scenario.	If yes, registered vehicle and user to communicate in V2V scenario.

Figure 5. Authentication phase.

3.5 Communication Phase

In this part of the protocol, one vehicle can communicate with other vehicles in the range of DSRC after passing the authentication phase. Let vehicle A,V_a wants to communicate with vehicle B, V_b.The steps of the communication phase and the details are represented in the document (See Figure 6).

3.5.1 Vehicle A to Vehicle B

- Vehicle A, V_a produces a request Rq to vehicle B, V_b. Let the operation happens at T_1 time.
- V_a generates nonce q_a.
- V_a computes $h(K'_{VIS})$ by the help of equation 14.

$$h(K'_{VIS}) = E_a \oplus (h(D_a \,||\, h(ID_{V_a} \,||\, PW_{V_a} \,||\, H(B_a)) \,||\, h(t_a)) \quad (14)$$

- After that, V_a generates F_a , G_a , and H_a respectively as shown in equation 15, 16, 17.

$$F_a = h(h(K'_{VIS} \,||\, T_1)) \oplus H(q_a) \quad (15)$$
$$G_a = F_a \oplus h(q_a) \oplus h(K_{VIS}) \quad (16)$$
$$H_a = Rq \oplus G_a \oplus h(K_{VIS}) \oplus T_1 \quad (17)$$

- Then, V_a sends F_a, H_a *and* T_1 to V_b as message M_3.

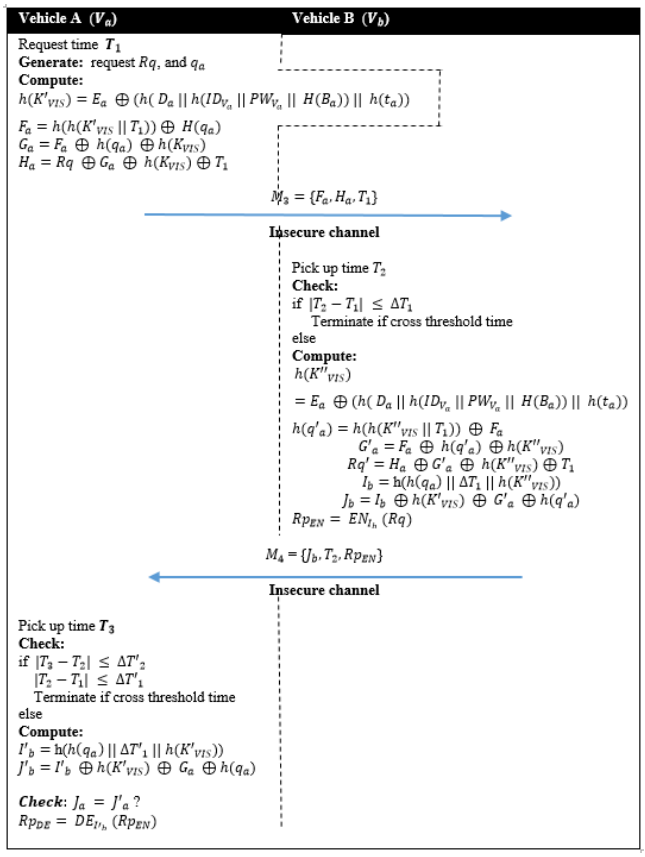


Figure 6. Communication phase.

3.5.2 Vehicle B to Vehicle A

- After receiving M_3 from V_a, V_b pick up time T_2 and check the threshold time ΔT by performing equation 18 to check whether the request is current. If not satisfied the communication stops here.

$$\text{if } |T_2 - T_1| \leq \Delta T_1 \quad (18)$$

- V_b computes $h(K''_{VIS})$ to extract actual request Rq by using the following equations.

$$h(K''_{VIS}) = E_a \oplus (h(D_a \,||\, h(ID_{V_a} \,||\, PW_{V_a} \,||\, H(B_a)) \,||\, h(t_a)) \quad (19)$$
$$h(q'_a) = h(h(K''_{VIS} \,||\, T_1)) \oplus F_a \quad (20)$$
$$G'_a = F_a \oplus h(q'_a) \oplus h(K''_{VIS}) \quad (21)$$
$$Rq' = H_a \oplus G'_a \oplus h(K''_{VIS}) \oplus T_1 \quad (22)$$

- Then, V_b generates I_b and J_b by the help of the following equations.

$$I_b = h(h(q_a) \,||\, \Delta T_1 \,||\, h(K''_{VIS})) \quad (23)$$
$$J_b = I_b \oplus h(K'_{VIS}) \oplus G'_a \oplus h(q'_a) \quad (24)$$

- Finally, V_b produce a reply and encrypt the reply to $Rp_{EN}$and send a message over the insecure network as m4 to V_a, containingJ_B, T_2, Rp_{EN}.

3.5.3 Vehicle A

- V_a receives an encrypted reply and pick up time T_3.
- V_a checks the threshold value of ΔT_1 and ΔT_2 using equations 25 and 26. If not satisfied terminate the communication.

$$|T_3 - T_2| \leq \Delta T'_2 \quad (25)$$
$$|T_2 - T_1| \leq \Delta T'_1 \quad (26)$$

- V_a computes I'_b and J'_b and checks if J'_b is the same as J_b. If not the same, V_a close the communication or continue.
- Finally, V_a decrypt the reply Rp_{DE} as equation 27.

$$Rp_{DE} = DE_{I'_b}(Rp_{EN}) \quad (27)$$

The authentication between the vehicles (V_a *and* V_b) through three phases 1) initial setup phase, 2) registration phase, and 3)authentication phase are shown in intensive ways. Moreover, rational and mathematical justifications are clearly demonstrated the working pattern of the scheme. In the next part of the paper, we will discuss about the security analysis on the proposed scheme.

4. SECURITY ANALYSIS

Interconnected network is vulnerable for attacks [4]. There can be enormous attacks on the intelligent transport system from inside and outside of the network. In this section, the paper discussed various security analyses and shows proof of protection against a range of common attacks in VANET. To continue further discussion, let consider an intruder as $\mathscr{A}$ and a victim car is V_a.

4.1 Insider Attack

As the protocol uses a strong hash function and P_a, an internal intruder $\mathscr{A}$ will be unable to get any information about another user U_i. Therefore, the proposed protocol fight against Insider attack.

4.2 Masquerade Attack

The proposed protocol uses biometric information B_a of the user U_i of the vehicle. Moreover, this information is protected using the bio-hashing function $H(.)$. Therefore, $\mathscr{A}$ cannot masquerade as another user and continue the communication. Therefore, the scheme is well enough to protect the car from Masquerade attack.

4.3 Password Guessing

In the proposed protocol, the password PW_{V_a} is never sent with any messages M_i. During the registration process, if $\mathscr{A}$ gets the information of D_a, it is hard to guess the password PW_{V_a} from there, because D_a is calculated based on not only the hashed password PW_{V_a} but also vehicle id ID_{V_a}, biometric value B_a of user U_i and nonce n_a of V_a, which is secret to V_a. During communication over an insecure channel, none of F_a, H_a, T_1 carries information about the password.

4.4 Stolen Device

In this scenario, $\mathscr{A}$ steels the TPD from V_a and tries to get information from OBU. V_a only stores the calculated value of D_a and E_a and hashed value of vehicle nonce n_a and server nonce t_a, which are hard to get.

4.5 Replay Attack

$\mathscr{A}$ tries to stop or delay the communication and tries to pass the fake message to V_a. However, in the proposed system, V_a and V_b use the timestamp T_i to ensure the message pick up time and measure a threshold value $|T_{i+1} - T_i| \leq \Delta T_i$ to accept or decline the message.

4.6 Modification

$\mathscr{A}$ may try to modify after intruding communication data between V_a and V_b. However, the proposed protocol uses different calculations to produce J_b on both sides and check if the value $J_b = J'_b$ is valid. Therefore, modification of any message can be easily traced out.

4.7 Identity Protection

The identity of a vehicle V_a is never passed to another vehicle V_b in V2V communication. Therefore, information about the car is protected in the proposed protocol.

5. DISCUSSION AND FUTURE WORK

A few important points need to be discussed and established for further improvement. As per the related work, we found various drawbacks on the existing protocols, which we overcame in the proposed scheme. The discussion of them is consecutively explained here. Firstly, the Elliptic Curve Digital Signature Algorithm (ECDSA) uses a large number of keys to perform, which needs high primary storage capacity. Therefore, our protocol uses HASH and XOR operation to make the system less complex and more powerful. On the other hand, an only biometric-based protocol cannot protect the system alone. We use bio-hashing to protect biometric information. Additionally, our scheme does not depend on the RSU during the communication, makes the system to perform in any circumstances.

The study will be further improved to detect the intruder vehicle if a legitimate vehicle wants to attack another car. Formal security analysis can be conducted using BAN logic [16], Automated Validation of Internet Security Protocols and Applications (AVISPA)[17] or Random Oracle Model (ROM)[18]. In the future, we will conduct performance analysis for the proposed work in well-accepted tools like NS3, to compare with the existing authentication protocols. Besides, authentication protocols depend on a secure communication channel in some phases, we will try to implement all phases in an insecure channel and will improve if any bugs come. In addition, the proper acceptance threshold for the communication needs to be defined. This study concentrated on authentication based on OBU and users of vehicles. Furthermore, multiuser registration for a single vehicle is also important. Additionally, a password update or biometric information update needs to be a consideration. Therefore, we will focus on the above-mentioned criteria for our future work with this study.

6. CONCLUSION

V2V communication is still in the development stage. The improvement of security in VANET needs more attention because securing communication in VANET is an alarming issue. From that point of view, the proposed protocol is designed. Moreover, to make the scheme efficient and effective, we acquire the lightweight mechanism by implementing the HASH and XOR operation. Additionally, the protocol computes less and important equations to make the system more powerful on the basis of security and usefulness. We have proposed a novel technique of

authenticating the vehicle and its users in VANET communication. This protocol can register new and old vehicles in VIS to perform on-road communication among cars. Additionally, we proposed a self-authentication scheme for vehicles prior to process communication. Furthermore, we discussed how the suggested protocol resists current common threats via an informal security analysis. Finally, open issues and future scopes have been discussed. To conclude, the proposed protocol will not only provide an efficient and effective authentication mechanism but also will support other security and privacy features like authorization and anonymity for V2V communication in DSRC in VANET.

7. ACKNOWLEDGMENT

This research is supported by a partnership grant of University Malaya, RK004-2017. Authors of this article acknowledge their parent organization the University of Malaya for providing resources for this research. Furthermore, the authors thank all anonymous reviewers to make this research work more powerful and effective.

8. REFERENCES

[1] H. Hartenstein and K. Laberteaux, VANET: vehicular applications and inter-networking technologies. Wiley Online Library, 2010.

[2] T. Litman, Autonomous vehicle implementation predictions. Victoria Transport Policy Institute Victoria, Canada, 2017.

[3] T. Ghosh and S. Mitra, "Congestion Control by Dynamic Sharing of Bandwidth among Vehicles in VANET," in 2012 12th International Conference on Intelligent Systems Design and Applications, A. Abraham et al. Eds., (International Conference on Intelligent Systems Design and Applications. New York: Ieee, 2012, pp. 291-296.

[4] T. Nandy et al., "Review on Security of Internet of Things Authentication Mechanism," IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2947723. In press.

[5] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," (in English), IEEE Trans. Intell. Transp. Syst., Article vol. 16, no. 2, pp. 546-556, Apr 2015, doi: 10.1109/tits.2014.2342271.

[6] K. Ravi, S. A. Kulkarni, and Ieee, A Secure Message Authentication Scheme for VANET using ECDSA (2013 Fourth International Conference on Computing, Communications and Networking Technologies). New York: Ieee (in English), 2013.

[7] L. Yao et al., Biometrics-based Data Link Layer Anonymous Authentication in VANETs (2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing). New York: Ieee (in English), 2013, pp. 182-187.

[8] H. Hasrouny, C. Bassil, A. E. Samhat, A. Laouiti, and Ieee, Group-Based Authentication in V2V communications (2015 Fifth International Conference on Digital Information and Communication Technology and Its Applications). New York: Ieee (in English), 2015, pp. 173-177.

[9] P. Prathima, K. Rajendiran, G. S. Ranjani, P. Kurian, S. Swarupa, and Ieee, Simple and Flexible Authentication Framework for Vehicular Ad hoc Networks (2015 International Conference on Communications and Signal Processing). New York: Ieee (in English), 2015, pp. 1176-1180.

[10] U. Rajput, F. Abbas, J. Wang, H. Eun, H. Oh, and Ieee, "CACPPA: A Cloud-Assisted Conditional Privacy Preserving Authentication Protocol for VANET," in 2016 16th Ieee/Acm International Symposium on Cluster, Cloud and Grid Computing, (IEEE-ACM International Symposium on Cluster Cloud and Grid Computing. New York: Ieee, 2016, pp. 434-442.

[11] R. Waghmode, R. Gonsalves, D. Ambawade, and Ieee, Security Enhancement in Group Based Authentication for VANET (2016 Ieee International Conference on Recent Trends in Electronics, Information & Communication Technology). New York: Ieee (in English), 2016, pp. 1436-1441.

[12] M. Rekik, A. Makhlouf, F. Zarai, and Ieee, "Improved Dual Authentication and Key Management Techniques in Vehicular Ad Hoc Networks," in 2017 Ieee/Acs 14th International Conference on Computer Systems and Applications, (International Conference on Computer Systems and Applications. New York: Ieee, 2017, pp. 1133-1140.

[13] H. Vasudev and D. Das, A Lightweight Authentication Protocol for V2V Communication in VANETs (2018 Ieee Smartworld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation). New York: Ieee (in English), 2018, pp. 1237-1242.

[14] K. Lim, K. M. Tuladhar, and Ieee, "LIDAR: Lidar Information based Dynamic V2V Authentication for Roadside Infrastructure-less Vehicular Networks," in 2019 16th Ieee Annual Consumer Communications & Networking Conference, (IEEE Consumer Communications and Networking Conference. New York: Ieee, 2019.

[15] S. Rowan, M. Clear, M. Huggard, and C. Mc Goldrick, "Securing vehicle to vehicle data sharing using blockchain through visible light and acoustic side-channels," ed: eprint, 2017.

[16] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18-36, 1990, doi: 10.1145/77648.77649.

[17] Information Society Technology. "Automated Validation of Internet Security Protocols and Applications." http://www.avispa-project.org (accessed 18th April, 2019).

[18] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proceedings of the 1st ACM conference on Computer and communications security, 1993: ACM, pp. 62-73.

An Educational Smart Desk Control System for the Whole Family

Xinran Shao
Internet of Things Security
Zhengzhou University
China
+86 18903862198
ranxin101@gmail.com

Zhifeng He
Internet of Things Engineering
Zhengzhou University
China
+86 17638598501
Manage_hzf@163.com

Yutong Kang
Information Security
Zhengzhou University
China
+86 15237715202
kyt990830@163.com

ABSTRACT
With the rapid development of wireless communication technology and mobile network technology, the Internet of Things technology is also constantly being updated, and the number of people entering smart homes has exploded. Noticing the family of small-sized houses, placing too many desks and chairs in the home will take up too much space. If there are children in the family, as the children grow up, the inappropriate table will face multiple eliminations. To meet the height requirements of family members of different heights and help children achieve more efficient, intelligent learning to make up for the disadvantages of traditional learning methods, this paper uses a combination of sensors, hardware, software and servers to design and implement an educational smart desk control system for the whole family.

CCS Concepts
• **Computer systems organization→Sensors and actuators.**

Keywords
Internet of Things; Embedded Systems; Sensor network; web networking products; smart home.

1. INTRODUCTION
Integration of wireless communication technology with sensor and receiver modules can produce related information which called IOT (Internet of Things) system [1]. With the rapid development of technologies related to the Internet of Things perception layer, network layer and application layer, the number of people entering “smart home” has exploded.

We intend smart Home or Home Automation to bring comfort, security and render life much easier for its occupants. Daily and repeated tasks with in the home environment now can be automated and made more simple for users to deal with [2]. In the Internet of Things era, all the equipment in the home can be intelligent and humanized through the corresponding technology, bringing more convenience and meaning to the residents' lives.

Noticing the family of small-sized houses, placing too many tables and chairs in the home will take up too much space. As children grow, we will eliminate the inappropriate desks, increasing the cost of the family and also wasting resources. That's not environmentally friendly. To meet the differences between desk heights requirements of family members of different heights, and make up for the lack of traditional learning methods, such as non-intelligence and low efficiency. This paper designs and implements an Education-oriented intelligent desk control system for the whole family. It can customize this work based on the traditional study desk, combined with software design. And it helps users improve learning efficiency. The overall architecture is shown in Figures 1.

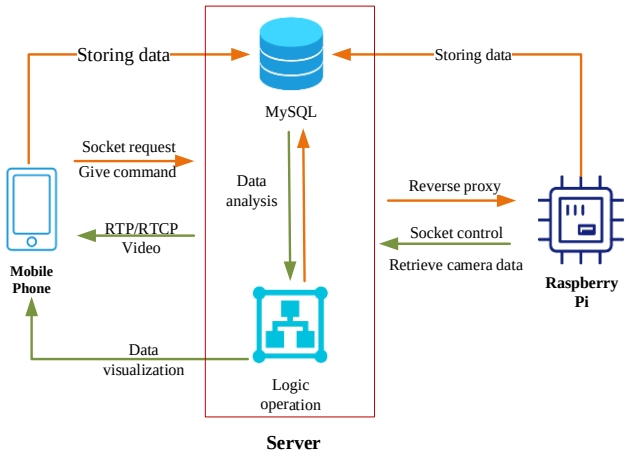


Figure 1. System architecture figure.

1.1 Hardware Design
The main components of the hardware system are Raspberry Pi, STM32F103ZET6, SONY IMX307 image sensor module, HY-SRF05 ultrasonic module, GY30 photosensitive module, PAJ7620U2 gesture recognition sensor, Arduino, push rod motor, touch screen, table lamp. As the host computer, the Raspberry Pi takes on the communication functions of software and hardware in the system, and simultaneously stores the role information and height information of each member in the family. As the lower computer, STM32 assumes the control of various components in the hardware system. Considering that the Raspberry Pi is in a private network, reverse proxy technology is used to redirect requests and responses to the public network [3]. Figure 2 shows the various devices of the hardware system.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388215

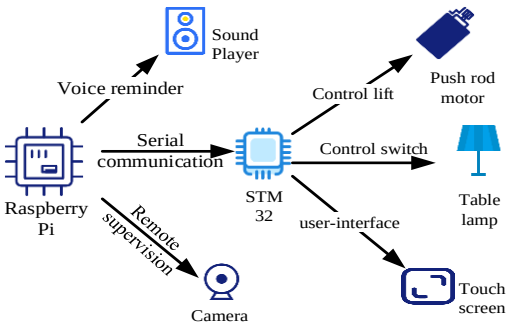


Figure 2. Hardware control system.

1.2 Software Design

The software is used by parents. When the parents go out, they can use this software to view the children's learning situation in real time and can arrange the learning tasks and send voice reminders. They can view the weekly or monthly learning status statistics of the children sent by the server.

2. SYSTEM IMPLEMENTATION

This paper divides the system into six modules shown in figure3. It includes lifting module, intelligent sensing module, learning customization module, visualization module, gesture interaction module and remote supervision. Each module works together to achieve design goals.

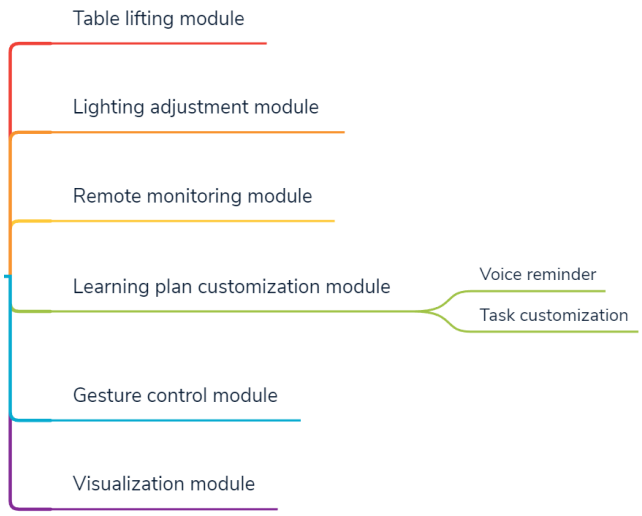


Figure 3. System module division.

2.1 Desk Lifting Module

STM32 F103ZET6 is the main control chip and Arduino is the auxiliary chip. The push rod motor with a stroke of 300 mm, a speed of 24 mm/s. a thrust of 500 N, and a voltage of 12 VDC was connected to the desk by eight M6 screws. The desk is lifted and lowered according to the PID algorithm[4]. The ultrasonic sensor HC-SR04 detects the current height of the desk. the Arduino UNO R3 chip controls three relay switches. Among them, the No. 1 relay controls the on and off of the whole circuit, and the No. 2 and No. 3 relays invert the positive and negative poles, controlling the motor to reverse. The control circuit diagram is shown in Figure 4. And you can also connect to the STM32 via the Bluetooth serial port of your mobile phone and send commands to control the height of the desk.

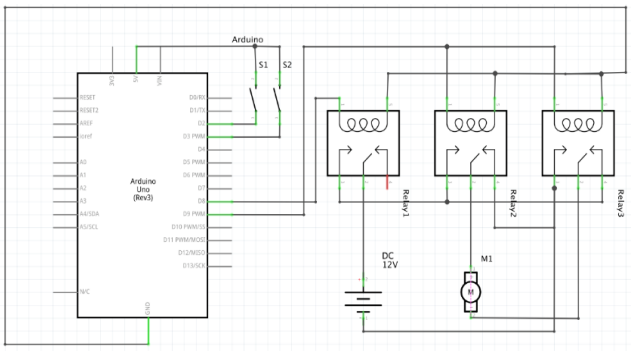


Figure 4. Push rod motor control figure.

The ultrasonic sensor module, HY-SRF05 is set under the desktop, the sensor is called by STM32. Detect desktop height with ultrasonic ranging [5]. Five sets of data are measured in a certain period, the maximum and minimum values are removed by the sorting algorithm, and the middle three sets are averaged to reduce the error. In this system, the Raspberry Pi serves as a data storage center and a software and hardware communication center. When different users use the desk for the first time, enter the character and height and save it in the local database MySQL of the Raspberry Pi. According to the Chinese GB/T3976-2002 standard [6], it is concluded that human height and desktop height are linear under the standard sitting and seat height conditions. Table 1 shows some data in the GB / T3976-2002 standard. This can be obtained as shown in figure 5. In figure 5, x(cm) stands for standard height and Y(cm) stands for standard table height.

$$Y = 0.4005x + 3.912$$

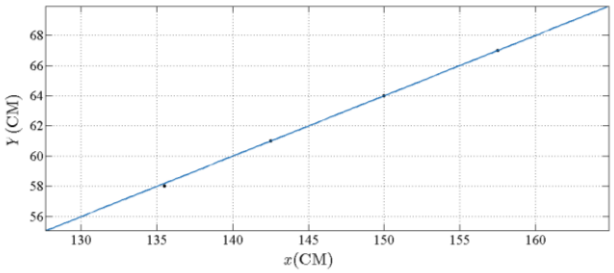


Figure 5. Linear diagram of *x* and *Y*.

Taking into account the individual differences of different users, the height of the desktop is adjusted by the touch screen. This part will be explained in the visualization module.

Table 1. Height and table height data in GB T3976-2002 standard

Standard height (cm)	Applicable height range (cm)	Desktop height (cm)
180.0	≥ 173.5	76
172.5	165 – 179	73
165.0	158 – 172	70
157.5	150 – 164	67
150.0	143 – 157	64
142.5	135 – 149	61
135.5	128 – 142	58
127.5	120 – 134	55

120.0	113 – 127	52
112.5	≤ 119	49

The adaptation algorithm of human height and desktop height is shown in Figure 6.

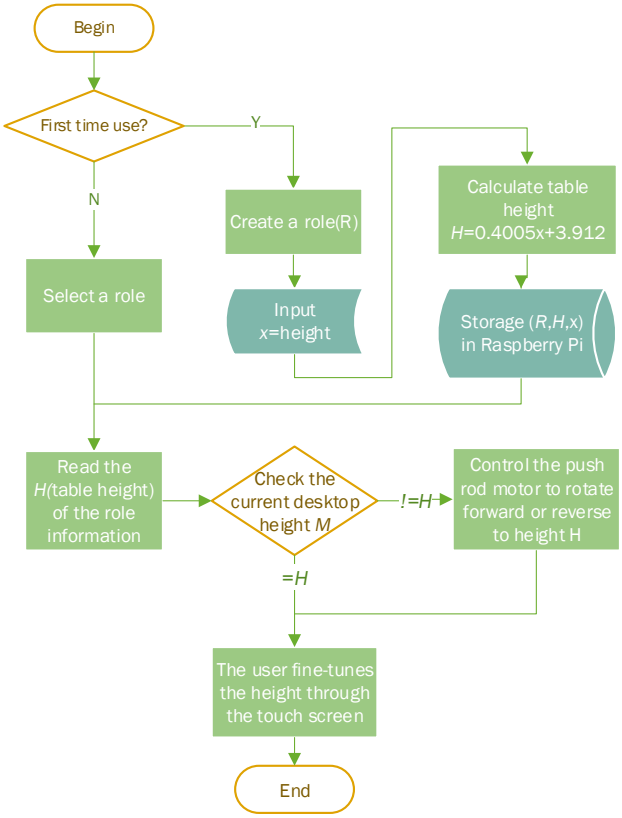


Figure 6. Adjust table height algorithm flow chart.

2.2 Lighting Adjustment Module

The system uses GY30 photosensitive module [7] to connect with STM32 main control chip through IIC bus to sense external light changes. When the ambient light intensity is lower than the set threshold, the LED light is turned on, and when the ambient light is higher than the set threshold, the LED light is turned off. Digital light intensity detection module GY-30 power supply is 3-5V, the illuminance range is 0-65535 lx. The sensor has a built-in 16-bit AD converted, direct digital output, omitting complex calculations and omitting calibration. It does not distinguish between ambient light sources, spectral characteristics close to visual sensitivity, and high-accuracy measurement of 1 lux for a wide range of brightness.

2.3 Remote Supervision Module

The video information collected by the camera is compressed by H264 encoding and sent to the mobile phone app through the reverse proxy technology via the RTP/RTCP protocol, so that the parent can remotely supervise the child's learning function. If the parent finds that the child is not serious about learning, he can make a remote reminder on the app. If the parent finds that the child intentionally obscures the camera, he can click on the corresponding button on the app to make the embedded system of the desk send a reminder "Do not block the camera". Figure 7 below shows the data flow of this module.

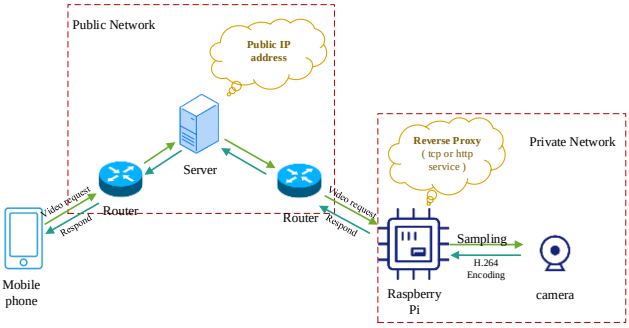


Figure 7. Remote supervision function principle figure.

2.4 Learning Plan Customization Module

Parents can use the mobile app to create a personalized learning program, set up daily learning tasks and more. After receiving the command, the Raspberry Pi will feedback the task to the STM32, which will be displayed on the touch screen and alert the user at the set time. The end user's task completion is fed back to the server. According to the algorithm, the server analyzes the data in units of day, week and month, and calculates the weekly or monthly learning status, task completion amount, fatigue level, etc, so that the user or parent can adjust the learning plan and arrange the time reasonably. This system can enhance the learning experience and improve the learning efficiency of the children. The workflow of this module is shown in figure 8.

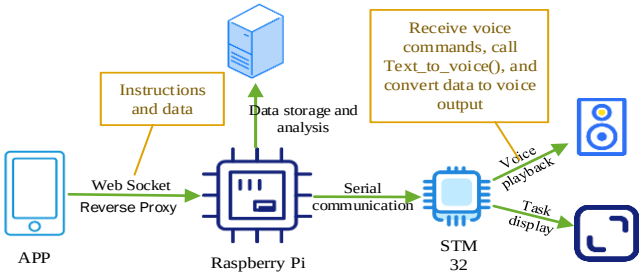


Figure 8. Learning plan customization principle figure.

In the user's learning process, he can play white noise through the touch screen to improve learning efficiency [8]. After the user's instruction is received by the STM32 through the touch screen, it will be transmitted to the Raspberry Pi by serial communication. The Raspberry Pi receives the command to control the speaker to play the white noise stored locally.

2.5 Gesture Control Module

The system uses the PAJ7620 gesture recognition sensor to connect directly to the STM32. The principle is shown in Figure 9. User can control the height of the desk and the status of the desk lamp switch by gestures, which is convenient for the user to operate. For example: wave up, desk rises; wave down, desk down; left and right wave can be console light switch.

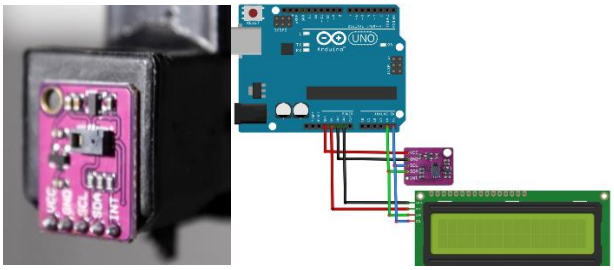


Figure 9. PAJ7620U2 gesture recognition sensor.

2.6 Visualization Module

The visualization module provides user interaction interfaces for the above five modules. Display the current desktop height, current character, task list, light control buttons, white noise buttons, etc. on the touch screen. Figure 10 shows the main screen of the touch screen

Figure 10. Capacitive touch serial screen figure.

3. SYSTEM EXPERIMENT

3.1 Hardware Experiment

After a lot of experimental tests, the hardware part of the system has a low delay, sensitive sensitivity, and the table can reach the specified height quickly. Some test data is in table 2. The hardware deployment is good and the communication between modules is normal. The experience of different users on the system can achieve the expected results.

Table 2. Partial experimental data.

User(cm)	Actual height (cm)	Table theory reaches height (cm)	Actual height of the table (cm)
Dad	180	76.002	76
Mom	165	69.995	70
Brother	185	78.005	78
Sister	160	67.992	68

3.2 Software Experiment

The parent can smoothly send task instructions to the table from the mobile app to display on the touch screen. The parent can smoothly send task instructions to the table from the mobile app to display on the touch screen. Monitor screen is shown in figure 11. Parents can smoothly check the current learning status of the child from the mobile app. After repeated trials by the system, the quality of the transmitted video is good, and the CPU occupancy and RAM occupancy rate are low during the whole process. The test data is shown in table 3.

Test environment:

OS: Android; RAM: 4G; CPU: Helio P25.

During the use of the software, the average RAM occupancy is approximately 26.46% and the average CPU occupancy is approximately 16.26%.

Table 3. Software Experiment data.

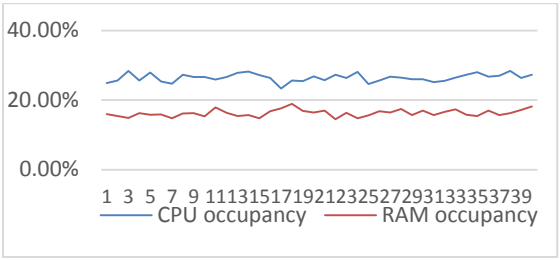


Figure 11. Monitor screen.

4. CONCLUSIONS

According to the conclusions of theoretical analysis and experimental tests, the system can effectively realize the reuse of different members on the same table and improve the learning efficiency of children and achieve the expected results. Moreover, there is no product on the market that has the functions discussed in this paper, so the system has great market potential and research significance. But the stability and fluency of the system still need to be improved.

5. REFERENCES

[1] Benfano Soewito, Christian, Fergyanto E. Gunawan, Diana, I Gede Putra Kusuma. 2019. *Websocket to Support Real Time Smart Home Applications.* Procedia Computer Science,157(157).

[2] Tahar Dahoumane. Web Services and GSM based Smart Home Control System. *International Conference on Applied Smart Systems* (ICASS2018).

[3] Kenneth Araujo, Reginald Best, Devin Heitmueller, Dmitri Tikhonov. *Network access using reverse proxy*. 2005.

[4] Jianhua Zhao, Yongliang Shen. 2001. *An Adaptive PID Control Algorithm.* Journal of Automation.417-420.(In Chinese).

[5] A. Hernandez , J. Urena, J.J. Garcia. 2004. *Ultrasonic ranging sensor using simultaneous emissions from different transducers*. IEEE Transactions on Ultrasonics, Ferroelectrics and Frequency Control.

[6] GB/T3976-2002. *Functional dimensions of school desks and chairs*. China Standards Press.

[7] Digital Light intensity detection module GY-30 for Arduino document from, [online] Available: http://www.uctronics.com/gy-30-bh1750fvi-intensity-digital-light-sensor-module-for-arduino-p-1494.html.

[8] Suzannah K. Helps, Susan Bamford, Edmund J. S, Sonuga-Barke, Göran B. W. Söderlund. 2014. *Different Effects of Adding White Noise on Cognitive Performance of Sub-, Normal and Super-Attentive School Children*. PLoS One

Utilizing SDN to Deliver Maximum TCP Flow for Data Centers

Norah S. Bin Saeed
Department of Computer Engineering, CCIS
King Saud University
Riyadh, KSA
nbinsaeed@ksu.edu.sa

Mohammed J.F. Alenazi
Department of Computer Engineering, CCIS
King Saud University
Riyadh, KSA
mjalenazi@ksu.edu.sa

ABSTRACT

Data centers host tens of thousands of interconnected servers, and they need to move a vast amount of data from one server to another for mirroring and backup purposes. Many new network technologies have been used to provide high throughput for bulk transfers of data in data centers. One of the evolving structures is the software-defined network (SDN), which is a new network paradigm that eases network management by separating the control plane from the data plane. In this paper, we introduce a novel method of utilizing traditional TCP and SDN to deliver maximum flow throughput. We also discuss our evaluation of our new method, MaxFlowTCP, against StandardTCP, ParallelTCP, and MPTCP. The results show that MaxFlowTCP provides higher throughput for the tested topology. Compared to StandardTCP, MaxFlowTCP had 130% better throughput, and compared to ParallelTCP and MPTCP, it had an average of 40% more throughput.

CCS CONCEPTS

• **Networks** → **Programmable networks**; *Data center networks.*

KEYWORDS

Data center, maximum flow, MPTCP, multipath, OpenFlow, SDN

ACM Reference Format:
Norah S. Bin Saeed and Mohammed J.F. Alenazi. 2020. Utilizing SDN to Deliver Maximum TCP Flow for Data Centers. In *2020 The 3rd International Conference on Information Science and System (ICISS 2020), March 19–22, 2020, Cambridge, United Kingdom.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3388176.3388216

1 INTRODUCTION

Data centers play a significant role in any organization's computing landscape. They house the data storage, computing resources, and critical systems that an organization uses to organize, manage, process, store, analyze, and distribute bulk data. This makes the data center a vital asset for everyday operations. The processing and computing of the large volumes of data hosted in data centers like the one shown in Figure 1 will generate enormous data flows that need high throughput to avoid any performance degradation.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388216

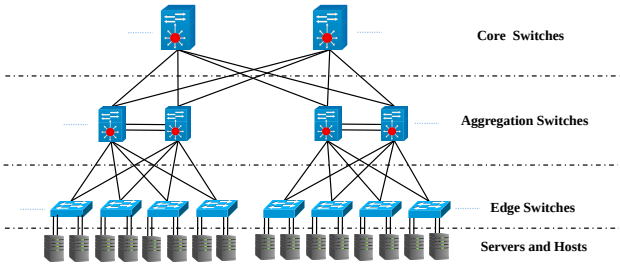


Figure 1: Typical data center architecture

Data centers have evolved rapidly in recent years. Their size in terms of hosted servers is continuously growing to facilitate and serve the increased demand for their services and resources, and modern data centers usually host tens to hundreds of thousands of servers. For example, Facebook's first data center building was located in Prineville, Oregon, and had 1.1 million square feet [29]. In terms of number of servers hosted in most data centers, in July 2013, it was estimated that both Google and Microsoft each hosted around 900,000-1,000,000 servers [12]. This continuing expansion of the size of data centers means more network bandwidth and resources are needed to meet the expected performance.

In addition to high throughput, careful traffic management and policy imposition are crucial in scaled environments like data centers [30]. Using software-defined network (SDN) [31] technology in data centers was motivated by the need for customized routing and traffic engineering and the ability to achieve more scalability and control that cannot be accomplished using traditional networks. The SDN structure separates the control plane from the data plane, and it is used in many network applications, including data centers [19]. The advantages of using SDN in data centers come mainly from its ability to provide network virtualization, abstraction, automation, and flexible management. Many companies have adopted SDN in their data centers, including Google[20] and Microsoft [16].

Multipath TCP (MPTCP) [9] is also one of the evolving protocols used in data centers in recent years to improve data throughput. MPTCP utilizes multiple interfaces in two communicating peers to establish simultaneous sub-connection paths between the two. It can utilize full bisection bandwidth in topologies like dual-homed FatTree and BCube by creating multiple subflows between two servers [18]. In Amazon's EC2 data centers, MPTCP with four

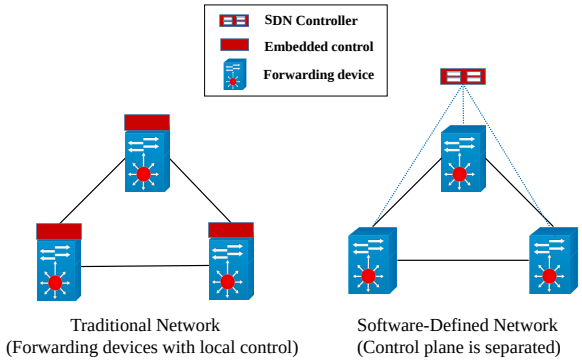


Figure 2: SDN network compared to traditional network [30]

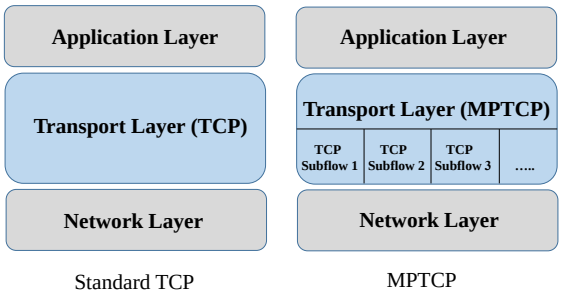


Figure 3: Standard TCP compared to MPTCP

subflows achieves three times the throughput of a single-path TCP (SPTCP) [32].

In this paper, we present a new method named MaxFlowTCP that utilizes traditional TCP and SDN to deliver maximum flow throughput by creating multiple paths between the source and destination peers without the use of MPTCP. We evaluated our method against StandardTCP, ParallelTCP, and MPTCP, and the results showed that the MaxFlowTCP algorithm provided higher throughput for the tested topology.

The rest of this paper is structured as follows: in Section 2 The necessary background for the proposed method is covered, including SDN, maximum flow algorithm, and MPTCP. Section 3 discusses the related work. Section 4 introduces the proposed method, and Section 5 presents the implementation and the evaluation results. Finally, the last section, 6, presents the conclusion and discusses future work.

2 BACKGROUND

In this section, we present an overview of SDN, MPTCP, and the maximum flow problem.

2.1 Software-Defined Networks

SDN is a network structure that aims to make the network more flexible, scalable, and easy to manage. The key idea behind SDN is to separate the control plane from the data plane. This can be done by modifying a centralized control console (the controller) with all decision-making activities without the need to configure every switch or router device in the network. These devices will only be forwarding devices that received commands from the controller instructing them how to handle the packets they receive [31]. This is in contrast to a traditional network, where each individual device needs to be configured separately and each device makes a traffic forwarding decision based on their configuration. Figure 2 shows the difference between an SDN network and a traditional network. OpenFlow [28] is the most widely used SDN standard; it defines how to exchange information between the SDN controller and data plane devices.

2.2 Multipath TCP

Using standard TCP when multiple interfaces are available between two communicating pairs has a significant limitation because it will only use one interface at each end of the communication. On the other hand, MPTCP can utilize multiple interfaces by creating simultaneous subflow connections between the communicating peers. This allows MPTCP to increase resource usage and redundancy and improve total throughput. MPTCP uses the same socket implementation in the transport layer as standard TCP. Figure 3 shows the standard TCP structure compared to MPTCP. Each subflow in MPTCP acts as a single-path standard TCP that transfers the segments divided by the MPTCP packet scheduler [10].In addition to enhancing throughput, MPTCP can provide redundancy and aims to improve network resilience to interface failure [21].

2.3 Maximum Flow Problem

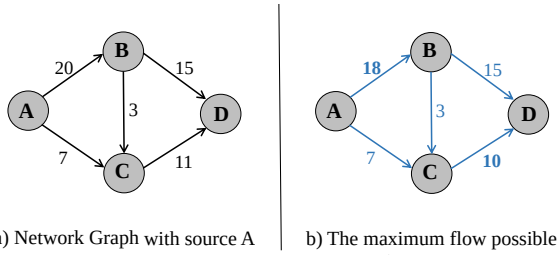
The maximum flow problem is how to find the maximum flow value from a source node S to a destination node D. This concept is essential in all types of networks, including transportation and communication networks [25].The first algorithm created to solve this problem was the Ford–Fulkerson algorithm by Lester R. Ford and Delbert R. Fulkerson [11]. Many methods and algorithms have been proposed over the years to solve this problem, including a shortest augmenting path algorithm by Edmonds and Karp [7], Dinic's algorithm with power estimation [5], the preflow push algorithm by Karzanov [23], the push-relabel algorithm of Goldberg and Tarjan [14], the binary blocking flow algorithm of Goldberg and Rao [13]; and many others.

The network graph is usually represented by connected nodes, with arc links showing the capacity for each link. Figure 4.a shows an example of a flow network with a source node A and a destination node D. figure 4.b shows the maximum possible flow from A to D.

3 RELATED WORK

In this section, we present several approaches used with SDN and multipathing to improve data center bulk data transfer throughput.

In [20], Google presented B4, an SDN based data center architecture that separates the control plane from the data plane to deploy new network control services faster. It balances capacity with application priority by splitting application flows. The implemented



a) Network Graph with source A and destination D

b) The maximum flow possible from A to D

Figure 4: Maximum flow problem example

cost-effective WAN bandwidth has an average of 70% utilization of all links over long time periods, resulting in a twofold to threefold improvement when compared with standard practices.

A Microsoft software-driven WAN (SWAN) was presented in [16]. It is an SDN based method that improves the utilization of inter-data center networks by centrally controlling when and how much traffic each service sends and frequently re-configuring the network's data plane to match current traffic demand. Experiments and simulations have shown that SWAN carried 60% more traffic than then-current practice.

An SDN-based load-balanced multipath routing algorithm was proposed in [22]. It depends on a central controller to collect network state information for directing all traffic flows in the network and making optimized routing decisions. It can better distribute the traffic load and utilize the available bandwidth in a FatTree network.

In [33], a reliable and efficient underlying bulk data transfer service in a geo-distributed data center system was proposed. The model is designed within an SDN architecture and enables dynamic, optimal routing of a distinct segment within each bulk data transfer instead of treating each transfer as an infinite flow. Intermediate data centers are used to temporarily store the segments to alleviate bandwidth contention with more urgent transfers.

In [32], MPTCP was used in data centers to utilize the offered high aggregated bandwidth with multiple paths in the network core. This requires different flows to take different paths, which could not be accomplished using a single-path TCP. They replaced TCP with MPTCP to improve throughput and provide better fairness on many topologies, and their experiment on Amazon's EC2 data centers showed that MPTCP with four subflows achieved three times the throughput of a single-path TCP.

However, The regular MPTCP usually does not handle short flows in data center networks effectively because of the long delay from excessive timeouts. In [24] and [18], two methods were presented to overcome this limitation in standard MPTCP. The first one proposed Maximum MultiPath TCP (MMPTCP), which operates in two phases. First, it randomly scatters packets in the network using a single congestion window to utilize all available paths, which is advantageous to latency-sensitive short flows. Then, after a certain amount of data has been sent, MMPTCP switches to a regular MPTCP mode that can handle long flows efficiently. The second paper proposed a fast coupled retransmission mechanism for MPTCP, which assumed that one path will be congested if packets are out-of-order, even after all data packets have been delivered. If that happens, it will forward packets to another non-congested path and quickly retransmit them.

An SDN-enhanced MPTCP proposed by [17] maximizes throughput in data center L2 networks without adding a lot of overhead. It divides the load between the controller and the host servers. The cooperation from the servers improves the MPTCP subflow routing and dynamically adapts the number of subflows according to the network conditions. The method test results showed a 20% to 30% throughput increase compared to regular MPTCP.

The responsive MPTCP system introduced in [6] overcame two significant limitations of MPTCP: a fixed number of subflows regardless of the actual traffic, which can waste network resources, and the routing of subflows relying primarily on ECMP-based random hashing, which can lead to slower throughput when multiple subflows collide on the same path. It accomplishes this by using a centralized controller for intelligent subflow route calculation and a monitor running on each server for actively adjusting the number of subflows. This allows MPTCP flows to respond to the traffic conditions and continue having higher throughput.

In [34], path diversity in data centers using MPTCP-aware SDN is explored. The SDN controller uses packet inspection to provide deterministic subflow assignments to paths, which provides a new routing mechanism for MPTCP subflows. It can deliver significantly improved performance when connections are not limited by the access links of hosts.

A stochastic load-balanced multipath routing (SLMR) algorithm was proposed in [8]. It considers the stochastic nature of traffic in data centers and tries to achieve optimal load balancing by utilizing the multipath properties of multi-rooted data center networks. It balances traffic among multiple links by minimizing the probability of each link facing congestion.

4 MAXFLOWTCP SYSTEM

In this section, we introduce a system that utilizes a maximum flow algorithm and SDN to provide optimal flow between two servers within a data center.

4.1 MaxFlowTCP Components

In a typical computer network, there are several paths between a sender and a receiver. Traditional TCP/IP protocols use a single path between a sender and receiver. However, this approach suffers from the bottleneck link, which is a constraint on the end-to-end throughput. To tackle this issue, many researchers have proposed multipath solutions for utilizing alternative paths to enhance end-to-end throughput. All multipath solutions relay on k-shortest paths to provide alternative paths, which yields a disjointed path without consideration of maximum flow between the sender and receiver. As a result, these multipath solutions still suffer from the bottleneck problem for each alternative path. In our system, we propose a scheme that relays on a maximum flow algorithm to provide optimal throughput.

This system uses the maximum flow algorithm between the sender and receiver to identify the intermediate switches where

Table 1: Maximum Flow Solution for the Example Network

Link	Flow Value
(H1,S1)	5
(H1,S2)	2
(S1,S2)	2
(S1,H2)	3
(S2,H2)	4

flows are split. Then, it will use OpenFlow to push rules to split flows based on TCP port numbers. We note that traditional routing and forwarding is done based on destination IP addresses. However, for multipath, we will use both port numbers and IP addresses. In the final step, the sender creates multiple TCP connections with the same TCP port numbers used in OpenFlow. Figure 5 shows a general SDN network topology between a pair of devices. When Host 1 sends data to Host 2, the SDN controller determines the intermediate switches using a maximum flow algorithm and then tells Host 1 how many TCP connections it has to create in order to achieve the maximum flow from Host 1 to Host 2.

For example, Figure 6 shows the graph representation of a network example. When the maximum flow algorithm is applied where the source is H1 and the sink is H2, the solution is shown in Table 1. We observe that the flow-in for S1 is 5 using the link (H1,S1) while the flow-out is split links (S1,S2) with a flow value of 2 and (S1,H2) with a flow value of 3. Since there is a split into two flows at S1, we need to create two TCP connections, TCP-Conn-1 and TCP-Conn-2, from H1 to S1, as shown in the figure. For S1, we need to add two OpenFlow rules to forward the incoming packets from H1 into S2 and H2 based on TCP port numbers. In addition, we observe that the flow-in for S2 is 4 using the two links, link (H1,S2) and link (S1,S2), while the flow-out is 4 for the link (S2, H2). For S2, we need to add OpenFlow rules to forward the incoming packets from H1 into S2 and H2 based on TCP port numbers. Since the flow from the link (H1,S2) does not split, we only need one TCP connection for that particular link, which is denoted as TCP-Conn-3. As a result, for this specific example, the number of required connections is three.

5 EVALUATION AND DISCUSSIONS

In this section, we will present our experiment and its parameters. Then we will present the evaluation of MaxFlowTCP and discuss the performance results.

5.1 Experiment Topology and Parameters

In this section, we will present our experiment and its parameters. To evaluate the MaxFlowTCP method, Mininet 2.3.0d4 emulation was used on a Ubuntu 16.04 host that had a six-core 2.2 GHz processor with 16GB of RAM. Mininet connects virtual Linux hosts with a given topology. In the emulation topology, two OpenvSwitch switches were used to connect two hosts A and B. Each host was connected to both switches, and the data traffic between the two hosts was generated using iperf. Each evaluation test had five runs,

Table 2: Default Emulation Parameters

Parameter	Values
Emulator	Mininet 2.3.0d4
Operating System	Ubuntu 16.04
CPU	six-core 2.2 GHz
Memory	16GB
TCP Congestion	CUBIC
Virtual Switches	OpenvSwitch 2.5.5
Number of Runs	Five for each method
Experiment Duration	30 seconds
Sampling Rate	One sample per second
Link Bandwidth	H1 - S1 link 50 Mbps
	H1,S2 link 20 Mbps
	S1,S2 link 20 Mbps
	S1,H2 link 30 Mbps
	S2,H2 link 40 Mbps

with a duration of thirty seconds of data flow. The throughput sampling rate was one per second. The evaluation parameters and the test topology are shown in Table 2 and Figure 7, respectively.

Before testing the proposed MaxFlowTCP method, we first examined multiple TCP congestion control methods that are suitable for data centers in the emulation topology in order to choose the best performing TCP variants that would be used in the rest of the evaluation. The TCP variants chosen were CUBIC [15], BIC[27], DCTCP [1], BBR [4], HTCP[26], and NV [3]. Table 3 shows the throughput for each of the TCP variants.

As shown in Table 3 and Figure 8, the throughput results for BIC, CUBIC, DCTCP, BBR, and HTCP were very close. From these results and according to [2], we chose CUBIC as the congestion control method.

5.2 MaxFlowTCP Evaluation

To evaluate the MaxFlowTCP method, we compared its performance against three other methods. In each method, data is generated using iperf and sent from host A to host B with five runs for each one. The number of runs is satisfying, and we do not have to increase it since the data variability is very low, as we will see later in the data throughput comparison. The evaluated methods are as follows:

(1) StandardTCP: Application data is transferred using *only* one TCP connection regardless of the number of available interfaces.
(2) ParallelTCP: For each interface, one TCP connection is created to transfer application data. These connections operate in parallel.
(3) MPTCP: Application data is transferred using an MCPTCP connection, which internally creates multiple sub TCP connections for each available interface.
(4) MaxFlowTCP: For each interface, multiple TCP connections are created to transfer application data. These connections operated in parallel, while the number of connections depended on the flow value of the MaxFlow algorithm.

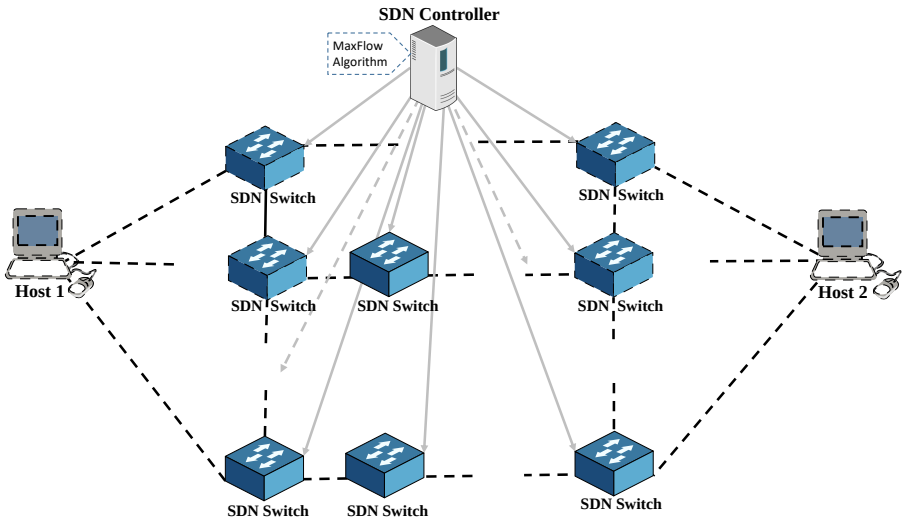


Figure 5: MaxFlowTCP system

Table 3: Throughput for Different Congestion Control Variants

TCP Variants	Total Data		Throughput	
	Average (Mbps)	*Standard Deviation*	*Average (Mbps)*	*Standard Deviation*
CUBIC	858.54	14.33	27.58	0.50
BIC	922.32	8.88	27.79	0.28
DCTCP	911.88	14.26	27.56	0.49
BBR	830.77	16.64	27.53	0.58
HTCP	917.61	7.86	27.60	0.27
NV	803.49	14.89	26.59	0.51

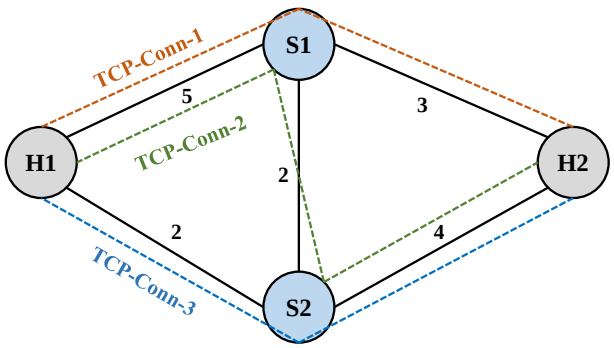


Figure 6: Example topology

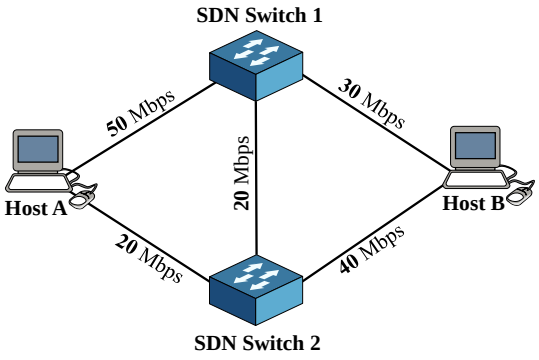


Figure 7: Mininet evaluation topology

In each method, the throughput from Host A to Host B was observed. Table 4 shows the total data and throughput results for each method. Figure 9 shows the average throughput for each method. The error bars in the figure represent the standard deviation with 95% confidence interval. As shown in the figure, MaxFlowTCP started at 50 Mbps in the first two seconds, then it gave a steady throughput average of 63 Mpbs during the entire simulation. MaxFlowTCP had the highest throughput of the four methods, and it could almost reach the maximum possible throughput by using a maximum flow algorithm that efficiently utilized all of the available links.

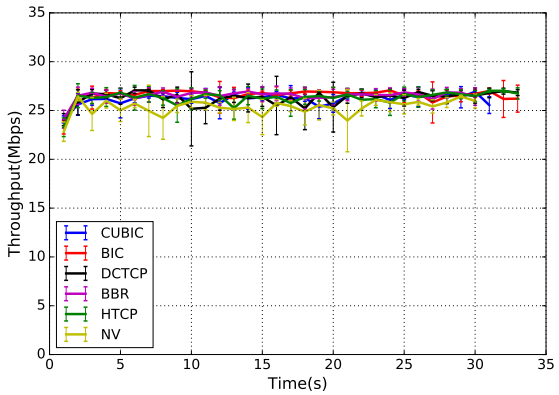


Figure 8: Throughput average in different TCP congestion control variants

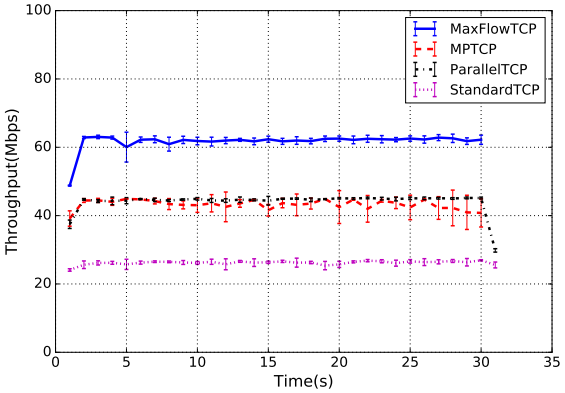


Figure 9: Throughput average in StandardTCP, MPTCP , ParallelTCP, and MaxFlowTCP

ParallelTCP and MPTCP showed nearly identical results. They both yielded around 45 Mbps of average throughput during the whole simulation. They had better performance compared to StandardTCP because they each established two connections in the two available links. However, they provided lower throughput than MaxFlowTCP because they did not utilize all of the available bandwidth in the network. MaxFlowTCP had 40% more throughput, on average, when compared to ParallelTCP and MPTCP methods.

Finally, StandardTCP gave an average throughput of around 27 Mbps during the whole simulation, which is considered the lowest throughput among the studied methods because it used only one link to transfer the data and did not benefit from the availability of the other link. Compared to StandardTCP, MaxFlowTCP had 130% better throughput.

6 CONCLUSIONS AND FUTURE WORK

For any organization, the data center is a crucial asset that hosts vital systems needed for critical daily operations. A data center network requires a practical and efficient method of processing and computing the bulk data it generates. SDN is a technology that aims to make network configuration programmable and dynamic for better management and scalability, and the use of SDN technology in data centers has created significant improvements in different aspects.

In this paper, we proposed a new method, called MaxFlowTCP, that utilizes SDN with traditional TCP to deliver maximum flow throughput in data centers by creating multiple paths between the source and destination peers. The results from the test topology showed that MaxFlowTCP was a significant improvement when compared to StandardTCP, MPTCP, and ParallelTCP. It outperformed the other methods because it utilizes the available links bandwidth by using the maximum flow algorithm to reach almost the maximum throughput.

Future work aims to implement a dynamic MaxFlowTCP SDN system that can work on any data center topology. We also plan to evaluate MaxFlowTCP in different data center typologies, such as FatTree and others. In addition, we plan to use an ns-3 simulation to better evaluate MaxFlowTCP's performance.

7 ACKNOWLEDGMENTS

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through Research Project No. R5-16-03-03.

REFERENCES

[1] Mohammad Alizadeh, Albert Greenberg, David A Maltz, Jitendra Padhye, Parveen Patel, Balaji Prabhakar, Sudipta Sengupta, and Murari Sridharan. 2011. Data center tcp (dctcp). *ACM SIGCOMM computer communication review* 41, 4 (2011), 63–74.

[2] Tabinda Ashraf, Noor ul Sabah, and Mohammad Junaid Arshad. 2017. Comparative Study of TCP Protocols : A Survey.

[3] L Brakmo. 2010. TCP-NV: Congestion avoidance for data centers. In *Linux Plumbers Conference*.

[4] Neal Cardwell, Yuchung Cheng, C. Stephen Gunn, Soheil Hassas Yeganeh, and Van Jacobson. 2016. BBR: Congestion-Based Congestion Control. *Queue* 14, 5, Article 50 (Oct. 2016), 34 pages. https://doi.org/10.1145/3012426.3022184

[5] Yefim Dinitz. 1970. Algorithm for Solution of a Problem of Maximum Flow in Networks with Power Estimation. *Soviet Math. Dokl.* 11 (01 1970), 1277–1280.

[6] J. Duan, Z. Wang, and C. Wu. 2015. Responsive multipath TCP in SDN-based datacenters. In *2015 IEEE International Conference on Communications (ICC)*. 5296–5301. https://doi.org/10.1109/ICC.2015.7249165

[7] Jack Edmonds and Richard M. Karp. 1972. Theoretical Improvements in Algorithmic Efficiency for Network Flow Problems. *J. ACM* 19, 2 (April 1972), 248–264. https://doi.org/10.1145/321694.321699

[8] O. Fatmi and D. Pan. 2014. Distributed multipath routing for data center networks based on stochastic traffic modeling. In *Proceedings of the 11th IEEE International Conference on Networking, Sensing and Control*. 536–541. https://doi.org/10.1109/ICNSC.2014.6819683

[9] A. Ford, c. Raiciu, M. Handley, and O. Bonaventure. 2013. *TCP Extensions for Multipath Operation with Multiple Addresses*. RFC 6824. IETF. https://tools.ietf.org/html/rfc6824

[10] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure. 2013. TCP extensions for multipath operation with multiple addresses. RFC 6824 (Experimental). http://www.ietf.org/rfc/rfc6824.txt

[11] Lester Randolph Ford and Delbert R Fulkerson. 2009. Maximal flow through a network. In *Classic papers in combinatorics*. Springer, 243–248.

[12] A. Ghiasi and R. Baca. 2014. Overview of Largest Data Centers. http://www.ieee802.org/3/bs/public/14_05/ghiasi_3bs_01b_0514.pdf. [Online; accessed 8-Septemper-2019].

[13] Andrew V. Goldberg, Satish Rao, and Satish Rao. 1998. Beyond the Flow Decomposition Barrier. *J. ACM* 45, 5 (Sept. 1998), 783–797. https://doi.org/10.1145/290179.290181

[14] Andrew V. Goldberg and Robert E. Tarjan. 1988. A New Approach to the Maximum-flow Problem. *J. ACM* 35, 4 (Oct. 1988), 921–940. https://doi.org/10.1145/48014.61051

Table 4: Throughput in StandardTCP, MPTCP , ParallelTCP, and MaxFlowTCP

Methods	Total Data		Throughput	
	Average (Mbps)	*Standard Deviation*	*Average (Mbps)*	*Standard Deviation*
MaxFlow	1994.75	36.49	63.76	1.08
MPTCP	1413.12	38.31	45.28	1.33
ParallelTCP	1470.46	9.16	46.17	0.23
StandardTCP	858.54	14.33	27.58	0.50

[15] Sangtae Ha, Injong Rhee, and Lisong Xu. 2008. CUBIC: A New TCP-friendly High-speed TCP Variant. *SIGOPS Oper. Syst. Rev.* 42, 5 (July 2008), 64–74. https://doi.org/10.1145/1400097.1400105

[16] Chi-Yao Hong, Srikanth Kandula, Ratul Mahajan, Ming Zhang, Vijay Gill, Mohan Nanduri, and Roger Wattenhofer. 2013. Achieving High Utilization with Software-driven WAN. *SIGCOMM Comput. Commun. Rev.* 43, 4 (Aug. 2013), 15–26. https://doi.org/10.1145/2534169.2486012

[17] A. Hussein, I. H. Elhajj, A. Chehab, and A. Kayssi. 2017. SDN for MPTCP: An enhanced architecture for large data transfers in datacenters. In *2017 IEEE International Conference on Communications (ICC)*. 1–7. https://doi.org/10.1109/ICC.2017.7996653

[18] J. Hwang, A. Walid, and J. Yoo. 2018. Fast Coupled Retransmission for Multipath TCP in Data Center Networks. *IEEE Systems Journal* 12, 1 (March 2018), 1056–1059. https://doi.org/10.1109/JSYST.2016.2582527

[19] R. Hwang, H. Tseng, and Y. Tang. 2015. Design of SDN-Enabled Cloud Data Center. In *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*. 950–957. https://doi.org/10.1109/SmartCity.2015.193

[20] Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, et al. 2013. B4: Experience with a globally-deployed software defined WAN. In *ACM SIGCOMM Computer Communication Review*, Vol. 43. ACM, 3–14.

[21] Mohammed J.F. Alenazi. 2019. Evaluating Multipath TCP Resilience against Link Failures. *The ISC International Journal of Information Security* 11, 3 (2019), 113–122. https://doi.org/10.22042/isecure.2019.11.0.15

[22] E. Jo, D. Pan, J. Liu, and L. Butler. 2014. A simulation and emulation study of SDN-based multipath routing for fat-tree data center networks. In *Proceedings of the Winter Simulation Conference 2014*. 3072–3083. https://doi.org/10.1109/WSC.2014.7020145

[23] Alexander Karzanov. 1974. Determining the maximal flow in a network by the method of preflows. *Doklady Mathematics* 15 (02 1974), 434–437.

[24] M. Kheirkhah, I. Wakeman, and G. Parisis. 2016. MMPTCP: A multipath transport protocol for data centers. In *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*. 1–9. https://doi.org/10.1109/INFOCOM.2016.7524530

[25] Bharat Kinariwala and A. G. Rao. 1977. Flow Switching Approach to the Maximum Flow Problem: I. *J. ACM* 24, 4 (Oct. 1977), 630–645. https://doi.org/10.1145/322033.322042

[26] Douglas Leith and Robert Shorten. 2004. H-TCP: TCP for high-speed and long-distance networks. In *Proceedings of PFLDnet*, Vol. 2004.

[27] Lisong Xu, K. Harfoush, and Injong Rhee. 2004. Binary increase congestion control (BIC) for fast long-distance networks. In *IEEE INFOCOM 2004*, Vol. 4. 2514–2524 vol.4. https://doi.org/10.1109/INFCOM.2004.1354672

[28] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. 2008. OpenFlow: Enabling Innovation in Campus Networks. *SIGCOMM Comput. Commun. Rev.* 38, 2 (March 2008), 69–74. https://doi.org/10.1145/1355734.1355746

[29] Team Nuggets. 2017. The 6 largest data centers in the world. https://www.cbtnuggets.com/blog/technology/data/the-6-largest-data-centers-in-the-world. [Online; accessed 8-Septemper-2019].

[30] B. A. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka, and T. Turletti. 2014. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *IEEE Communications Surveys Tutorials* 16, 3 (Third 2014), 1617–1634. https://doi.org/10.1109/SURV.2014.012214.00180

[31] ONF. 2012. *Software-Defined Networking: The New Norm for Networks*. Technical Report. Open Networking Foundation. https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

[32] Costin Raiciu, Sebastien Barre, Christopher Pluntke, Adam Greenhalgh, Damon Wischik, and Mark Handley. 2011. Improving datacenter performance and robustness with multipath TCP. In *ACM SIGCOMM Computer Communication Review*, Vol. 41. Citeseer, 266–277.

[33] Y. Wu, Z. Zhang, C. Wu, C. Guo, Z. Li, and F. C. M. Lau. 2017. Orchestrating Bulk Data Transfers across Geo-Distributed Datacenters. *IEEE Transactions on Cloud Computing* 5, 1 (Jan 2017), 112–125. https://doi.org/10.1109/TCC.2015.2389842

[34] Savvas Zannettou, Michael Sirivianos, and Fragkiskos Papadopoulos. 2016. Exploiting path diversity in datacenters using MPTCP-aware SDN. *2016 IEEE Symposium on Computers and Communication (ISCC)* (2016), 539–546.

Chapter 5

Computer and Information Science

Assessing the Information Services on National Archives Websites: A Case Study of the Website of the National Center for Documentation and Archives in Saudi Arabia

Hind Alghanem
Imam Mohammed Bin Saud Islamic University- CISC
Riyadh- Saudi Arabia
966591106641
haalghanem@imamu.edu.sa

ABSTRACT
This paper assesses the information services available on the National Center for Documentation and Archives (NCAR) website in Saudi Arabia. It uses as its criteria the UK Archive Service Accreditation Standard specifically the third section, which deals with stakeholders, their experiences, and the accessibility of services. In general, ease of access to the services of the NCAR website is demonstrated to meet a high standard, basic information about NCAR informatics services is available at a good standard, accessibility of NCAR services on the website meets an acceptable standard, the availability of interactive services through the NCAR achieves a low standard, and the NCAR meets a generally acceptable standard for information retrieval services. Overall, the availability of information services on the NCAR website is at an acceptable level.

CCS Concepts
• **Human-centered computing→ Accessibility design and evaluation methods.**

Keywords
Accessibility; national archives; information services.

1. INTRODUCTION
Archives, as information institutions, keep abreast of the latest developments in information and communications technologies (ICTs) and invest in these developments to enable the public to access and benefit from their own information resources. They have created their own websites and made good use of their potential to provide information services and reach the largest number of actual and potential beneficiaries by marketing their services through these websites. In this way they make their information resources available not only to their local audience but also to the global community. Their web portals are among the electronic information resources generated by the information and communication revolution.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388178

Many projects have been undertaken globally with a view to developing national archives. The aims of these projects include keeping pace with developments in ICT and the internet, meeting the requirements of the knowledge society, sharing archive resources, and providing researchers with access to services, regardless of where they are.

National archives are any institution that specializes in the collection and preservation of documents of historical or archival value to the state. They are responsible for organizing and preparing research tools, and making documents available for viewing and reproduction in conformance with the applicable rules and regulations. They are also responsible for transmitting historical information to the public [1]. There are significant differences between the information services provided by national archives in the advanced countries of Europe and North America and those in other countries, especially the Arab countries, in terms of the investment in ICTs and the diversity and effectiveness of services.

The use of digital systems in national archives has proved beneficial in a number of ways. Examples include the following:

- assisting in the preservation of documents, especially damaged ones;
- making documents available without relying on the assets;
- revealing details that cannot be seen directly in a document with the use of ultraviolet light during scanning;
- facilitating retrieval according to subject, date, place, person, and entity;
- ensuring easy and rapid retrieval for more than one person at the same time; and
- providing accessible information with a wide range of options for copying, printing, loading, and so on [2].

A wide variety of information services are available on national archives' websites, the most important of which are reviewed below. An online public access catalogue service is a database collection of bibliographical records that describe archival materials owned and used by an automated archive system. It allows users to print and upload records or send them to an email account.

Reference services are provided in a number of different ways. There are asynchronous services, such as a 'Contact Us' link, that simply use email or web forms. Sometimes queries are answered via links such as 'Ask Us', 'Ask an Archivist', 'Ask Me', or 'Ask a Question'. Frequently asked questions (FAQs) functions and chat services are also used. These services benefit from certain important Web 2.0 technologies, such as instant messaging and

chat [3]. There are also virtual exhibitions. Alerting services are offered via subscriptions to a newsletter and really simple syndication (RSS) feeds. Marketing and promoting awareness of the importance of national archives is a diverse service that can be linked with certain archive services such as educational services, visit requests, reference services and investment in social media applications, such as Facebook, Twitter and YouTube. A Facebook page is a promotional channel that can be invested in to motivate visitors to engage with the activities and services of the national archives; it encourages them to participate and to express their views on various historical and cultural topics [4]. Moreover, an archive's products such as its holdings, training courses and educational services can be marketed via YouTube [5]. National archives are particularly interested in providing educational services, whether by creating special education programmes for school students and teachers or by offering training programmes to introduce document specialists to the nature of documents; methods of organizing, archiving, and retrieving them; and modern techniques used in their management and control [6].

Eager to keep abreast of developments in the field of ICT, the National Center for Documentation and Archives in Saudi Arabia (NCAR), like other information institutions, has established its own website to exploit the potential of the web to provide better services [7].

In light of the importance of national archive websites in research, scientific and educational activities, and the development of the knowledge society, in addition to their role in providing services to both local and global communities, the need arose to assess these websites' services using the criteria established in this field and in previous studies; that assessment is the goal of this study. The importance of this study stems from the significant role national archives play in managing and collecting records and archives of government agencies, and from the need to promote their use among the public both locally and globally. This study is one of very few that benchmarks national archives against international standards. The standards concerned are British standards published in June 2018. They set out accepted good practice standards for obtaining international accreditation in this field, thus promoting and supporting the development of archival services. Previous studies of Arab national archives and the information services available on their websites have not used such a benchmark. Therefore, this study contributes to filling the gaps in this field. It is hoped that this field will be opened to researchers in the future to address in greater depth many of the factors relating to accreditation standards for the services of national and international archives.

This paper assesses the information services available on the website of the NCAR in Saudi Arabia. Its objectives include the following:

- identifying the ease of access to the services of the NCAR website;
- identifying the availability of basic information, such as the centre's policies and working hours, via the website;
- assessing the accessibility of services via the website of the national archives;
- identifying the availability of interactive services; and
- identifying the availability of information retrieval services.

2. RELATED WORK

Reference has been made in the literature to the dearth of Arab studies in this field. Many studies have been undertaken on topics similar to that of this study. They include work by Ibrahim [8], which assessed 14 digital archive websites according to criteria such as content, services, form and design, and usability. The results revealed that seven archive websites provided access to certain documents online – namely, those of Tunisia, Japan, India, the United States (US), the United Kingdom (UK), Jamaica and Germany. The number of documents available on these websites varied. The US archives had the greatest number of documents available, followed by the UK archives. Moreover, 71.4% of all the websites provided indexes and databases of documents, 35.7% explained the conditions for ensuring the confidentiality of personal information and the existence of means of protection, 14.2% stated the options for use and browsing, 42.8% included maps illustrating the various sections of the website, 42.8% made use of a special search engine, 50% could be accessed via popular online search engines, 35.7% offered links to other national archives, 50% provided links to important institutions in the field of document and archive services, 85.7% provided lists of publications produced by the archive, and 92.8% offered a service for answering questions and present FAQs. In addition, the study revealed weaknesses in the level of service of these archives in general, including a lack of investment in the most advanced technology for website construction and design. Most of the websites did not specify their objectives or date of establishment and did not indicate the date on which they had last been updated.

Essawy's study [2] of national archives and their new role in the information society included a case study on the National Archives of Egypt. It identified the beneficiaries of the archive's services, presented the most important problems facing the Egyptian archives, and clarified details about the services offered. In addition, El-Sherif's research [9] examined the attitudes of national archives in advanced countries and ways to exploit their websites to provide information services in a sophisticated manner to meets the needs of stakeholders. The study also identified the attitudes of the Arab archives to providing these services and making documents available to the public and to Arab researchers. This research focused on a range of digital information services provided by national archives on the web – for example, an online public access catalogue (OPAC) search service, archival databases services, electronic reference services, current awareness services, and virtual exhibitions. The study sample consisted of 10 archives and used the descriptive analytical method. The results demonstrated that most of these services were fully provided in the US, UK, and Australian archives, while only a few of them were provided in the archives of India, Argentina, Egypt, and the United Arab Emirates.

Millar [10] discussed the basic principles of archive services. He stated that the fundamental principles of accountable and reliable archive services are to ensure that archives are preserved and protected by their confidential values and to ensure that archives are as widely available as possible. The availability of services must be ensured in a responsible and structured manner, respecting not only the documentary evidence itself but also the individuals and groups who created it and the people who may wish to access it. The author stated that to understand the nature of an archive service, it is necessary to identify the basic duties and skills of the archive specialist. He identified the main challenges and stressed the need to find a balance between the right to access documents and protection of the rights of others, to ensure that their personal information is protected from illegal use. He also examined the need to provide archival services to the community. Ngoepe and Ngulube [11] assessed the extent to which the South African National Archives and Records Service

(NARS) succeeded in making archival material accessible to the public, promoted and their use by the audience , and identifying outreach programmes to improve the overall image of the archive and to promote the awareness and use of archives. A 2009 survey made use of a targeted sample and concluded that there was a need to enhance the overall image of the NARS and the use of archives through strong outreach programmes.

Nengomasha and Nyanga [12] examined the conditions that guided the provision of services in the National Archives of Namibia and how the latter complied with the International Council on Archives (ICA) Code of Ethics and its Universal Declaration on Access to Archives. The study population included researchers, members and staff of the National Archives of Namibia. The study found that the National Archives of Namibia did not have a programme to strengthen its activities and did not fully utilize information technology and social media to enhance access to its collections. A prolonged closure period of up to 30 years; accumulations of orders and descriptions; and a lack of clarity in response, confidentiality and privacy issues were some of the challenges identified. The authors made a number of recommendations, including the development of clear guidelines on response, confidentiality and privacy; revision of the National Archives Act to reduce the closure period; and the use of ICTs and social media to enhance access to archive collections.

Chaterera's [13] study sought to develop a framework to access and use the documentary heritage in the National Archives of Zimbabwe (NAZ). Although access and use are the reasons for the existence of national archival institutions, the level of use of the NAZ had long been low. The researcher therefore investigated the question of bibliographic, intellectual and physical access to the archive. The study made use of observation and interviews to collect the empirical evidence necessary to develop a framework for accessing and using documentary heritage in the NAZ. The results demonstrated that the NAZ website, as a public information resource centre, was threatened by many obstacles hindering access to and use of the archive's documentary heritage. These obstacles included the lack of a national policy on access to public archives, the lack of an institutional access policy, the lack of a standing committee on access to and use of archives, the lack of a budget, the increased accumulation of untreated archives, and incorrect perceptions about which members of the public make use of the NAZ and its services. There were also problems relating to access constraints imposed by legislation, limited use of digital technology, and a failure to use media and Web 2.0 technologies. The researcher provided a framework to enhance access to and use of the archives to serve as a baseline on which architects could reflect and improve their practices.

Other studies have been interested in the investment by national archives in Web 2.0 applications, such as the study by Sharif [14], which addressed Web 2.0 applications in the US National Archives as a guideline for Arab archives, since Arab archives have not benefited from Web 2.0 applications. Sawy's study [6] described and analysed the effects of Web 2.0 on archives and presidential libraries websites , thus determining the extent to which archival institutions have benefitted from these applications in modernizing the information services they provide and increasing the interaction between archive staff and the public. As a result of Sawy's study , archives have started to invest in these applications to develop their services and to become acquainted with a wider range of opinions and ideas in matters related to archive policy, Sawy found almost no presence of Arabic archives on Web 2.0 sites . Al-Labban's study [4] reviewed the use of Facebook by Arab and foreign national archives. It found that foreign national archives did a better job of interacting via Facebook than Arab national archives did. It also found that Facebook contributed to the promotion of an archive's services, attracted visitors, allowed for knowledge sharing, and enhanced the knowledge environment. Research by Nada [5] assessed national archives' channels on YouTube. It found that the YouTube channel of the US National Archives ranked first in terms of the numbers of subscribers, videos and views. It also identified the Australian National Archives' channel as the first YouTube channel established by a national archive.

Another study by Nada [15] examined the presence of national archives, libraries and presidential museums on Twitter. It is an analytical study that explained what services Twitter can offer national archives and their beneficiaries. It found that most national archives lack specific criteria and a clear policy on the use of Twitter. The exception was the US National Archives, which did have a strategy and a clear and published policy in relation to Twitter. Hager's study [16] examined the use of Facebook by archives and concluded that Facebook was a successful social media tool for linking archives and the public, due to its popularity.

The review of the previous studies demonstrates the importance of the national archives and their effective role in managing and collecting documentary records of government agencies and promoting their use by the audience of beneficiaries at the local and global levels. The review also reveals the problems and difficulties faced by these institutions.

Elements addressed by the previous studies align with the current study as follows:

- Previous studies have shown the importance of national archives and their new role in the information society. The current study agrees with them in focusing on studying the information services provided by these archives.
- Those studies have shown there is a global and Arabic interest in information services provided by national archives and have made clear the need to invest in various web technologies, such as websites and Web 2.0 applications, to enhance access to archives' services for all categories of stakeholders.
- Many of the recommendations and results of previous studies justify the current study's need to assess the services of national archives.
- The current study benefits from previous studies in that they crystallized the study problem and clarified the literature related to the subject of the study. They also aided in identifying the appropriate research method and in preparing a research tool that fits the current study, as well as in linking the results of previous studies with the current study.

The current study differs from previous studies in some aspects, such as in its aim to assess the information services available on the NCAR website in Saudi Arabia. In addition, it uses international standards – the UK Archive Service Accreditation Standards – to assess those services.

3. METHODOLOGY

This study relies on two approaches: the case study approach, to assess the information services available on the NCAR website, and the content analysis approach. The nature of this study requires the use of this approach, as it collects information directly from the NCAR website. This approach is suitable for

such studies because it allows the research to be conducted without the need for direct contact with human resources. To perform content analysis, the researcher chooses a specific medium such as a website and systematically collects data from this source.

A checklist for services of national archive websites was designed making use of the 2018 UK Archive Service Accreditation Standard – specifically the third section relating to stakeholders and access to services.

The checklist includes the following five criteria for assessing the information services available on the NCAR website:

- easy access to services;
- provision of basic information about the services provided by the NCAR;
- accessibility to the centre's services on the website;
- interactive services; and
- information retrieval services.

4. UK ARCHIVE ACCREDITATION STANDARDS

British standards were brought out in June 2018. They set out accepted good practice standards for obtaining international accreditation in this field, thus promoting and supporting the development of archival services. They are divided into three sections: organizational quality; collections; and stakeholders and stakeholder expertise and access to services. This study is primarily interested in the third section, which relates to the accessibility of national archives services, including the following:

i) Service access policies: The most important requirements in this area are that the archive should have a clear policy about accessibility of services and should determine and reinforce the means of access for all stakeholders, in proportion to the organization's mission statement and the nature and size of its collection. The policy must be approved by senior management or the appropriate delegated authority.

ii) Service access plans: The most important requirements in this area are that the archive service demonstrates a good understanding of the needs of the community it serves. It must also have detailed plans to meet the requirements of providing services to stakeholders and to continuously improve service provision. The plans must be appropriate to the organization's mission statement and the nature and size of its collection, this includes two conditions:

- The archive service should understand the community and have effective ways to collect, analyse and evaluate information about the community's needs and interests of current and potential stakeholders.
- The archive service must be have plans to continuously improve its services and its availability to respond the specific needs and interests of its community; and these plans must implemented and actively reviewed.

iii) Procedures for service access and their activities: The most important requirements are that the archive service provides access to its holdings and has a variety of ways to reach its collections and interact with them. It should deliver clear and practical information about how to access services and collections, should respond to the needs of its community, and should protect copyright, privacy and other legislations ,this includes three conditions:

- Appropriate access to archive collections and services, both on-site and off-site.
- Effective access procedures for all stakeholders.
- A variety of means of accessing archive collections and services, in proportion to the mission statement of the organization and the nature and size of its collections [17], [18], [19].

5. RESULTS AND DISCUSSION

This section presents the results of the analysis related to the research questions. It comprises a description of the data, the research questions, and the results. To facilitate the interpretation of the results, the level of the answers to the checklist items was measured on the basis of weightings assigned to the various alternatives (available = 3, somewhat available = 2, unavailable = 1).

5.1 Easy Access to Services through the NCAR Website

Table 1. Easy access to NCAR services

Items	Average
• The website can be accessed using popular search engines.	3
• Information services are easily accessible via the website.	3
• Page links are visible from the main page.	3
• Visitors can move from page to page and link to another page easily, without bewilderment or loss.	3
• Access to services does not require subscription or passwords.	3
• A map of the website is provided.	1
• It is available 24 hours	3
• Quick access lists	1
Overall average	2.5

Table 1, which presents the ease of access to the services on the NCAR website, demonstrates that the averages representing the availability of these services are generally high,these indicating the availability of most features that achieve easy access to the archive services.

In addition, the table demonstrates that the lowest averages were 1.00, representing the lack of quick access lists and the lack of a map or a directory of the website despite their importance in facilitating access to services. In general, ease of access to the services of the NCAR website was demonstrated to be of a high standard, with an average score of 2.5.

5.2 Basic Information about NCAR Informatics Services

Table 2. Basic information about NCAR informatics services

Items	Average
• A welcome message appears on the services pages.	3
• Site objectives and tasks	3
• Target audience	1
• Means of communication	3

• Hours of operation’	1
• Map of the geographic location of the NCAR	1
• Information about the NCAR staff	1
• NCAR’s collections and methods of organizing them	2
• Privacy policy	3
• Legislation and ethical laws	1
• Information on NCAR policies	2
• Service policies are reviewed regularly	2
• Services guide	1
• Information about organizations NCAR collaborates with	3
• News and events	3
Overall average	2

Table 2, which presents the availability of basic information about NCAR informatics services, demonstrates that the availability of these information services is generally acceptable.

In addition, the table demonstrates that information about the centre's collections and methods of organizing them and information about its policies achieved an average score of 2.00, indicating that while information was provided, it was not sufficient. Furthermore, the lowest average (1.00) indicates a lack of availability of information on legislation and ethical laws, services guidance, and target audience, although these items are considered essential for the provision of information services. In general, the availability of basic information about NCAR informatics services achieves a good standard average of 2.0.

5.3 Accessibility of NCAR Services on the Website

Table 3. Accessibility of NCAR services on the website

Items	Average
• Guidance services to deal with NCAR services and resources	2
• A reference service	2
• Website provides links to other websites of interest to users	3
• Information about the NCAR's agenda of activities	3
• Display of NCAR publications	1
• Web 2.0 applications	2
• The current awareness service	2
• Different formats to access content	1
• Really simple syndication (RSS)	1
• Virtual exhibitions	2
• Design of the website enables easy use by disabled people.	2
• A children’s page	1
• Community education, awareness, and marketing of NCAR services	2
• Website information is regularly reviewed and updated	1
Overall average	1.8

Table 3 presents scores for the accessibility of the NCAR's services on the website on the basis of a set of indicators. It demonstrates that the average scores for these indicators vary widely.

It is clear that many services are available to some extent, such as guidance services related to NCAR’s services and resources; Web 2.0 applications; the current awareness service; and community education, awareness and marketing of NCAR services. However, these services were not sufficiently effective. In addition, the NCAR website lacks many services: for example, it does not identify its publications, it lacks an RSS service (although it is a modern technique for maintaining public awareness) and it lacks a children's page. Archive services should include a page and events for children and school students to attract them and link them to their national heritage.

In general, the accessibility of the NCAR's services on the website was at an acceptable level, with an average score of 1.8.

5.4 Interactive Services

Table 4. Interactive services

Items	Average
• User feedback form	1
• Communication service	3
• Ask the archivist	1
• Usable interfaces	2
• Participation in research, scientific and educational activities	1
• Educational programmes	1
• Research service in document collections	1
• Frequently asked questions	1
• Assessment of current and potential needs of the community	1
• Visitor page where users can record their comments and see others' comments	1
• Referendum to identify the opinions of users	1
Overall average	1.3

Table 4 demonstrates that the average scores for the availability of interactive services on the NCAR website are generally low, indicating that most of these services are not available.

- The website lacks many interactive services, including the following:
- an Ask the Archivist service to enable communication with a document specialist, although this is important as a basis for providing a digital reference service;
- participation in research, scientific and educational activities, which is part of community service as well as indirect marketing of the NCAR;
- educational programmes for students and teachers and educational projects in archive field; and
- a research service in document collections, which is an essential service in the knowledge society.

Further interactive services that are lacking include a set of frequently asked questions. Many archives and other websites provide such a link, because it saves much effort and time for both visitors and archival staff. Moreover, this service prevents users from re-asking the same questions. Also lacking is a survey to learn the opinions of users, despite the importance of this service to identify the level of satisfaction of visitors, and thus the extent to which NCAR's objectives are being achieved. Such surveys also identify the strengths and weaknesses of provided services, driving improvements in services.

In general, the availability of interactive services through the NCAR website achieved an average score of 1.3, which represents a low standard.

5.5 Information Retrieval Services

Table 5. Information retrieval services

Items	Average
• Online public access catalogue (OPAC)	**1**
• Links to retrieve electronic documents	3
• Link to search in the databases of the NCAR's holdings	**1**
• Query service about documents with individual specifications	3
• Query service about request status	3
• Search service in the NCAR library	**1**
• Internal search engine	3
• Service to request documents and the options to deal them	3
• Links to relevant websites	**1**
Overall average	2

Table 5 shows that the average scores relating to the availability of information retrieval services on the NCAR website were generally good, although many necessary retrieval services were not available. Services that were lacking included an OPAC, which is important to facilitate quick access to document collections; a link to search in the databases of the NCAR's holdings; a service to search the NCAR library; and links to relevant websites. All these services would play major roles in enhancing information services on the NCAR website.

It is clear that the NCAR website had a generally acceptable standard for information retrieval services, with an average score of 2.00.

5.6 The Availability of Information Services via the NCAR Website

Table 6 summarizes the availability of information services via the NCAR website in Saudi Arabia, based on five items from the UK Archive Service Accreditation Standard.

Table 6. Availability of information services via the NCAR website in Saudi Arabia

Criteria	Average
• Easy access to services	2.5
• Basic information about NCAR information services	2
• Accessibility of NCAR services on the website	1.8
• Interactive services	1.3
• Information retrieval services	2
Overall average	1.9

Table 6 demonstrates that the availability of information services through the NCAR website in Saudi Arabia achieved an average score of 1.9 using the criteria of the UK Archive Service Accreditation Standards referred to earlier. In general, the availability of services was at an acceptable standard.

6. CONCLUSION

This paper assessed the information services available on the NCAR website in Saudi Arabia on the basis of the UK Archive Service Accreditation Standard – specifically the third section, which deals with stakeholders, their experiences, and the accessibility of services. Overall, the availability of information services on the NCAR website was at an acceptable level.

Based on the research, the following recommendations are made:

- Update the content of archive websites on a regular basis.
- Promote interest in the development of human resources in the field of archives using the digital resources .
- Devote attention to interactive services because they are an attractive element and a mean of marketing and electronically promoting the archive and its services.
- Develop and diversify the digital reference service.
- Provide a map or directory of the archive website, as well as a map indicating the geographical location of the archive.

7. REFERENCES

[1] Sawy, E. S. E. 2016. Metadata and its importance in supporting access to digital archival content. Cybrarians Journal.- 42 (June 2016). DOI= http:/doi. http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=733:ssawy&catid=290:studies&Itemid=93

[2] Issawi, E. 2008. National archives services in the age of the knowledge society. Cyberarians Journal. 16 (Nov. 2018), x-x - . DOI= http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=522:2011-08-22-00-05-26&catid=232:2011-07-23-12-32-19&Itemid=77

[3] Sawy, A. 2012. Web 2.0 features on archive websites and presidential libraries online. Journal of King Fahd National Library - Saudi Arabia. 18, 2 (Month 2012), 215 - 248. DOI= http://doi.http://search.mandumah.com/Record/444513

[4] Allaban, N.2018 . The use of national archives of the Facebook network in sustainable development. International Journal of Library and Information Science - Egyptian Library and Information association . 5, 2 (2018), 191-227.

[5] Nada, A. 2017. YouTube Channels of National Archives on the Internet. Recent trends in libraries and information. 24, 48 (Month 2017), 333 - 361.

[6] Elsawy, E. S. 2018. National archives programs for electronic document management training. JIS&T. 2018, 1 (Mar. 2018), 1-20. DOI= https://doi.org/10.5339/jist.2018.4

[7] National Center for Documents and Archives. Retrieved from http://www.ncar.gov.sa/Home/Index

[8] Ibrahim, R. 2009. National archives online. Cairo: Supreme Council of Culture, 222 p.

[9] Sharif, A. 2017. Digital Information services with national archives on the web and the Arab archives position: An analytical study. Cybrarians Journal. 46 (June 2017), 1-50. doi.http://www.journal.cybrarians.org/index.php?option=com_content&view=article&id=793:asharif&catid=307:papers&Itemid=93

[10] Millar, L. A. 2017. The Principles of Archival Service. Facet Publishing, London.

[11] Ngoepe, M. and Ngulube, P. 2011. Assessing the extent to which the National Archives and Records Service of South Africa has fulfilled its mandate of taking archives to the people. Innovation. 42 (June 2011), 3-22. DOI= https://www.researchgate.net/publication/274952034_Assessing_the_extent_to_which_the_National_Archives_and_Records_Service_of_South_Africa_has_fulfilled_its_mandate_of_taking_archives_to_the_people

[12] Nengomasha, C. T. and Nyanga, E. H. 2015. Access to archives at the national archives of Namibia. ESARBICA Journal. 34, 88 (2015), . DOI= http://doi:10.4314/esarjo.v34i1

[13] Chaterera, F. 2017 . A framework for access and use of documentary heritage at the national archives of Zimbabwe. Doctoral Dissertation. University of South Africa. Retrieved from http://uir.unisa.ac.za/bitstream/handle/10500/23841/thesis_chaterera_f.pdf.pdf?sequence=1&isAllowed=y

[14] Sharif, A. 2012. Web Applications 2.0 in National Archives (US National Archives Guidance Model for Arab Archives) - Alroznamh (10), 507-574

[15] Nada, A. 2016. Tweets of national archives, libraries and presidential museums via Twitter on the Internet. International Journal of Library and Information Science - Egyptian Library and Information association . 3, 3 (2016), 84-112.

[16] Hager, J. D. 2015. To like or not to like: Understanding and Maximizing the Utility of Archival Outreach on Facebook. Am. Arch. 78, 1 (Sprg/Summ. 2015), 18-37. DOI= https://doi.org/10.17723/0360-9081.78.1.18

[17] Accredited Archive Service. 2018. Archive services accreditation. - (June 2018). Retrieved from https://www.nationalarchives.gov.uk/documents/archives/archive-service-accreditation-glossary-june-2018.pdf.

[18] Accredited Archive Service. 2018. Archive service accreditation Eligibility Criteria. (June 2018).Retrieved from https://www.nationalarchives.gov.uk/documents/archives/archive-service-accreditation-eligibility-june-2018.pdf.

[19] Accredited Archive Service. 2018. Archive services accreditation standard. (June 2018).Retrieved from https://www.nationalarchives.gov.uk/documents/archives/archive-service-accreditation-standard-june-2018.pdf.

The Effect of Attitude on Student's Academic Performance in Cataloguing and Classification Course in Nigerian Polytechnics

Jimoh, Rafiu (Ango)
Federal Polytechnic Offa, Kwara State Nigeria
Offa, Kwara State, Nigeria.
Department of Library and information Science, Federal Polytechnic Offa, Kwara State, Nigeria
+2348076670531
Jrafiu91@gmail.com

ABSRTACT

The study investigates the effect of attitude on student's performance in cataloguing and classification courses in polytechnic based library schools in Nigeria. This is against the background of the phobia the students have on cataloguing and classification. Descriptive survey method was adopted while a questionnaire, student's attitudinal test and cataloguing and classification test were used for data collection. Total enumeration technique was used to select all the 1019 HND students from four purposively selected Nigerian polytechnics. Data were analysed using Pearson product moment correlation at 0.05 level of significance. The result on student's attitude towards cataloguing and classification course (r=0.73) and cataloguing and classification achievement test (r=0.74) the federal Polytechnic Offa has most favourable attitude ($\bar{x}$ = 39.914) to cataloguing and classification course in the library school followed by Federal Polytechnic Oko (x=35.887) Federal Polytechnic Kaduna ($\bar{x}$ = 32.244) and Federal Polytechnic Nekede ($\bar{x}$ = 29.22). The study reveals that student's attitude has a significant correlation with performance in cataloguing and classification courses. The study recommended that student's positive attitude influenced academic performance of Higher National Diploma students in cataloguing and classification courses in Nigerian polytechnics.

CCS Concepts

•**Information Systems→Document Structure.**

Keywords

Student's Attitude; Academic Performance; Cataloguing and Classification.

1. INTRODUCTION

The issue of students' academic performance remains a source of concern to educational administrators, government at all levels and the society at large. The recent decline in the academic performance of students is a burning issue in the Nigerian society. Parents, teachers and other educational stakeholders have all expressed their fear over this poor academic performance among the Nigerian students. According to Ali (2009), students' academic performance plays an important role in producing the best quality graduates to become great leaders and sources of manpower development for a sustainable and social transformation leading to economic development of any nation. Annie, Howard and Mildred (1996) defined academic performance as the outcome of education, the extent to which a student, teacher or institution has achieved their educational goals. Academic performance can also be referred to as the observable and measurable behavior of a student in a particular situation. Students' academic performance is the achievement of students in their courses of study.

Academic performance can be perceived as high, average or low. Jayanthi et. al (2014) stated that poor academic performance or high failure rates may result in unacceptable levels of attrition, reduced graduate output and increased cost of education. This also reduces admission opportunities for tertiary students seeking higher degrees. Hence, students' academic performance has always been a topic of interest for educators. The level of students' academic performance is determined by several factors. Sommai (2008) identified four causes of students' low academic performance as insufficient basic knowledge, parents' inadequate income, helping work of family and strict control of parents over studies. In addition, too much assignment could also affect students' academic performance and students' inability to adjust to life on their own. Factors like psychological, economic and environmental factors have been identified by previous studies to strongly influence students' academic performance (Hussain, 2006; Amitava, 2010).

Students' attitude could have a significant relationship with the academic performance in cataloguing and classification course in the library schools in polytechnics in Nigeria. Mcleod (2009) defined attitude as a learned tendency to evaluate things in a certain way. This can include evaluation of people, issues, objects or events. Such evaluations are often positive or negative, but they can also be uncertain. For example, students might have certain feelings about a particular person or issue. Eysenek (2004) and Zimmerman (2012), in their studies, stated that there are different components of attitude such as emotional component which reveals how students feel about an object, a person or an issue. Cognitive component of attitude is about individual thoughts and beliefs about the subject and the behavioural component which

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388182

shows how the attitude influences individual behaviour. Mcloed (2009) gave further insight about attitude to be explicit and implicit. The explicit attitude refers to those that students are conscious of and which clearly influence student behaviour and beliefs. Implicit attitude are unconscious, but still have an effect on students beliefs and behaviour. The cognitive component of attitude which is based on students' thoughts and beliefs about cataloguing and classification as a subject which could be positive or negative attitude will be the focus of this study.

1.1 Statement of the Problem

The core problem noticed among the students of polytechnic-based library schools in Nigeria is poor academic performance in cataloguing and classification course. These students often feel relieved with poor grade as long as they do not have to resit cataloguing and classification courses. This is a source of concern as poor performance in cataloguing and classification course constitute serious setbacks to their careers in librarianship. This poor academic performance may be due to students' negative attitude, the students' attitude, especially the negative aspect, where most students have expressed uninspiring views on cataloguing, has very often been reflected in their performance in the course. In spite of all efforts to sustain students' interest in cataloguing and classification like other courses offered in library schools, it was however, observed that the students' performance in cataloguing and classification compared to other courses taken in the library schools, is still low. There is, therefore, the need to examine the factor that is largely responsible for the students' poor academic performance in cataloguing and classification course.

1.2 Objectives of the Study

The general objective of this study is to examine the influence of attitude, on the performance of students in cataloguing and classification in polytechnic-based library schools in Nigeria.

The specific objectives of the study are to:

- find out the attitude of students towards cataloguing and classification course in polytechnic-based library schools in Nigeria;
- find out the performance level of students in cataloguing and classification course in polytechnic-based library schools in Nigeria;

1.3 Research Questions

The study provides answers to the following research questions:

- What is the attitude of students towards cataloguing and classification course in polytechnic based library schools in Nigeria?
- What is the performance level of students in cataloguing and classification course in polytechnic-based library schools in Nigeria?

1.4 Significance of the Study

This study is important because the result of the study could help in identifying the major reasons why academic performance of diploma students in cataloguing and classification courses are relatively poor in comparison with other courses offered, and the need for students to develop more positive attitude towards cataloguing and classification courses to bring about a successful outcome in their librarianship career. The study will serve as a point of reference on how to sustain the interest of students learning cataloguing and classification courses. Students' training in librarianship could be deficient without a thorough understanding of cataloguing and classification courses. It is also expected to serve as catalyst for students learning cataloguing and classification to do away with negative attitude about the course.

1.5 Scope and Limitation of the Study

The study covers attitude and students' performance in cataloguing and classification courses among all the National Diploma students in all federal polytechnic-based library schools in Nigeria. The study investigates students' attitude to cataloguing and classification courses and its influence on their academic performance. The study examines students' academic performance in cataloguing and classification courses and was limited only to the selected federal polytechnic library schools in Nigeria.

2. LITERATURE REVIEW

2.1 Cataloguing and Classification in Library and Information Science Schools

Librarians believe that cataloguing and classification is the core of library and information science (LIS) education. They also supported the idea of cataloguing and classification as an important component of library and information science education. Ocholla and Ocholla (2011), observed that in Brazil, Library and Information Science schools education has recorded a success in its efforts to cooperate within the country and across Mercosual Region (Argentina, Brazil, Chile, Paraguay, and Uruguay) as well as across information and documentation professions. All types of schools have strong link of communication with each other resulting in mutual collaboration. This effort focuses more on information or knowledge organisation in the realm of information science to serve as the theoretical domain which furnishes a common domain including archival, library and museum sciences. In the study carried out by Ocholla and Ocholla (2011) in South Africa from eight library and information science schools, it was noted that all the professionals agreed that cataloguing and classification is the core of library and information science and the backbone of librarianship's professional qualification. They also perceived cataloguing and classification as courses that support knowledge of library information and reference services, extremely useful for the critical analysis and synthesis of a library collection by knowledge domains or structure for effective information services and essential for the organisation of knowledge in libraries.

In a related study in Brazil, information processing, including classification, indexing, abstracting, cataloguing and information retrieval are believed to be the nucleus of library and information science studies and constitute an average of twenty-five percent of the hours of the total library course. This is also in accordance with the Mercosual Library and Information Science Agreement which is based on the basic concept of relationship between the role of information science as a theoretical domain supporting the practical information domains like archival science, library science as well as museology. In the study, all the respondents declared that the teaching of cataloguing and classification in library schools are very important, with a caveat that there is the need for changes and adaptations to fit new users' needs such as technological empowerment to librarians and users. However, there is the need for theory and principles of knowledge organisation which are needed to be connected with technological knowledge to enhance the education and knowledge of cataloguing and classification.

3. METHODOLOGY

3.1 Introduction

This aspect of the research discusses the research design, population of the study, sample and sampling technique, research instruments, validity and reliability of research instruments, data collection procedure and method of data analysis.

3.2 Population of the study

The total population of this study consists of four federal polytechnics out of the eight federal polytechnics offering library and information science in Nigeria as indicated in the list of accredited programmes by the National Board for Technical Education (NBTE) and Unified Tertiary Matriculation Examination (UTME) brochures. It includes the Ordinary National Diploma and Higher National Diploma students as well as lecturers teaching cataloguing and classification courses in these library schools with a total of 1388 students and 10 lecturers. See Table 3.1 representing the population of the study.

4. RESULTS AND DISCUSSION

This aspect presented the result of the findings in order of sequence such as frequency distribution, research questions and hypotheses. Simple percentage, Multiple regression analysis, analysis of variance and Pearson Product Moment Correlation statistical tools were used to analyze the data collected.

4.1 Sampling Technique and Sample Size

The study used purposive sampling technique to select federal polytechnics offering library and information science in Nigeria. This included all HND I and HND II students as well as the lecturers teaching cataloguing and classification courses in the selected library schools in Nigerian polytechnics. The choice of HND I and HND II students was based on their fairly long periods of interaction with the library schools and their familiarity with cataloguing and classification courses. The lecturers were included due to their involvement in the teaching of cataloguing and classification courses in the polytechnics at the HND level. The choice of sampling technique and sample size was based on the homogeneous nature of the study population and that all HND I and HND II students enumerated in the study was covered. A total enumeration was used to cover 1388 students and 10 lecturers.

4.2 Data Collection Instruments

The instruments that were used for data collection in this study include: (i) Questionnaire for students (ii) Questionnaire for lecturers; (iii) Cataloguing and Classification Achievement Test (CCAT);

This section presented the result of the findings in order of sequence such as frequency distribution, research questions and hypotheses. Simple percentage, Multiple regression analysis, analysis of variance and Pearson Product Moment Correlation statistical tools were used to analyze the data collected.

Research Question I: What is the attitude of students towards cataloguing and classification course in polytechnic based library schools in Nigeria?

Results from Table below indicated that majority of the students of the Federal polytechnic Kaduna agreed to the statement that they are excited learning cataloguing and classification course with library tools like Anglo American Cataloguing Rules, Dewey Decimal Classification scheme and Library of Congress Classification scheme if introduced for practical (x = 8.30). They also claimed that they prefer other courses taught in the department to cataloguing and classification (x = 7.07). Most of them equally agreed to the statement which says 'I prefer to work in cataloguing and classification department of the library after my graduation' (x = 6.76). The implication of this is that majority of the students from the Federal polytechnic Kaduna in this study expressed positive attitude towards cataloguing and classification course.

Table 1. Students' attitude towards cataloguing and classification course in Federal Polytechnic, Kaduna

Hint: SD= Strongly Disagree, D = Disagree, A= Agree, SA= Strongly Agree

S/N	STATEMENTS	SD freq (1)	D freq (2)	A freq (3)	SA freq (4)	Mean	SD
1	Cataloguing and classification are too boring to me.	4.5%	9.7%	48.8 %	37.1%	2.66	.487
2	I prefer missing cataloguing and classification classes.	5.5%	7.0%	49.3%	38.2%	5.13	2.351
3	Cataloguing and classification are better removed from the curriculum of library studies.	11.9%	8.7%	42.8 %	36.7%	5.73	2.457
4	I find cataloguing and classification to be more interesting than other courses.	3.7%	5.7%	49.8%	40.8%	4.06	1.258
5	Cataloguing and classification are uninteresting to me.	2.8%	8.2 %	44.9%	34.1%	3.33	2.487
6	I enjoy studying cataloguing and classification.	5.9 %	8.1%	51.7%	34.3%	4.76	2.438
7	Among the courses offered in the department, cataloguing and classification is my favourite.	5.9%	7.1%	48.7%	38.3%	5.69	2.480
8	I prefer to work in cataloguing and classification department of the library after my graduation.	3.5%	12.8%	48.6%	35.1%	6.76	2.238
9	I am excited learning cataloguing and classification with library tools like AACR2, DDC, and LC if introduced for practicals.	10.3 %	16.2%	29.8	43.7%	8.30	3.480
10	I prefer other courses taught in the department to cataloguing and classification.	2.6%	10.4%	37.5%	49.5%	7.07	3.277
11	If I have my way, I will prefer working in other sections instead of cataloguing and classification department of the library when I graduate.	3.5%	13.1%	40.9%	42.5%	.961	1.506
12	I am frustrated when using cataloguing and classification tools.	17.5%	8.5%	38.6%	35.4%	5.07	2.277
13	My choice of research topic will exclude cataloguing and classification as it difficult.	14.9%	14.9%	37.9%	32.3%	4.63	2.492
14	Only the extremely brilliant students pass cataloguing and classification course.	2.4%	6.9%	50.3%	34.6%	5.636	1.492 3

Table 2. Students' attitude towards cataloguing and classification course in Federal Polytechnic, Offa

Hint: SD= Strongly Disagree, D = Disagree, A= Agree, SA= Strongly Agree

S/N	Statements	SD freq. (1)	D freq .(2)	A freq. (3)	SA freq (4)	Mean	SD
1	Cataloguing and classification are too boring to me.	6.1 %	30.1%	59.9 %	3.8%	4.50	1.511
2	I prefer missing cataloguing and classification classes.	13.5%	28.2%	52.8%	5.5%	.327	1.455
3	Cataloguing and classification are better removed from the curriculum of library studies.	3.4%	32.9%	62.3 %	1.3%	3.04	1.213
4	I find cataloguing and classification to be more interesting than other courses.	4.9%	29.0%	63.5	2.7%	5.54	2.509
5	Cataloguing and classification are uninteresting to me.	4.8%	37.3%	56.7%	1.2%	5.09	1.294
6	I enjoy studying cataloguing and classification.	2.9%	29.9%	63.3%	3.8%	7.59	2.503
7	Among the courses offered in the department, cataloguing and classification is my favourite.	4.3%	25.1%	68.8 %	1.8 %	5.75	.447
8	I prefer to work in cataloguing and classification department of the library after my graduation.	11.3%	18.7%	65.2%	4.9%	4.80	1.410
9	I am excited learning cataloguing and classification with library tools like AACR2, DDC, and LC if introduced for practical.	6.27%	12.27%	60.4%	20.93%	3.55	2.510
10	I prefer other courses taught in the department to cataloguing and classification.	7.1%	34.6%	54.2%	4.1%	3.65	1.489
11	If I have my way, I will prefer working in other sections instead of cataloguing and classification department of the library when I graduate.	10.1%	35.%	49.0 %	5.8%	5.54	2.509
12	I am frustrated when using cataloguing and classification tools.	82 5.5%	511 34.1%	872 58.1%	35 2.3%	3.812	.118
13	My choice of research topic will exclude cataloguing and classification as it difficult.	6.1%	45.1%	47.4%	1.3%	4.187	.002
14	Only the extremely brilliant students pass cataloguing and classification course.	12.27%	20.93%	60.4%	6.27%	3.807	.838

The results in Table above revealed that most students from Federal Polytechnic, Offa agreed to enjoying studying cataloguing and classification courses (x = 7.59) and they find cataloguing and classification courses to be more interesting than other courses (x = 5.54). However, if they have their way, they will prefer working in other sections instead of cataloguing and classification department of the library on graduation (5.54).

Table 3. Students' attitude towards cataloguing and classification course in Federal Polytechnic, Oko

Hint: SD= Strongly Disagree, D = Disagree, A= Agree, SA= Strongly Agree

S/N	ITEMS	SD freq. (1)	D freq. (2)	A freq. (3)	SA freq (4)	Mean	SD
1	Cataloguing and classification are too boring to me.	2.3%	6.9%	48.1 %	42.7 %	3.30	1.69
2	I prefer missing cataloguing and classification classes.	6.0%	13.1 %	44.3 %	36.7 %	3.10	.087
3	Cataloguing and classification are better removed from the curriculum of library studies.	8.3%	9.3%	45.9 %	36.5 %	4.40	1.894
4	I find cataloguing and classification to be more interesting than other courses.	10.3 %	10.5 %	47.1 %	32.1 %	1.866	1.076
5	Cataloguing and classification are uninteresting to me.	7.1%	42.7 %	45.7 %	4.6%	2.133	1.198
6	I enjoy studying cataloguing and classification.	5.2%	43.2 %	49.2 %	2.4%	3.066	1.966
7	Among the courses offered in the department, cataloguing and classification is my favourite.	5.9%	42.6 %	44.4 %	7.1%	3.000	.296
8	I prefer to work in cataloguing and classification department of the library after my graduation.	5.3%	46.5 %	46.7 %	1.5%	3.615	.355
9	I am excited learning cataloguing and classification with library tools like AACR2, DDC, and LC if introduced for practical.	4.9%	29.7 %	48.6 %	16.8 %	4.846	1.949
10	I prefer other courses taught in the department to cataloguing and classification.	4.7%	44.5 %	49.0 %	1.7%	3.666	.937
11	If I have my way, I will prefer working in other sections instead of cataloguing and classification department of the library when I graduate.	4.5%	9.7%	48.8 %	37.1 %	2.444	.065
12	I am frustrated when using cataloguing and classification tools.	5.5%	7.0%	49.3 %	38.2 %	4.111	1.050

13	My choice of research topic will exclude cataloguing and classification as it difficult.	11.9 %	8.7%	42.8 %	36.7 %	2.750	1.583
14	Only the extremely brilliant students pass cataloguing and classification course.	3.7%	5.7%	49.8 %	40.8 %	3.250	.897

Table above reveals that the attitude of students of Federal Polytechnic Oko to cataloguing and classification courses was positive because most of the respondents stated that they were excited learning cataloguing and classification with library tools like AACR, DDC, and LC if introduced for practical (x = 4.846). However, they were frustrated when using cataloguing and classification tools (4.111) and they prefer other courses taught in the department to cataloguing and classification (3.666).

Table 4. Students' attitude towards cataloguing and classification course in Federal Polytechnic, Nekede based on strongly agreed and agreed responses Hint: SD= Strongly Disagree, D = Disagree, A= Agree, SA= Strongly Agree

S/N	ITEMS	SD Freq . (1)	D Freq .(2)	A Freq. (3)	SA Freq (4)	Mean	SD
1	Cataloguing and classification are too boring to me.	2.8%	8.2 %	44.9%	34.1%	4.750	.664
2	I prefer missing cataloguing and classification classes.	5.9 %	8.1%	51.7%	34.3%	3.727	1.140
3	Cataloguing and classification are better removed from the curriculum of library studies.	5.9%	7.1%	48.7%	38.3%	3.818	.897
4	I find cataloguing and classification to be more interesting than other courses.	3.5%	12.8%	48.6%	35.1%	4.090	1.741
5	Cataloguing and classification are uninteresting to me.	10.3 %	16.2%	29.8	43.7%	3.310	.186
6	I enjoy studying cataloguing and classification.	2.6%	10.4%	37.5%	49.5%	2.620	.539
7	Among the courses offered in the department, cataloguing and classification is my favourite.	3.5%	13.1%	40.9%	42.5%	4.793	1.446
8	I prefer to work in cataloguing and classification department of the library after my graduation.	17.5%	8.5%	38.6%	35.4%	2.222	1.042
9	I am excited learning cataloguing and classification with library tools like AACR2, DDC, and LC if introduced for practicals.	14.9%	14.9%	37.9%	32.3%	2.444	1.694
10	I prefer other courses taught in the department to cataloguing and classification.	2.4%	6.9%	50.3%	34.6%	2.666	1.027
11	If I have my way, I will prefer working in other sections instead of cataloguing and classification department of the library when I graduate.	2.3%	6.9%	48.1%	42.7%	3.937	.991
12	I am frustrated when using cataloguing and classification tools.	6.0%	13.1%	44.3%	36.7%	1.687	.301
13	My choice of research topic will exclude cataloguing and classification as it difficult.	8.3%	9.3%	45.9%	36.5%	4.437	.262
14	Only the extremely brilliant students pass cataloguing and classification course	10.3%	10.5%	47.1%	32.1%	3.000	.633

Table above shows that most of the students indicated preference for cataloguing and classification courses in the department (x = 4.793). In contrast, they indicated that cataloguing and classification are too boring (x = 4.750) and their choice of research topic will be outside cataloguing and classification to avoid its difficulty (x = 4.437). This implies that they mostly have negative attitude to cataloguing and classification course.

Table 5. Students' attitude towards cataloguing and classification course across the polytechnics based on summed up of agreed and strongly agreed ratings.

S/N	Name of library schools	N	Mean	Std. Deviation	Std. Error
1	Federal Polytechnic Kaduna, Kaduna State	135	32.244	13.838	1.19101
2	Federal Polytechnic Offa, Kwara State	223	39.914	16.591	1.11105
3	Federal Polytechnic Oko, Anambra State	409	35.887	15.133	.74831
4	Federal Polytechnic Nekede, Imo State	252	29.222	15.046	.94786
	Total	**1019**	**34.643**	**15.728**	**.49248**

From the results on Table above, there are differential mean scores on attitude of students towards cataloguing and classification courses in polytechnic-based library schools in Nigeria. Based on the scale, the students from the Federal Polytechnic Offa have the most positive attitude (x = 39.914) towards cataloguing and classification courses in polytechnic-based library schools in Nigeria. This was followed by students from Federal Polytechnic, Oko (x = 35.887), Polytechnic, Kaduna (x = 32.224) and Federal Polytechnic, Nekede (x = 29.222) had the least positive respectively.

Research Question II: What is the performance level of students in cataloguing and classification achievement test in polytechnic-based library schools in Nigeria?

Cataloguing and classification achievement test was conducted by the researcher for the Higher National Diploma students of polytechnic-based library schools in Nigeria. Table 5 showed that there are differential mean scores on performance of students in cataloguing and classification achievement test in polytechnic-based library schools in Nigeria. Students from the Federal Polytechnic, Kaduna had the highest performance (72.1%) followed by students at the Federal Polytechnic, Nekede (70.9%), Federal Polytechnic Oko (68.5%) and Federal Polytechnic, Offa (65.4%) respectively.

Table 6. Performance level of students in cataloguing and classification performance test in polytechnic-based library schools in Nigeria

	Polytechnics	(Population)N	Average Obtained percentage
Cataloguing/Classification Achievement	Federal Polytechnic Kaduna	135	72.1%
	Federal Polytechnic Offa	223	65.4%
	Federal Polytechnic Oko	409	68.5%
	Federal Polytechnic Nekede	252	70.9%
	Total	**1019**	**69.2%**

5. SUMMARY, CONCLUSION AND RECOMMENDATIONS

This aspect has presented the summary of the findings of the study, conclusion, recommendations, implications of the study, contributions to knowledge, limitation of study and suggestions for further research.

5.1 Summary of Findings

The following are the major findings of the study:

- Students with positive attitude were more than those that expressed negative attitude towards cataloguing and classification courses.
- The performance of the students in cataloguing and classification test was below average performance.
- There is a significant and positive relationship between students' attitude and academic achievement of students in cataloguing and classification courses in polytechnic-based library schools in Nigeria.

5.2 Conclusion

The study confirmed that attitude, have significant and positive relationship with academic achievement of Higher National Diploma students in cataloguing and classification courses in polytechnic-based library schools in Nigeria. National Diploma students would record higher achievement in cataloguing and classification if they develop more positive attitude towards the courses.

5.3 Recommendations

Based on the findings of the study, the following recommendations are hereby made:

- The results of the study reveal that some students have negative attitude towards cataloguing and classification courses which accounts for the below average performance recorded in the courses. Hence, the management of Nigerian polytechnics should ensure that lecturers teaching cataloguing and classification course make the class more interesting to students for a better attitude towards the course.
- Owing to the current trends in librarianship which affect all aspects of the discipline especially cataloguing and classification, lecturers teaching this course should be sponsored to cataloguing and classification/indexing section of the Nigerian Library Association (NLA) at their annual workshop to keep them updated on the latest best practices in tune with the principles of consistency in cataloguing.
- Nigerian students are admonished to develop a more positive attitude towards learning generally while students from various library schools should remove phobia they had already associated for cataloguing and classification courses to bring about an excellent performance in the course.

6. REFRENCES

[1] Ali, N. 2009. *The factors influencing student performance at university Teknologi Mara Kedah, Malaysia. Canada research development center of science and culture 3:4.*

[2] Amitava, R. 2010. *Factors affecting Student's academic performance: A case study in Agartala municipal concial area.Bangladesh e-journal of sociology 7:2.*

[3] Annie, W., Howard, W. S. and Mildred, M. 1996. *Achievement and Ability Tests: Definition of the Domain. Educational Measurement 2. University Press of America, pp. 2–5.*

[4] Hussain, C. A. 2006. *Effect of Guidance Services on Study Attitudes, Study Habits and Academic Achievement of Secondary School Students. Bulletin of Education and Research. 28.1:35-45.*

[5] Jayanthi, S. V., Balakrishnan, S., Ching, A. L., AbdulLatiff, N. A. and Nasirudeen, A. M. (2014). *Factors Contributing to Academic Performance of Students in a Tertiary Institution in Singapore. American Journal of Educational Research, 2.9: 752-758.*

[6] Mcloed, S. A. 2009. Attitudes and behaviour. Retrieved from http://www.simplypsychology.org/attitudes.html

[7] Sommai, P. 2008. *Study of problem leisure of low learning achievement students Nakhonsawan Career College. Nakhonsawan: Nakhonsawan Career College.*

Legal Judgement Prediction for UK Courts

Benjamin Strickson
University of East Anglia
Norwich, UK
benjamin.strickson@gmail.com

Beatriz De La Iglesia
University of East Anglia
Norwich, UK
B.Iglesia@uea.ac.uk

ABSTRACT
Legal Judgement Prediction (LJP) is the task of automatically predicting the outcome of a court case given only the case document. During the last five years researchers have successfully attempted this task for the supreme courts of three jurisdictions: the European Union, France, and China. Motivation includes the many real world applications including: a prediction system that can be used at the judgement drafting stage, and the identification of the most important words and phrases within a judgement. The aim of our research was to build, for the first time, an LJP model for UK court cases. This required the creation of a labelled data set of UK court judgements and the subsequent application of machine learning models. We evaluated different feature representations and different algorithms.

Our best performing model achieved: 69.05% accuracy and 69.02 F1 score. We demonstrate that LJP is a promising area of further research for UK courts by achieving high model performance and the ability to easily extract useful features.

CCS Concepts
• Information systems→Content analysis and feature selection
• Information systems→Clustering and classification
• Information systems→Document topic models.

Keywords
Legal judgement prediction; legal calculus; feature extraction.

1. INTRODUCTION
The ability of computers to predict the outcome of legal cases from the text documentation began to attract serious attention from the 1960s onward. Lawlor [13] argued that it should be possible to predict how the facts and legal arguments of a case would be received by a judge. In the subsequent decades several studies [2, 3, 26] have attempted to manually derive a legal calculus, which is defined as an abstract system of argument structures or schemes that are linguistically realised in legal texts.

A new approach [21], based on machine learning techniques, emerged to move the field forward. The first attempts [9, 11, 17] used machine learning models to predict the judgements of the Supreme Court of the United States (SCOTUS). These attempts used document tags as predictive features, tags such as type of case and judge name.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388183

Subsequent researchers built predictive models which relied only on unstructured text features, this became known as LJP. Aletras et al. [1] were the first to apply this approach, attempting LJP on the European Court of Human Rights (ECHR) data set. Three subsequent published studies share a common methodology and research objectives, two of those also used the ECHR data set [16, 18], and the other used the French Court of Cassation data set [19]. Our research also aims to rely solely on text-derived features and machine learning. It will be the first study to attempt LJP for UK court decisions and represents further important evidence of the potential to successfully apply machine learning for LJP.

There are two significant problems this study is required to overcome when attempting LJP on UK court documents. The first is the currently limited ability of Natural Language Processing (NLP) techniques to recognise complex semantic structures such as arguments. The second problem is specific to the UK; there is currently no structured public data set of UK court cases.

Our research aim is to build an interpretable predictive model for UK court cases using only the court documents. The objectives that will help us to achieve this aim are:

- To build a labelled data set of UK court judgements with an outcome variable that can be used in prediction tasks.
- To build a prediction model using machine learning techniques previously applied by comparable studies.
- To test alternative text mining techniques such as word embedding features with neural network models.

In this paper we explain how we built our labelled data set for UK court judgements and then used it to test existing and newer text mining techniques obtaining good accuracy and usable features. Section 2 reviews similar work done by other researchers; Section 3 explains our methodology; Sections 4 and 5 present our text mining results and discussions; and finally we present our conclusions in Section 6.

2. RELATED WORK
One of the very important decisions that affects any text mining application is how to represent text as features that can be handled by machine learning algorithms. The n-gram has become a hugely popular feature set in text classification tasks, where a gram is often equivalent to a word. First utilised by Shannon [23], its main advantage is that it allows documents to be represented as vectors. All individual words (one-grams) or larger n-grams from the corpus are represented as columns, and each document is represented as a single row in the matrix. The value at the intersection of the row and column represents how often a term, or n-gram, appears in a document. This value is most commonly a simple count statistic or the Term Frequency-Inverse Document Frequency (TFIDF) [25] statistic. These vector space models proved beneficial for the application of machine learning models.

The first paper to apply these features to the task of LJP was Aletras et al. [1], who used n-grams ranging from one-grams to

four-grams. Three other published studies [16, 18, 19] followed using the same methodology.

An alternative approach known as generative language models has also been applied to extract feature sets for the task of text classification. Blei et al. [5] developed the Latent Dirichlet Allocation (LDA) algorithm which implements this theory by constructing topic clusters out of text documents. The algorithm assumes that documents are composed of a random mixture of latent topics, and each of the topics is characterised by a distribution over words. Some studies [5, 15] have been able to demonstrate a performance benefit in text classification tasks to support the application of LDA feature sets.

A recent alternative to the vector space feature set emerged to address their short-comings; Bengio et al. [4] argued that n-gram feature sets were problematic as they did not consider the similarity between words. They developed a technique known as neural network-based word embeddings in which each word is represented as a vector with multiple dimensions. These dimensions contain values that encode information concerning the target word's surrounding words. This work was supported by Mikolov et al. [20] who developed the Word2Vec algorithm that we will use. This algorithm has two distinct phases: the first phase involves training a neural network to learn word distributions. We will use the Continuous Bag Of Words (CBOW) architecture, where a window of surrounding words is used to predict a target word. The second phase feeds the word vectors from the learned hidden layer into an output layer, to represent each word as an n-dimensional vector.

In terms of classification algorithms, we looked at the current LJP literature to select suitable models. All the LJP studies mentioned so far have used Support Vector Machine (SVM)s. Their popularity is due to their high performance across a range of text classification tasks [10, 27, 29]. Additionally we included the Logistic Regression (LR), Random Forest (RF), and k-Nearest Neighbour (k-NN) as used by Liu and Chen [16]. To meet our third research objective we included two neural networks: a Single Layer Perceptron (SLP) and a Multi-Layer Perceptron (MLP).

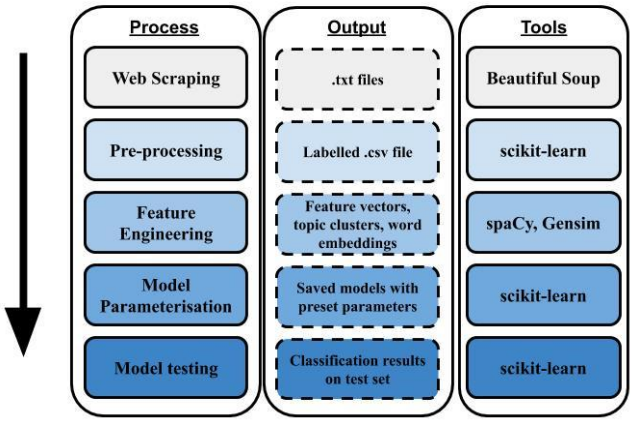


Figure 1. Research methodology workflow.

3. RESEARCH METHODOLOGY

3.1 Data Collection

The data set used in this study was restricted to the judgements issued by the UK's highest court of appeal, similar to other studies [1, 6, 16, 18, 19] which focused on one court within one country's legal system. To collect these judgements a web scraper was built.

3.2 Data Labelling

Each web-scraped case file was divided into the separate judgements passed down by the individual judges. Next, each of these rulings were automatically labelled into 'allow' or 'dismiss' using a pattern matching approach. The files which could not be labelled with an outcome were individually examined before being excluded from the data set. They represent the cases where no final judgement was reached by the judges. To check the accuracy of the labelling methodology a random stratified sample of 5% of the data set was examined. A total of 4,959 text files were labelled after exclusions. This is comparable to three other studies where 584 cases [1, 16] and 3,132 cases [18] were used. It is, however, far fewer than the number of cases used in the study by Medvedeva et al. [19] on the French court of Cassation which had 126,865 cases. Our data collection methodology and code has been made publicly available[1].

3.3 Pre-processing

Text that identified with the outcome labels was removed from the data set to avoid giving the classifier the obvious information; this approach is inline with three other studies [1, 18, 19]. However, Liu and Chen [16] do not mention this stage in their review, we are thus cautious about their model results. To ensure that no words could be used as proxies for the labels an additional review of the most highly correlated model features was performed.

The remaining text consisted of a total set of 188,294 unique tokens (words). Reducing this high degree of dimensionality in our data set was considered important to prevent generalisation error and model over fitting. Therefore, we used the pre-processing steps set out by Joachims [10] as our guide and we achieved a significant reduction. The results of applying the different pre-processing steps such as converting to lowercase, removing numbers and stop words and lemmatization are presented in Table 1.

Table 1. Pre-processing steps and resulting token count

	Unique token (word) count
No pre-processing	188,294
Lowercase conversion	170,126
Numbers removed	166,949
Stop words removed	166,638
Lemmatize	157,648

3.4 Feature Engineering

To investigate which features gave best results for our specific environment, our feature sets were: n-grams, topic clusters and word embeddings. For n-grams we used the standard count and TFIDF implementations. We set n as one of the parameters to be optimised with a range from one to four. For the topic clusters we decided upon the LDA algorithm; a popular topic modelling

[1] Code available at https://github.com/BStricks/legal_document_classifier_V2

algorithm [5, 15]. We set the number of topics as one of the parameters to be optimised, ranging from five to thirty. For the word embedding feature set there was only one relevant study to draw from [6]. We chose to use untrained embeddings because our corpus contained a large number of words that was unique to the legal domain. These context specific words could have been problematic for pre-trained models such as those trained on Google's news feed. We also chose to use the Doc2Vec algorithm [14], which is an extension of the original Word2Vec algorithm that is able to generate document level vectors.

3.5 Model Tuning

All the above algorithms were implemented in the Python 3 language using the Scikit-learn package [22]. Below are the optimal parameters for each algorithm found by cross-validated random search, taken from the feature set that performed best:

SVM and TFIDF vectors: n-gram range (1,3), minimum feature occurrence (1), maximum features (10000), kernel (linear), c (5).

RF and TFIDF vectors: n-gram range (1,4), minimum feature occurrence (4), maximum features (4000), number of estimators (1000), max depth (20).

LR and TFIDF vectors: n-gram range (1,2), minimum feature occurrence (4), maximum features (None), solver (lbfgs), c (5).

k-NN and Doc2Vec: clusters (5).

SLP and TFIDF vectors: n-gram range (1,2), minimum feature occurrence (2), maximum features (10000).

MLP and TFIDF vectors: n-gram range (1,3), minimum feature occurrence (4), maximum features (10000), solver (adam), hidden layers (2,2), activation (logistic).

We report also for comparison the accuracy of Scikit-learn's dummy classifier which respects the training set's class distribution [22].

3.6 Evaluation

Our data set was split into two partitions. The first 80% of the data was used for a ten-fold cross-validated random search for hyperparameter optimisation with Scikit-learn [22]. The final 20% of the data, was used as a test set to report model scores. In LJP research average accuracy is the most commonly reported model score, we will report this for our test data. Our study will additionally report: F1, precision, and recall, as they provide important additional information on performance.

4. RESULTS

As shown in Table 3, the top performing combination of model and feature set was the LR algorithm paired with the TFIDF vector representation. This combination achieved an F1 score of 69.02, a precision of 69.05% and a recall of 69.02%. Overall both the RF and LR algorithms performed well across feature sets. SVM, k-NN, and SLP algorithms tended to perform worse across most of the feature sets. Overall the best performing feature sets were the Count and TFIDF vectors, with the topic clusters and word embeddings feature sets performing worse.

For the majority of the model and feature set pairings the F1, recall, and precision scores were roughly equivalent. This is partly due to having a balanced data set; with 2,525 'Allow' cases and 2,434 'Reject' cases. It also suggests that the models are generally good at selecting true positives and avoiding false positives, as well as selecting many of the relevant data points, avoiding false negatives. Additionally the best performing models from each feature set models were analysed with Receiver Operating Characteristic (ROC) curves. This was done to better understand performance at various threshold levels of sensitivity (True Positive Rate or recall) and specificity (or False Positive Rate). The curves, see Fig. 2, support our initial observations of stronger model performance for the count and TFIDF vector feature sets.

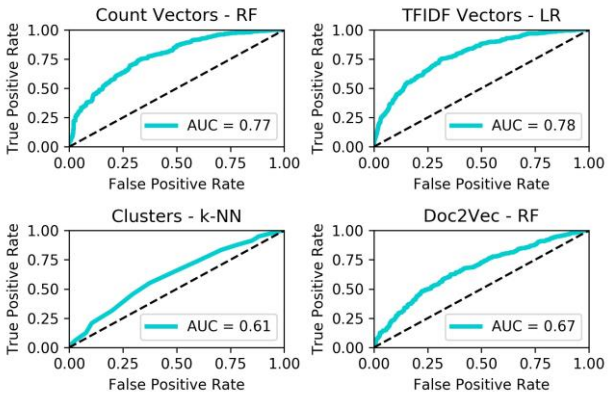


Figure 2. ROC curves for best model and features pairings.

5. DISCUSSION

5.1 n-grams

The strongest performing feature set as measured by the prediction scores was the TFIDF vectors composed of one-grams to two-grams. Given other text classification study results in this area, the high performance of this feature set was expected. Next we considered the usability of the n-gram features, this was an important secondary consideration when evaluating model performance. We extracted the most important n-gram features for our strongest performing vector-space model. Separating the features by outcome label, these are presented in Table 2. A preliminary review shows that these features contain interpretable meanings, and that most of them would generalise well to new cases.

Table 2. Most important n-gram features for the LR model extracted from the TFIDF representation associated with each outcome

	Top 15 most important features
Reject	rely, Iraq, instance, submit, minimum, actual, main, wreck, hire, hall, covenant, territory, regime, agency, product
Allow	restore, remit, siac, cross appeal, restore order, carrier, situation, segregation, account, declaration, directive, commission, avoid, perform, long

Table 3. Results showing Accuracy, F1, Precision and Recall measurements on the test data for different model and feature pairings

	Count vectors				TFIDF vectors				LDA topic clusters				Word embeddings			
	Acc.	F1	Prec.	Rec.	Acc.	F1	Prec.	Rec.	Acc.	F1	Prec.	Rec.	Acc.	F1	Prec.	Rec.
Dummy	52.02	52.01	52.02	52.02	49.09	49.04	49.05	49.05	49.90	49.90	49.91	49.91	49.60	49.59	49.64	49.64
SVM	61.49	61.49	61.50	61.50	65.93	65.89	65.92	65.89	52.12	50.47	52.05	51.80	60.79	60.11	62.58	61.45
RF	**66.13**	**66.12**	**66.12**	**66.13**	66.63	66.62	66.62	66.61	56.25	55.93	56.26	56.11	**64.21**	**64.17**	**64.17**	**64.18**
LR	65.12	65.12	65.13	65.13	**69.05**	**69.02**	**69.05**	**69.02**	53.12	53.11	53.11	53.11	62.10	62.00	62.66	62.42
k-NN	61.79	61.76	61.93	61.87	59.98	59.86	60.31	60.11	**57.76**	**57.63**	**58.01**	**57.88**	62.70	62.59	63.33	63.05
SLP	62.50	62.50	62.52	62.52	64.72	64.71	64.79	64.76	50.91	33.73	25.45	50.00	57.56	53.00	59.55	56.34
MLP	65.62	65.85	65.62	65.58	66.94	66.94	66.95	66.95	55.95	55.71	55.93	55.83	61.59	61.58	61.61	61.63

5.2 Topic Clusters

Topic clusters performed relatively poorly compared to the other feature sets, with the best performing model achieving an F1 score of 57.63. Despite these low scores, we assessed their usability by extracting the main features for each topic in Table 4. We can see promising results with each of the topics appearing to coalesce around similar legal areas and terminology. However, a full review of the topics by a trained lawyer may be necessary, though it is considered outside the scope of this paper.

Table 4. Topic clusters and the most important features associated with each. ('pron' is code for all pronouns)

Topic number	Top 5 most important topic features
1	act, pron, provision, section, parliament
2	pron, court, right, tax, company
3	pron, order, court, make, sentence
4	pron, act, lord, rule, board
5	pron, lord, friend, noble, pron noble
6	pron, company, pay, tax, payment
7	pron, article, right, state, convention
8	pron, offence, criminal, act, police
9	pron, child, case, pron, pron court
10	pron, court, decision, case, appeal
11	pron, law, state, court, jurisdiction
12	pron, regulation, work, member, directive
13	pron, case, claim, damage, lord
14	pron, right, property, land, use
15	pron, contract, party, agreement, clause

5.3 Word Embeddings

Our experiments show that the Doc2Vec word embedding feature set performed reasonably well with the best model achieving an F1 score of 64.17. The expectation had been that word embeddings would deliver the best overall model, given that other researchers have used this feature set to achieve state of the art results. Our explanation for the observed results is that whilst the word embeddings incorporated more contextual information than the other feature sets, the low number of data points in our data set may not have provided the necessary context. Given the success found elsewhere with pre-trained word embeddings we could attempt to construct these for future studies. A potential corpus constructed of all legal judgements from UK courts would provide ideal pretraining for our task. Finally we considered feature usability; it is noted that they provide significantly less insight than our alternative feature sets.

5.4 Machine Learning Algorithms

We can say that the k-NN and RF algorithms delivered the most consistent results across the feature sets. Whereas the SVM and LR algorithms less consistent performance, determined partly by feature set. We can say that in almost all cases the machine learning algorithms performed better with a reduced feature space. As demonstrated by the parameters selected during cross-validation.

5.5 Neural Nets

Our choice of artificial neural network architectures for our LJP task did not provide a clear improvement over our standard machine learning models. We used two of the simplest models, whereas text mining researchers working in other domains have recently applied more complex architectures with good results. As expected the MLP out-performed the SLP; this was most likely due to the complex nature of the classification problem. MLP's have an ability to handle complex decision boundaries which may exist in this problem.

Convolution Neural Networks [12, 30], Recurrent Neural Networks [24] or other Deep Learning algorithms may be more suitable for word embeddings [7, 8]. Also, the unpublished results of Chalkidis et al. [6] show the promise of the Hierarchical Attention Network (HAN) architecture. Their models achieved state of the art performance, due to the HAN architecture's suitability for document classification [28].

It is also worth considering that given the black box nature of these algorithms it is much harder to understand which features are used by the models when making their predictions. This means that even those studies [6] which have successfully used neural networks to boost LJP results have been unable to justify model decisions. Current research [6] indicates that there is the potential for attention scores to be used as a proxy for feature extraction; however, this metric has not been thoroughly reviewed or tested for use by legal experts.

6. CONCLUSION AND FURTHER WORK

Against our first objective we achieved the creation of 100 years of labelled UK court judgements. Against our second objective we delivered a predictive model that was both accurate and highly interpretable. We found that both vector space feature sets were able to deliver good results, though TFIDF features paired with the LR algorithm achieved the highest F1 score of 69.02. Extracting the most important features from the vector space and topic cluster models was a relatively easy task and indicates good

potential model usability. Our third objective was the application of word embeddings and neural networks to the task of LJP. Our results were unable to show that word embeddings combined with our choice of neural networks could improve model performance.

A number of more advanced neural network architectures have been used to great effect in other text classification tasks, we believe these could be used to great effect for LJP. Significantly improving the results we had with the SLP and MLP algorithms. The use of ngrams and topic clusters proved successful as predictive feature sets, however, in order to understand their usefulness further testing is needed. Our proposal would be for the independent examination and testing of the extracted features by professional lawyers.

7. REFERENCES

[1] Nikolaos Aletras, Dimitrios Tsarapatsanis, Daniel Preoţiuc-Pietro, and Vasileios Lampos. 2016. Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective. *PeerJ Computer Science* 2 (2016), e93.

[2] Kevin D. Ashley. 1991. *Modeling Legal Arguments: Reasoning with Cases and Hypotheticals*. MIT Press, Cambridge, MA, USA.

[3] Trevor Bench-Capon. 1997. Argument in artificial intelligence and law. *Artificial Intelligence and Law* 5, 4 (1997), 249–261.

[4] Yoshua Bengio, Réjean Ducharme, Pascal Vincent, and Christian Jauvin. 2003. A neural probabilistic language model. *Journal of machine learning research* 3, Feb (2003), 1137–1155.

[5] David M Blei, Andrew Y Ng, and Michael I Jordan. 2003. Latent dirichlet allocation. *Journal of machine Learning research* 3, Jan (2003), 993–1022.

[6] Ilias Chalkidis, Ion Androutsopoulos, and Nikolaos Aletras. 2019. Neural Legal Judgment Prediction in English. *CoRR* abs/1906.02059 (2019). arXiv:1906.02059 http://arxiv.org/abs/1906.02059

[7] Oduwa Edo-Osagie, Beatriz de la Iglesia, Iain R. Lake, and Obaghe Edeghere. 2019. Deep Learning for Relevance Filtering in Syndromic Surveillance: A Case Study in Asthma/Difficulty Breathing. In *ICPRAM*.

[8] Oduwa Edo-Osagie, Iain Lake, Obaghe Edeghere, and Beatriz DeÂăLa Iglesia. 2019. Attention-Based Recurrent Neural Networks (RNNs) for Short Text Classification: An Application in Public Health Monitoring. In *Advances in Computational Intelligence*, Ignacio Rojas, Gonzalo Joya, and Andreu Catala (Eds.). Springer International Publishing, Cham, 895–911.

[9] Roger Guimerà and Marta Sales-Pardo. 2011. Justice blocks and predictability of us supreme court votes. *PloS one* 6, 11 (2011), e27188.

[10] Thorsten Joachims. 1998. Text categorization with Support Vector Machines: Learning with many relevant features. In *Machine Learning: ECML-98*, Claire Nédellec and Céline Rouveirol (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 137–142.

[11] Daniel Martin Katz, Michael J Bommarito II, and Josh Blackman. 2017. A general approach for predicting the behavior of the Supreme Court of the United States. *PloS one* 12, 4 (2017), e0174698.

[12] Siwei Lai, Liheng Xu, Kang Liu, and Jun Zhao. 2015. Recurrent Convolutional Neural Networks for Text Classification. In *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence (AAAI'15)*. AAAI Press, 2267–2273. http://dl.acm.org/citation.cfm?id=2886521.2886636

[13] Reed C Lawlor. 1963. What computers can do: Analysis and prediction of judicial decisions. *ABAJ* 49 (1963), 337.

[14] Quoc Le and Tomas Mikolov. 2014. Distributed representations of sentences and documents. In *Proceedings of the 31st International Conference on International Conference on Machine Learning - Volume 32 (ICML'14)*. JMLR.org, II–1188–II–1196. http://dl.acm.org/citation.cfm?id=3044805.3045025

[15] Sangno Lee, Jaeki Song, and Yongjin Kim. 2010. An empirical comparison of four text mining methods. *Journal of Computer Information Systems* 51, 1 (2010), 1–10.

[16] Zhenyu Liu and Huanhuan Chen. 2017. A predictive performance comparison of machine learning models for judicial cases. In *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, IEEE, 1–6.

[17] Andrew D Martin, Kevin M Quinn, Theodore W Ruger, and Pauline T Kim. 2004. Competing approaches to predicting supreme court decision making. *Perspectives on Politics* 2, 4 (2004), 761–767.

[18] Masha Medvedeva, Michel Vols, and Martijn Wieling. 2018. Judicial Decisions of the European Court of Human Rights: Looking into the Crystal Ball. In *Proceedings of the Conference on Empirical Legal Studies*.

[19] Masha Medvedeva, Michel Vols, and Martijn Wieling. 2019. Using machine learning to predict decisions of the European Court of Human Rights. *Artificial Intelligence and Law* (26 Jun 2019), 1–30. https://doi.org/10.1007/s10506-019-09255-y

[20] Tomas Mikolov, Wen-tau Yih, and Geoffrey Zweig. 2013. Linguistic Regularities in Continuous Space Word Representations. In *Proceedings of the 2013 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*. Association for Computational Linguistics, Atlanta, Georgia, 746–751. https://www.aclweb.org/anthology/N13-1090

[21] Marie-Francine Moens, Erik Boiy, Raquel Mochales Palau, and Chris Reed. 2007. Automatic Detection of Arguments in Legal Texts. In *Proceedings of the 11th International Conference on Artificial Intelligence and Law (ICAIL '07)*. ACM, New York, NY, USA, 225–230. https://doi.org/10.1145/1276318.1276362

[22] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay. 2011. Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research* 12 (2011), 2825–2830.

[23] Claude Elwood Shannon. 1948. A mathematical theory of communication. *Bell system technical journal* 27, 3 (1948), 379–423.

[24] Richard Socher, Alex Perelygin, Jean Wu, Jason Chuang, Christopher D. Manning, Andrew Ng, and Christopher Potts. 2013. Recursive Deep Models for Semantic Compositionality Over a Sentiment Treebank. In *Proceedings of the 2013 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, Seattle, Washington, USA, 1631–1642. https://www.aclweb.org/anthology/D13-1170

[25] Karen Sparck Jones. 1972. A statistical interpretation of term specificity and its application in retrieval. *Journal of documentation* 28, 1 (1972), 11–21.

[26] Adam Wyner and Trevor Bench-Capon. 2007. Argument Schemes for Legal Case-based Reasoning. In *Proceedings of the 2007 Conference on Legal Knowledge and Information Systems: JURIX 2007: The Twentieth Annual Conference*. IOS Press, Amsterdam, The Netherlands, The Netherlands, 139–149. http://dl.acm.org/citation.cfm?id=1565610.1565629

[27] Yiming Yang and Xin Liu. 1999. A Re-examination of Text Categorization Methods. In *Proceedings of the 22Nd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '99)*. ACM, New York, NY, USA,42–49. https://doi.org/10.1145/312624.312647

[28] Zichao Yang, Diyi Yang, Chris Dyer, Xiaodong He, Alex Smola, and Eduard Hovy. 2016. Hierarchical Attention Networks for Document Classification. In *Proceedings of the 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*. Association for Computational Linguistics, San Diego, California, 1480–1489. https://doi.org/10.18653/v1/N16-1174

[29] Tong Zhang and Frank J Oles. 2001. Text categorization based on regularized linear classification methods. *Information retrieval* 4, 1 (2001), 5–31.

[30] Xiang Zhang, Junbo Zhao, and Yann LeCun. 2015. Character-level Convolutional Networks for Text Classification. In *Proceedings of the 28th International Conference on Neural Information Processing Systems - Volume 1 (NIPS'15)*. MIT Press, Cambridge, MA, USA, 649–657. http://dl.acm.org/citation.cfm?id=2969239.2969312

A Mixed-Method Approach to Understand and Improve Individual Participation Behaviour in Online Health Communities

Tenuche S. Bashir
Kogi State University, Anyigba
Kogi State, Nigeria
P.M.B. 1008
+234 8126826647
bashirtenuche@gmail.com

ABSTRACT
With the expansion of online communities, extant research in multiple disciplines have attempted to investigate its adoption and use among individuals. However, the biggest challenge encountered by managers of these communities is supplying knowledge, particularly, the willingness to share knowledge among the members.

Cancers figure among the leading causes of morbidity and mortality worldwide, with approximately 14 million new cases and 8.2 million cancer related deaths up till 2012. The number of new cases is expected to rise by about 70% over the next two decades. For this reason, there is an ever-increasing need to establish communities to offer empathic support to patients. To achieve its objectives, this study mainly adopts the Social cognitive theory and two components of the social influence theory. The study aims to provide insights on how and why patients diagnosed with cancer (and their relatives) seek social support using the Internet and social media. In particular, we seek to understand the motivation for joining and participating within these groups and the values derived from the community for the users both active and non-active.

CCS Concepts
• **Information systems → Social networking sites.**

Keywords
Online communities; online health communities; Social cognitive theory; Social influence.

1. INTRODUCTION
Over the years, individuals have changed their ways of seeking for information and engaging with different sources of information. The internet enables ubiquitous meeting spaces and hence satisfying an essential human need – communication. As a result, we observe new paradigms for communication, one of which is online communities [1]. Online communities and web 2.0 technologies are increasingly influencing the way individuals manage healthcare and chronic conditions. More people are looking to the internet for information and guidance on issues such as their conditions, experiences of others suffering from similar circumstances, treatment alternatives [2], [3], sharing of information and experiences and creating a link between patients and healthcare providers. OHCs, however, differ from other online communities because of their particular context and the uniquely personal nature of healthcare management, the healthcare setting usually introduces complexities that are not commonly found in regular online communities.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388190

1.1 Participation
Participation in OHCs has been defined differently by several authors, ranging from frequency of interaction to the intensity or level to which an individual engages with peers in the community [4]. Participation in online communities will provide access to unique benefits that solely exist within the community [5]-[7]; hence, when users participate actively they can be assured of more information and social benefits. However, the advantage of information derived is its utility to the individual seeking information [8], [9]. Information utility refers to the satisfaction an individual derives from the usability of an information source. Alternatively, some users participate by engaging in passive surveillance of information shared in the community, termed as lurking. In this situation, information distributed among peers is gathered, assimilated and evaluated by the individual.

1.2 Research Purpose and Problem Statement
Extant research in the community literature shows that participation leads to outcomes such as loyalty and satisfaction among members towards the online community. Overall, social media has made users who actively participate by generating and sharing content the key elements of any social media sire [12].Thus, the research question formulated and guiding the entire study goes: What factors drive users to participate actively in an online health community?

The objectives of the study, therefore, are to:

- Review literature in online community studies to identify and explore the characteristics of online communities, online health communities and the existing factors leading to active participation in online communities

- Identify online community among several communities, especially communities related to the present study, for data collection.
- Develop a framework to investigate the relationships that exist among all factors of social influence and social cognition on user behaviour.
- A field study involving quantitative data collection and qualitative interviews from specific health related online community
- Analyzing both phases of qualitative and quantitative data to provide more insight into user behaviour, within an online health community.
- Detailed results and findings to be able to inform managers of communities on best practices to keep the energy and enthusiasm within a community on the high.

1.3 Online Health Community Moderators

While the core values remain information and peer support [14], OHCs are increasingly incorporating experts who supply clinical knowledge and as well, to control the quality of information shared. Per a study by[14], only a few support communities engage experts as moderators.

[15] compared posts managed by health and administrative moderators. Their study found that health experts provided clinical advice and expertise (expertise from their training and personal experience), whereas administrative moderators shared patient expertise, and both of this expertise play crucial roles in the success of an OHC. It remains up to OHCs to consider how patients and health professionals can provide synergetic efforts to manage and sustain vibrant communities [14]. One avenue that has lacked necessary attention in the study of the success of support communities is through engagement with the individuals who manage the said community, There has been little attention in this area till date except for a few, for example, [16], whose study inferred that moderators had a range of altruistic and intrinsic motives for managing online groups [17]. The role of the health professional moderator still seems to be evolving. While the current study is relevant in exploring the roles and perception of moderators, the number of moderators considered is limited. Also, there is a limit to the extent we can generalize across several support groups and gain better insight into the processes of helping to shape up an online support group.

2. METHODS AND PROCEDURES

Case study: Macmillan Cancer community, Embankment, London, UK
Quantitative phase: Online survey
Respondents: 1511 responses, 866 members

A mixed-method approach was adopted for the study where a survey was sent out as part of the quantitative phase of the study, along with interviews with managers of the community.

Furthermore, the study adopts the social cognitive theory along with two facets of social influence to study individual behaviour within the community. SCT refers to human behaviour as a triadic, yet dynamic and reciprocal interaction among personal factors, the social network and the behaviour (Bandura;[28]). The principal determinants of the theory include knowledge, perceived self-efficacy that one can exercise control over oneself and habits, outcome expectations, about the expected consequences of any action taken. [28] discussed that of all the factors affecting human behaviour, standing on the basis are self-efficacy and outcome expectations. Self-efficacy is the belief in the capability of oneself to execute given tasks, and outcome expectations if a judgement of the likely result that will be produced from completed tasks [29]. Personal cognition involves user expectation and beliefs. These expectation/ideas are further categorized into two; self-efficacy and perceived outcome (which are the primary cognitive factors influencing the behaviour of a user).

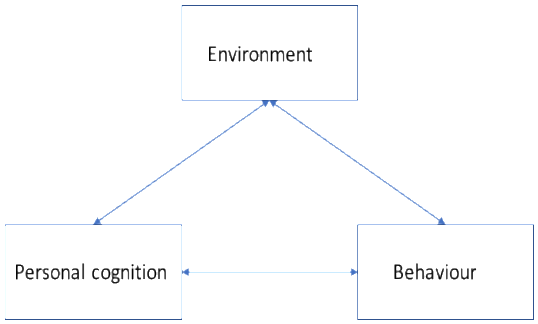


Figure 1. Shows the social cognitive theory and its relationships.

Though all determinants of self-efficacy are influential to user behaviour, it is important to realize that they become instructive only through cognitive appraisal [29]. Enactive Mastery: among most individuals, the result of performance i.e. mastery experience is the most influential source of efficacy beliefs. "This is because, mastery experiences provide direct performance information for the creation of stable and accurate efficacy beliefs" [30].

Vicarious Experiences: Per [30] otherwise termed as modelling, occurs when individuals observe competent and relevant people carry out a similar task and be rewarded and appraised for it. People may decide to turn to competent members or mentors to gain more knowledge on a given task, necessary skills or the necessary strategies to complete any task. Vicarious experiences occur when members of the community start to compare themselves with others regarding behaviour. When a user witnesses other users succeeding at something. Verbal Persuasion: persuasions from a trusted and competent other helps to strengthen self-efficacy. The purpose of enhancing efficacy beliefs by verbal persuasions has little to do in the aspect of increasing level of ability and skill. Rather the focus is on cognitive appraisal of individuals' self-efficacy regarding enhancing the personal beliefs of a person as to what they can accomplish by what they already have. Improvement in performance is achieved by the increased willingness to attempt a new task or to put in more effort on a current task. But persuasion "is not so much a matter of belief in one's ability to accomplish a task as of response willingness" [31].

Physiological and Psychological factors: this is a state of emotional arousal. This source of efficacy beliefs is important as individuals perceive it as signs of vulnerability and dysfunction [30]. Typically, the feeling of optimism in the face of stress and anxiety will enhance self-efficacy, whereas depression despondency and despair will only seek to diminish efficacy beliefs. According to Bandura, the intensity of user conditions or mood is hardly the case, as is the approach the individual lends to it. Members of OHCs with strong efficacy beliefs will approach a challenging and emotional state as energizing, and those who are overcome by feelings of self-doubt will find their state devastating.

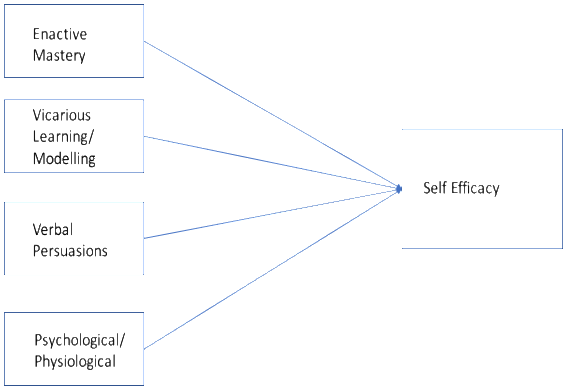


Figure 2. Shows the different Aspects of Self-efficacy.

Therefore;

- Self-efficacy is positively associated with active participation
- Mastery experience is positively associated with active participation
- Vicarious experience is positively associated with active participation
- Physiological/psychological factors are positively associated with active participation.

2.1 Outcome Expectations

Per [29] outcome expectations are made of three primary forms; Physical effects (pleasure and discomfort), social consequences (recognition, monetary rewards) and self-evaluation (self-satisfaction, self-devaluation). Within each of these forms, positive expectations are described as incentives; therefore, human behaviour can be regulated by the different types and their effects [29]. This ideology can be employed in the context of knowledge sharing because users will be more willing to participate when the rewards exceed the cost [32].

Personal outcome expectations entail user expectations such as personal image, respect from others, making friends in the community, and getting help and cooperation from other members, whereas community-related expectations (CROE) are about expectations of the user concerning the impact of his knowledge sharing in the community, helping to achieve the goals of the community, enriching the community knowledge base, etc. therefore,

- H1e: Personal outcome expectations are positively associated with active participation
- H1f: Community-related outcome expectations are positively associated with active participation

Extant studies in IS have shown that there is a significant relationship between self-efficacy and outcome expectations. In a survey carried out by [33], they found that self-efficacy is strongly associated with performance-related outcome expectations and personal outcome expectations. Also, [34] explained that self-efficacy has a positive influence on user performance which also affects the outcome the user expects. Therefore

- H3: Self-efficacy is positively associated with personal outcome expectations
- H4: Self-efficacy is positively associated with community-related outcome expectations.

With respect to the environmental factors affecting behaviour, compared to traditional offline communities, virtual communities are freed from the temporal and spatial limitations and provides communication convenience to its users [35], Yet, because of its anonymity, virtuality and lack of effective assurance mechanisms, some potential risks surround it's use. The present study views the role of the environment as trust. Trust is an inherent set of beliefs that individuals will abstain from opportunistic behaviours and not take advantage of one's situation [36]. When rules and regulations are insufficient to guarantee users that other individuals will behave the right way as expected as is often the case in virtual communities [37], trust serves as a convenient substitute, by creating an atmosphere that will make engagement with other community members more open [37], thus, trust rules out unwanted, undesirable, opportunistic behaviours among users of the community [38].

- H1a: Trust is positively associated with active participation

[39] motivation to examine social influence and its effects came out of his interest in understanding the changes brought about by external inputs to the attitude of an individual. Specifically, his study was directed towards understanding if attitude change resulting from external factors was temporary and superficial or a more lasting change that could become integrated, within the individual's value system. Per [40], Social influence is the change in the thoughts, feelings and attitudes or behaviours of an individual because of interaction with another person or group who share similar interests/beliefs, are desirable or are experts. It is common, studies show, for individuals to adjust their beliefs on other users to whom they feel similar to by psychological principles. [41] further distinguished the various processes of influence to be compliance, identification and internalization.

Each of the three processes represents a qualitative way of accepting influence.

[42] found that compliance did not have any effect on user behaviour because participation in an online community is usually voluntary and anonymous, members are free to come in and go as they please, so in most cases, members do not feel the need to comply with opinions and expectations of others. [43] showed that compliance might influence intention to participate; however, this effect will be overshadowed by the effects of the other two social processes (Identification and internalization). In their study, [44] found that when social influences generate a feeling of compliance, the resulting effect is negative on the users' attitude toward the new information systems. For this reason, the present study has not considered the effect of compliance on user behaviour. Social identity is the part of an individual's self-concept derived from knowledge of his membership of a social group together with the emotional significance attached to that membership [45]. Regarding the social identity theory, individuals define themselves regarding their social environment [46]; [47]. In the present study identification represents a personal sense of belonging and feelings of connection or having a positive feeling toward the community. [48] discussed three components that contribute to an individual's social identity: **a cognitive component**: evident during self-categorization. In an online community, members of the community develop a sense of awareness of community membership, which includes factors of similarities with members and dissimilarities with non-members [42]., **an evaluative component**: Evaluative identity, it the individual's group-based or collective self-esteem, defined as the evaluation of self-worth as it relates to belonging to the community [42], it reflects the perceived value of the user, and importance as a member of the community [43]. And **an emotional component**: suggests a sense of emotional attachment

with other members of the group, which is also referred to as affective commitment. This component fosters loyalty and citizenship behaviours in group settings [49]; [42].

- H2.1: Cognitive identification is positively associated with active participation
- H2.2: Evaluative identification is positively associated with active participation
- H3.3 Emotional identification is positively associated with active participation

Internalization or group norm are defined as an understanding of and commitment by an individual member to a set of goals, values, beliefs and conventions shared with other group members [42]. Group norms are agreements among members about their goals, shared values and expectations [43], this component is relevant to online communities as it represents group-related information and will regulate member interaction [42]. Users gain more understanding about group goals, values and conventions when they join the community, overtime; they perceive community norms through continuous long-term interaction. In another sense, studies have shown that group norms promote a cooperative motivational orientation among group members, when it becomes apparent that their values and goals are consistent with the community, they form active participation. Therefore

- H2b: Group Norm is positively associated with active participation

Group norms increase user inclination to mutually accommodate their schedules and activities with other to be able to engage in group actions and unanimity [42], this will lead the users to believe they have been accepted and are valid members of the community. When users realize this, they will develop a sense of trust, a willingness to be vulnerable to other members with the expectation of getting the same treatment from the other party.

- H7 Group norm is positively associated with trust

Social interactions are associated with intimacy and reciprocity in communication among members of the community. This interpersonal trust differs from system trust, which pertains to the willingness to rely on an OHC system [50]. Social interactions encourage and increase confidence among the members of the community. Per [51], when members trust one another and the system, it influences their confidence in the community in general, and consequently, an individual's general confidence in an OHC affects his attitude towards the community and the degree to which he/she likes or dislikes the community [50]. Studies have shown that OHC members through identification will share hobbies, goals and lead other members with shared interests and similar values, feelings, beliefs and behaviours in the community. Identification among members therefore, improves trust and accelerates their trust to the messages exchanged within the groups they belong to

- H7a: Community identification is positively associated with trust among members.

3. PROCESSES AND OUTCOMES

Hierarchical multiple regression using the Enter method was employed for the study to investigate the extent to which the facets of our theories (processes and predictors) could explain the outcome, over and above the background variables. As a first step, we calculated the cumulated results of a bivariate Pearson correlation test. Indicated there are the degrees of association among the elements of social cognition - trust, outcome expectations (personal and community-related outcome expectations), self-efficacy – and the elements of social influence - Identification and internalization. Then, Pearson's correlation coefficients were calculated to identify which background variables and what processes correlate with each of the outcomes and can, therefore, be included in the model. The R2 value for the first model in the regression analysis showed that the six variables of social cognitive theory explained 15.6% of the total variability in the model and as for the second model, after including the variables of identification and internalization from the social influence model, explained 15.7% of the total variability of the predictors to the outcome, participation. The F values indicate there are highly significant relationships between the variables of social cognitive theory and the variables of social influence theory. Both models presented significant relationships in the ANOVA table showing the F change as: First model, $F(7, 714) = 20.107$, $p < 0.001$, second model, $F(10, 711) = 14.469$, $p<0.001$. Throughout the analysis, trust was a significant predictor of all outcomes it was regressed against ($p<0.001$ to $p<0.01$). Self-efficacy as discussed in previous chapters involved: mastery experience, vicarious learning, physiological reactions, the effects of self-efficacy on user participation seemed to vary from one study to another. [29] insisted on the importance of self-efficacy, as a useful hypothetical construct for predicting behaviour, other studies including [31] have stated that self-efficacy may be a predictor of behaviour but has no claim to being the cause of behaviour. Physiological self-efficacy was not a significant predictor in all analysis where it was used as an independent variable.

Being a hierarchical regression, all predictor variables were not entered simultaneously, hence the need to include variables measuring identification (cognitive, emotional and evaluative social identity) and internalization (group norm) into the model to witness the effect these variables have on the entire model and the dependent variable. Internalization is a significant predictor of user participation ($p<0.01$)

3.1 Self-Efficacy on Outcome Expectations (Personal)

Self-efficacy had little variance on the overall variation of the outcome expectations, accounting for only 10% of the variance. Mastery experience and vicarious learning have significant relationships on the users' perception of the possibility of getting favourable personal outcomes (after carrying out behaviours) $p < 0.01$ and $p< 0.001$. Physiological Self-efficacy had no significant relationship, with personal outcome expectations, revealing that users who feel they have a good sense of their conditions or understand their conditions and needs do not necessarily feel the need to make friends and find more support within the community. On the other hand, users who believe in their skill sets (mastery experience) and the belief of being able to accomplish tasks based on the ability of other users to accomplish similar tasks (vicarious experiences) are more open to making friends and engaging more with other members of the community.

3.2 Self-Efficacy on Community-Related Outcome Expectations

Similarly, mastery experience and vicarious learning have significant relationships with the perception of the user to contribute actively to the community, enriching community knowledge base and maintaining community operation, $p< 0.01$ and $p< 0.001$. On the other hand, users who believe they have a good sense of their conditions and feel they understand their

condition and needs also don't feel the need to engage in active content contribution or increasing community knowledge.

3.3 Self-Efficacy on Trust

Mastery experience, vicarious learning and physiological self-efficacy were all regressed against the environment – represented by trust. From the outcome of the regression analysis, users who are confident about posting to the community have no need to develop any trust for the other members of the community or the environment. Vicarious learning and physiological experiences as forms of self-efficacy have significant relationships with trust. Users who are confident about surfing the internet but do not necessarily post information may require more trust and some form of connection with other members of the community. Similarly, users who are more aware of their condition and users who feel they have a good understanding of their condition or needs also have a significant relationship with the trust. Hence this category of users feels the need to express their feelings and support and hope to get it back from members of the community. Trust has a significant relationship with all forms of self-efficacy ($p<0.001$), the effect of the environment on the user is indicative of all outcomes derived from the study; indeed, studies show that environmental factors influence personal cognition (Zhou, 2008).

3.4 Social Influence and Environment (Trust)

Trust has a significant relationship on internalization. Users who have trust and feel support from the members of the community can more easily integrate their norms and values with the values of other members of the community. The environment, represented by trust, accounts for 30% of the total variance of internalization and is significant at $p<0.001$.

Internalization and emotional, social identity both had significant relationships with trust with $p<0.001$ and $p<0.05$. Members of the community who are willing to share their values with other members, in the form of accepting the norms and values of the community will develop or increase their trust in the environment, and hence with other members of the community. Users who identify as undergoing treatment or have recently undergone treatment, are willing to integrate with other similar users, they want to identify with similar others and share experiences with them, develop an emotional involvement, hear about their experiences, develop a sense of belonging and attachment with these users. This emotional connection fosters trust among members and can lead members to cultivate loyalty towards the community [43], as evident in the Macmillan community, where some users have decided to become volunteers, after caring for other members. In a cognitive sense, users form categories with the existing members and see where they fit, a phase where the individuals form a self-awareness of virtual community membership [42];[52]. The results show no significant relationship between cognitive/evaluative identity on trust. Evaluative social identity explains the user's perceived value, importance and evaluation of self-worth to the community. This category is represented by users who have been carers in the past, and have lost a friend or family to cancer. This group even though they develop a social identity with others in their circle, they do not seem to connect with the environment i.e. the trust factor, is restricted to a small circle.

The **second phase** of the study involved a total of three in-depth interviews conducted with the managers of the community to

- Understand their experiences and how they view the behaviours of members of the community.
- Explore the methods used by community managers to foster participation

The qualitative analysis was somewhat exploratory, in nature. The interview was conducted at the premises of the organization (Macmillan), as face to face interviews with open ended questions. Each interview in its entirety lasted about 50 minutes and was recorded and transcribed for further analysis. Findings from the interview data collected were integrated and will be used as a basis to account for the role of the managers on the community and existing methods in place to foster participation.

3.5 Identifying the Roles of Managers

A careful approach adopted by the managers of the community has been the use of "peer moderators"- these are members who facilitate discussions on voluntary basis. These moderators are used to engender trust, encourage trust and plant the seeds of the community (Sloan, review, 2000). This study focused on the factors determining the roles of the managers only, and not the peer moderators to elicit the functions and behaviours of the both parties separately. This theme represents the attempts of the managers as lead moderators to reinforce participation etiquette and forum rules, redirect patients to relevant fora, warn patients about the credibility of information and dangers of unreliable information, motivations and appraisals to the members of the community. There are very few instances of having to moderate where members have been misbehaving with language, or sometimes they get cross but it's quite calm." The champs who represent the most active 1% of the community are well valued in the community. The managers take it as serious business to keep in touch with the and show how much they are cared for.

4. CONCLUSION

4.1 Community Members

Macmillan has considerably, a much greater female population than the men 78% to 22% respectively, three times

the total male population of members. The highest population of members in the community fall in members who have just undergone a series of treatment (46%), members who are currently undergoing treatment (28%), and finally members whose friend or family died of cancer (26%) or friend/family affected by cancer (18%). These groups will probably have more information to share if they choose to, a result of the direct experience they have had with the illness.

4.2 Reasons for Participation

Online support communities offer support to individuals by providing access to valued resources that members can share among one another (Butler, 2001; Johnston, A. C., et al, 2013). Contrary to other lean sources of information such as Wikipedia and health information sites, these communities provide users with valuable information e.g. personal health experiences, personal success stories that can serve as a confidence boost and increased knowledge for its members. Secondly, online support communities offer intangible benefits to its members through emotional support and self-development. Family and friends can serve as support structures under normal circumstances, yet some users are still uncomfortable with information shared, unable to express their feelings to one who has no direct experience with cancer. Online health communities serve as a renewable source of support due to shared affiliation and a sense of belonging and attachment, gained from struggling together, through their medical issues.

In both phases of the study, information sharing was a very vital part of user needs. 76% of the members of the community claim they use the website to get information, 60% are there to get support. The managers of the community have realized this fact and are working hard to ensure adequate information and support is offered to members, for example, they constantly try to find tips from the community and put them in the blog. As for members of Macmillan who are affected by cancer, the community is a convenient medium to communicate with other members who are dealing with the similar issues directly or indirectly.

4.3 The value of knowledge and Information sharing: Expertise, Information Credibility, Accessibility, Restrictions, Signposting

Information is one of the major factors that keeps an online community thriving, without rich knowledge, participation would be low as so many users are only around to acquire more information. Member generated content is of great value, though difficult to stimulate, it is this characteristic more than any other that defines a virtual community (Chiu et al., 2006). One of the ways managers have addressed this is by constantly feeding off information to users, firstly, to cater for the needs of the users who have asked about a certain information, and secondly for the users who prefer just to read posts, and derive some value from reading. In areas that do not benefit from greater expertise, there are question and answer sessions or web chats, nurse experts that join the community to respond to the questions two times a week. More hands would help to keep up with these daily, i.e. constantly meeting information needs. In some cases, members are encouraged to leave questions, and experts answer them subsequently – a section in the community called "ask the experts". The intention of the management of the community is to get the section staffed by nurses for the support line to answer more medical questions. Another method used by the managers to diffuse information into the community is by identifying and picking up relevant tips from the community and put them in the blog, for example, advice about hair loss and how to manage it, the use of scarfs or even grabbing a magazine and this information are stored in one place for the members, etc. So, if other potential members or just internet surfers want to find information online, it will be found on Macmillan community, this will aid onboarding as it is a means to direct more individuals to the community. A common problem is the volume of information that is all spread out; the managers try to bring this information together so the user can see in a more user-friendly way.

The managers try to ensure there is adequate information to meet the needs of as many users as possible. Questions posed by other members are posted on the featured contents, a section Of the platform that displays useful information and essential tips. They ensure that there is a constant flow of information without crossing the lines, there are rules about the kind of information and quality of information given out to members because many of the members are vulnerable and will go with anything at all that gives value.

The credibility of the information posted on the forums is regularly scrutinized. Though at the moment, the managers agree they cannot look through all daily threads, they try to look through as many as they can to ensure no one is getting unchecked or unconfirmed information from peers. Most members of the community as stated earlier tend to be needy and vulnerable, their physical and mental states often lead to the feeling of wanting more support whether information or social support, however - how reliable is the information they consume? The guidelines of the community strictly note the zero tolerance approach the community has, to false information and the managers and peer moderators understand they only offer support and not any form of medical advice. The community signposts users to the health line or support line for queries that need medical advice.

4.4 Factors leading to active participation in the community

The study revealed that factors such as Trust, Self-efficacy, Personal Outcome Expectations, Internalization, Reciprocity, Social Interaction ties, all aid in improving user participation within the community.

However, Lurking can be viewed as significantly less optimistic than active participation, yet it must not be construed as a negative behaviour. [53] explained from their study of lurkers that users lurk for valid reasons. The present study showed 54 % of users are satisfied with just reading posts, in line with previous studies on the behaviour of lurkers in online communities, however, the values derived alone with their experiences remain less satisfying and less engaging. Active participation, a process of contributing content, is an evident trend among some of the members of the community, though the study did not consider the quality of information shared among these active members, more than half of the respondents of the study claimed to have participated at one point or another 67%. Where only 26% have admitted to not participating or sharing any information whatsoever. Per [2] active participation is a gateway to both information and social support. However, it is a known fact in community behaviour that some individuals participate by engaging in passive surveillance of information, termed as Lurking.

4.5 Limitations of the study

Research shows that the empirical studies of user participation in online communities have focused mainly on the most active and most dominant members of online communities who in the real sense represent a tiny percentage of community members. Rather than centering on the quantity of information shared, there should be more attention on the quality of information shared. The present study attempted to investigate factors that could lead to increased participation, but has not taken into consideration the quality of information shared at the moment, but rather, the quantity of information shared by already active users of the community. Members of the community used in this study, (Macmillan community) are vulnerable, also, geographical locations meant that the researcher could not arrange to get a hold of some members to discuss some of the issues posed in the research questions. Perhaps if the time-scale were longer, the possibility of travelling around to discuss with some members of the community in person would have been viable. Generalizing the results of this study may only apply to similar online health communities, to the community used in this study. The present study did not consider whether the severity of the conditions of users or the health stage of the participants affects their perceptions of the level of outcomes expected from the users. The Macmillan community constantly works to increase on-boarding within the community and a major challenge is being able to manage all different groups that exist within the general community. The groups include, breast cancers groups, lung cancer groups, carers groups among other. The present study has not considered the relationship between the types of cancer and the effect this has on active participation. Perhaps, cancer types

will influence user participation whether active or non-active (Lurking).

5. REFERENCES

[1] Stanoevska-Slabeva, K., & Schmid, B. F. 2001. *A Typology of Online Communities and Community Supporting Platforms*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.4946&rep=rep1&type=pdf

[2] Johnston, A. C., Worrell, J. L., Di Gangi, P. M., & Wasko, M. 2013. *Online health communities. Information Technology & People*. 26(2), 213–235. https://doi.org/10.1108/ITP-02-2013-0040

[3] Yang, L. and Tan, Y. 2010. *An empirical study of online supports among patients*, October 25, available at: http://ssrn.com/abstract=1697849 or http://dx.doi.org/10.2139/ssrn.1697849

[4] Nambisan, S. and Baron, R.A. 2009. *Virtual customer environments: testing a model of voluntary participation in value co-creation activities*. Journal of Product Innovation Management, Vol. 26 No. 4, pp. 388-406

[5] Burt, R.S. 1992. *Structural Holes: The Social Structure of Competition*. Harvard University Press, Cambridge, MA. 228 ITP 26,2

[6] Burt, R. 2004. *Structural holes and good ideas*. American Journal of Sociology, Vol. 110 No. 2, pp. 349-399.

[7] Burt, R.S. 2005. Brokerage and Closure: *An Introduction to Social Capital*", Oxford University Press, New York, NY.

[8] Adler, P. and Kwon, S.W. 2002. *Social capital: prospects for a new concept*. Academy of Management Review, Vol. 27 No. 1, pp. 17-40.

[9] Nahapiet, J. and Ghoshal, S. 1998. *Social capital, intellectual capital and the organizational advantage*. Academy of Management Review, Vol. 23 No. 2, pp. 242-266.

[10] Ellison, N., Steinfield, C. and Lampe, C. 2007. 'The benefits of Facebook" friends: "social capital and college students' use of online social network sites', JOURNAL OF COMPUTER MEDIATED COMMUNICATION-ELECTRONIC EDITION-, 12(4), pp. 1143.

[11] Koh, J., Kim, Y. G., Butler, B., & Bock, G. W. 2007. *Encouraging participation in virtual communities*. Communications of the ACM, 50(2), 69–73

[12] Malinen, S. 2015. *Understanding user participation in online communities: A systematic literature review of empirical studies*. Computers in Human Behavior, 46, 228–238. https://doi.org/10.1016/j.chb.2015.01.004

[13] Ridings, C., Gefen, D., & Arinze, B. 2006. *Psychological barriers: Lurker and poster motivation and behavior in online communities*. Communications of the Association for Information Systems, 18.

[14] Huh, J., Mcdonald, D. W., Hartzler, A., & Pratt, W. 2012. *Patient Moderator Interaction in Online Health Communities*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3900205/pdf/amia_2013_symposium_627.pdf

[15] Hartzler, A. & Pratt, W. 2011. *Managing the Personal Side of Health*. J Med Internet Res 13, e62.

[16] Van Uden-Kraan, C. F., Drossaert, C. H. C., Taal, E., Seydel, E. R. & van de Laar, M. A. F. J. 2010. *Participation in online patient support groups endorses patients' empowerment*". Patient Education and Counseling, 74(1), 61–69.

[17] Coulson, N. S., & Shaw, R. L. 2013. "*Nurturing health-related online support groups: Exploring the experiences of patient moderators*". Computers in Human Behavior, 29(4), 1695–1701. https://doi.org/10.1016/j.chb.2013.02.003

[18] Zhang, Y. 2015. *Understanding the Sustained Use of Online Health Communities from a Self-Determination Perspective*. https://doi.org/10.1002/asi.23560

[19] Eysenbach, G. 2008. *Medicine 2.0: Social networking, collaboration, participation, apomediation, and openness*. Journal of Medical Internet Research, 10(3), e22. Retrieved from http://www.jmir.org/2008/3/e22/

[20] Preece, J. 2000. *Online communities: Designing usability, supporting sociability*. New York, NY: Wiley.

[21] Durant, K.T., McCray, A.T., & Safran, C. 2010. "*Modeling the temporal evolution of an online cancer forum*". In Proceedings of the First ACM International Health Informatics Symposium (pp. 356–365). New York: ACM.

[22] Massimi, M., Bender, J.L., Witteman, H.O., & Ahmed, O.H. 2014. *Life transitions and online health communities: Reflecting on adoption, use, and disengagement*. In Proceedings of the CSCW'14 (pp. 1491–1501). New York: ACM

[23] Wang, Y.-C., Kraut, R., & Levine, J.M. 2012. *To stay or leave? The relationship of emotional and informational support to commitment in online*

[24] *health support groups*. In Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work (pp. 833–842). New York: ACM.

[25] Rodgers, S., & Chen, Q. 2005. *Internet community group participation: Psychosocial benefits for women with breast cancer*. Journal of Computer-Mediated Communication, 10(4).

[26] Butler, B., Sproull, L., Kiesler, S., & Kraut, R. 2007. *Community effort in online groups: Who does the work and why*? In S. Weisband & L. Atwater (Eds.), *Leadership at a distance: Research in technologically supported work* (pp. 171–194). Mahwah, NJ: Lawrence Erlbaum Associates.

[27] Welbourne, J.L., Blanchard, A.L., & Wadsworth, M.B. 2013. *Motivations in virtual health communities and their relationship to community, connectedness and stress*. Computers in Human Behavior, 29(1), 129–139.

[28] Zhang, X., Liu, S., Deng, Z., & Chen, X. 2017. *Knowledge sharing motivations in online health communities: A comparative study of health professionals and normal users*. Computers in Human Behavior, 75. https://doi.org/10.1016/j.chb.2017.06.028

[29] Chiu, C.-M., Hsu, M.-H., & Wang, E. T. G. 2006. "*Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories*". *Decision Support Systems*, *42*(3), 1872–1888. https://doi.org/10.1016/j.dss.2006.04.001

[30] Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ, Prentice-Hall.

[31] Stajkovic and Luthans, F., 2002**.** *Social cognitive theory and self-efficacy: Implications for motivation theory and practice.* Viewed n.d., rom https://www.researchgate.net/publication/258995495

[32] Hawkins, R. M. F. 1992. Self-efficacy: A predictor but not a cause of behavior. *Journal of Behavior Therapy and Experimental Psychiatry*, *23*(4), 251–256. https://doi.org/10.1016/0005-7916(92)90047-M

[33] Constant, D., Kiesler, S., & Sproull, L. 1994. *"What's mine is Ours or is it? A study of attitudes about Information Sharing."* Information Systems research 5(4), 400 – 421.

[34] Deborah R. Compeau and Christopher A. Higgins. 1995. Computer self-efficacy: development of a measure and initial test. MIS Q. 19, 2 (June 1995), 189-211. DOI=http://dx.doi.org/10.2307/249688

[35] Johnson, R. D., & Marakas, G.M., 2000. *Research Report: The role of behaviour modelling in computer skills acquisition – Toward refinement of the model.* Information Systems Research, 11(4), 402-417.

[36] Zhou, T. 2008. *Explaining Virtual Community User Knowledge Sharing Based on Social Cognitive Theory*. In 2008 4th International Conference on Wireless Communications Networking and Mobile Computing (pp. 1–4). IEEE. https://doi.org/10.1109/WiCom.2008.2227

[37] Moorman, C., Zaltman, G., Deshpande, R., 1992. *Relationships between providers and users of market research: the dynamics of trust within and between organizations*. Journal of Marketing Research 29, 314–328.

[38] Ridings, C. M., Gefen, D., & Arinze, B. 2002. *Some antecedents and effects of trust in virtual communities*. *The Journal of Strategic Information Systems*, *11*(3), 271–295. https://doi.org/10.1016/S0963-8687(02)00021-5

[39] Luhmann, Niklas (1979) Trust and Power. Chichester: John Wiley.

[40] Kelman, H. C. 1974. *Further thoughts on the processes of compliance, identification, and internalization*. Perspectives on Social Power. J. T. Tedeschi. Chicago, Aldine Press: 126-171.

[41] Rashotte, Lisa Slattery. 2011. *Social Influence*. In the Concise Blackwell Encyclopedia of Sociology, P. 563. George Ritzer and J. Michael Ryan, editors. Oxford: Blackwell Publishing.

[42] Kelman, H. C. 1958. *Compliance, Identification, and Internalization: Three Processes of Attitude Change*? Journal of Conflict Resolution, 2, pp. 51-60.

[43] Dholakia, U. M., Bagozzi, R. P. and Pearo, L. K. 2004. "*A social influence model of consumer participation in network- and small-group-based virtual communities*". International Journal of Research in Marketing, 21: 241-263.

[44] Zhou, T. 2011. *Understanding Online Community User Participation: A Social Influence Perspective*

[45] Malhotra, Y., & Galletta, D. F. 1999. *Extending the technology acceptance model to account for social influence: theoretical bases and empirical validation*. In Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers (p. 14). IEEE Computer Society. https://doi.org/10.1109/HICSS.1999.772658

[46] Tajfel, H. 1974. *Social identity and intergroup behaviour*. Social Science Information, 13(2), 65–93. https://doi.org/10.1177/053901847401300204

[47] Tajfel, H., & Turner, J. C. 1979. *An integrative theory of intergroup conflict*. In W. G. Austin & S.

[48] Guan, M., & So, J. 2016. *Influence of Social Identity on Self-Efficacy Beliefs Through Perceived Social Support: A Social Identity Theory Perspective*. Communication Studies, 67(5), 588–604. https://doi.org/10.1080/10510974.2016.1239645

[49] Ellemers, N., Spears, R., & Doosje, B. 1999. "*Social identity: Context, commitment, content*". Oxford, UK: Blackwell Science.

[50] Bergami M, Bagozzi RP 2000. *Self-categorization, affective commitment and group self-esteem as distinct aspects of social identity in the organization*. Br J Social Psychology 39(4):555–577.

[51] Zhao, J., Abrahamson, K., Anderson, J. G., Ha, S., & Widdows, R. 2013. *Behaviour & Information Technology Trust, empathy, social identity, and contribution of knowledge within patient online communities*. Behaviour & Information Technology, 32(10), 1041–1048. https://doi.org/10.1080/0144929X.2013.819529

[52] Grabner-Kräuter, S., 2009. *Web 2.0 social networks: the role of trust. Journal of Business Ethics*, 90 (4), 505–522.

[53] Turner*, J. C. (1985). "Social categorization and the self-concept: A social cognitive theory of group behavior". In E. J. Lawler (Ed.), Advances in group processes (pp. 77–122). Greenwich CT7 JAI Press.*

[54] Nonnecke, B., Andrews, D., & Preece, J. 2006. *Non-public and public online community participation:*

Design and Develop Artifact for Integrating with ERP and ECS Based on Design Science

YungYu Lin
Knowledge Science,
Japan Advanced Institute of Science and Technology,
Nomi City, Japan
s1820034@jaist.ac.jp

Yukari Nagai
Knowledge Science,
Japan Advanced Institute of Science and Technology,
Nomi City, Japan
ynagai@jaist.ac.jp

TzuHang Chiang
Information Management,
National Chin-Yi University of Technology,
Taichung, Taiwan
biochiang@succmail.com

HuaKo Chiang
Knowledge Science,
Japan Advanced Institute of Science and Technology,
Nomi City, Japan
s1820015@jaist.ac.jp

ABSTRACT
From past studies about ERP, most researchers pay more attention to before or during implementing, only a few studies have investigated the situation after ERP implementation. Also, there are no practical results explored. Some researchers pointed out that communication and cooperation in the ERP system are important factors for improving performance in the post-implementation. Design Science focuses not only on a heretofore unsolved and important business problem but also creates artifacts to serve human purposes. In this paper, we show the post-implementation process between ERP and ECS through Design Science and go through the context model, activity diagram, sequence diagram of the Software Engineering to prove it is a systematic approach. Finally, we use metrics of Cyclomatic complexity and Halstead complexity to measure our artifact and give explanations and suggestions based on the measurement results.

CCS Concepts
• Information systems→Enterprise application.

Keywords
Design Science; Enterprise Resource Planning; Enterprise Collaboration System; SuccMail.

1. INTRODUCTION
There are several organizations implement the enterprise resource planning (ERP) system, the ERP system stressing that it can enhance various benefits for the organizations, such as share knowledge, share data, cut costs, and improve management of business processes [3]. Since a lot of researchers depicted ERP systems as a panacea in the literature, there are many reports of companies that run into costly implementations, suffer fatal difficulties, have to deal with maintenance issues and most of the organizations underestimate the complexity of implementing an ERP system[12]. Huang et al. put forward the top ten issues of ERP implementation and most of the issues are related to the communication, coordination and cooperation between each member in the organization [7]. More and more research focus on topics such as analysis ERP implementation and success factors of ERP implementation. However, it is a kind of endlessly repeated pattern [8, 13]. There are few researchers dig deeper into the involvement process to investigate that organizations use less than 70 percent of the ERP system capabilities and a rate between 65 and 85 percent failure of ERP system from their experience. Less than 35 percent of the promised benefits from the ERP system [6, 15]. From the literature and critical statistics, most of the organizations are not function well after implementation.

Besides the issues that came from ERP systems, there is a rising number of researchers advocated the communication and coordination among different roles and workers in the company are even more relevant than the use of specific tools for the purpose of accompanying integration workers [1]. Unfortunately, Only a few researchers put their effort into the investigation of ERP maintenance and enhancement activities [5]

This paper aims to follow the process of Design Science (DS) to design the artifact to integrate with the ERP system and the Enterprise Collaboration System (ECS). We filled the gap in the post-implementation and customization by the proposed artifact.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388193

2. RELATED WORKS
2.1 Design Science (DS)
The DS paradigm has its roots in engineering and the sciences of the artificial [17]. Essentially, it is a problem-solving paradigm. The prior research further illustrates an agreement about the difference between DS and other paradigms of research. Simon advocated the natural sciences and social sciences attempt to understand reality, design science attempts to create things that serve a human purpose [17].

As stated above in the introduction, most ERP researchers have focused on the object of study in the behavioral-science research. However, Lee mentioned that technology and behavior are not dichotomous in an information system, they are inseparable [9]. Philosophically these arguments draw from the pragmatists, as Aboulafia argues that truth (justified theory) and utility (artifacts that are effective) are two sides of the one coin and that scientific research should consider its practical implications for evaluation [2]. Since we discovered the gap and lack of ERP research, also the aim of DS is close to our purpose, we will reveal the guideline and nominal process about the DS in the Information Science (IS) research from two important and representative research [14, 18].

Hevner et al. [18] aim to describe the performance of DS research in information systems via a concise conceptual framework and clear guidelines for understanding, executing, and testing the

research. The position of this framework is that truth and utility are inseparable. K. Peffers et al. [14] proposed and develop a design science research methodology (DSRM) for implement IS depend on DS research. There are six activities in the DSRM process includes: Problem identification and motivation, Define the objectives for a solution, Design and development, Demonstration, Evaluation, and Communication.

2.2 Enterprise Resource Planning (ERP)

The ERP was born from its predecessor–Material Requirements Planning (MRP) in the 1990s. M. Babaei et al. [4] summarized two major benefits of the ERP system: (1) a unified enterprise view of the business; and (2) an enterprise database where all business transactions are entered, recorded, processed, monitored, and reported. However, as we studied the review of the last decade about the enterprise resource planning systems, we found worth pondering and insufficient parts in the ERP research. L. Shaul and D. Tauber [16] mentioned both the ERP life cycle and specific phase dimensions have revealed serious issues from the late 1990s until the last decade that the ERP research focused primarily on the early planning and implementation phases but neglected post-implementation. Unfortunately, until the last decade, there is still a shortage of research into post-implementation issues apparently and the strategies and methods required to address them, even this issue already existed and discovered in the late 1990s.

Meanwhile, with the ERP incorporates other business extensions such as supply chain management and customer relationship management, that research review mentioned the organizations continue to underestimate the complexity of implementing an ERP system. Also, most of the researchers announced that the ERP software itself does not cause the failure of ERP implementation, but high complexity from the massive change ERP causes in organizations [10].

3. DESIGN AND SYSTEM MODELING

In this section, we will follow the DSRM proposed by K. Peffers et al [14] and adequately refer to the additional material from seven guidelines addressed by Hevner et al. [18] . Meanwhile, we rely on software engineering to develop middleware to ensure our research follows the systematic approach.

3.1 Problem Identification and Motivation

From the widely used systematic approach of software engineering, the process of software specification extremely close to the purpose of problem identification and motivation. Hence, we apply the user requirements definition and system requirements specification to present a more specific definition about the problem identification and motivation in Table 1 and 2.

Before we step into the next process, we defined our artifact as a middleware since our artifact able to share the data with the systems in the context, provide the interface and carry out the desired program.

3.2 Objectives of the Solution

We infer the objectives of the solution from the problem identification and knowledge of what is possible and workable. First, from the system requirements 1.1 to 1.3, there were functions and specifications necessary to meet the requirements including the comprehension of ERP database schema, access authorization. Second, the artifact should able to provide an efficient way for operation and achieve the functionality for their ERP customization in the IMS. Third, to improve the communication and coordination among different roles and workers in the company, the artifact should able to process and generate precise information from the ERP database. Generated information can deliver to a specific system.

Table 1. User requirements definition

1.	The artifact shall able to integrate with existed ERP systems, process the complex data and generate precise information from the ERP database. After that, deliver the information to the ECS to enhance the coordination among different roles and workers in the company.

Table 2. System requirements specification

1.1	Ensure the artifact able to access an ERP database.
1.2	Transform the received requests into the raw database statements from an ERP database.
1.3	Conclude the inductive logic of an ERP procedure (i.e., request order process, purchase order process, etc.), and document the structure of relative tables in an ERP database according to the statements.
1.4	Provide an information middleman system (IMS) for achieving a more flexible way to operate and able to communicate with the ERP system and ECS for further customization.
1.5	Execute the statements (i.e., insert, update, delete) in the ERP database and request the data for generating precise information.
1.6	Generate the report from the specific operations in a portable document format and able to view/download it from the ECS.

3.3 Design, Development and Demonstration

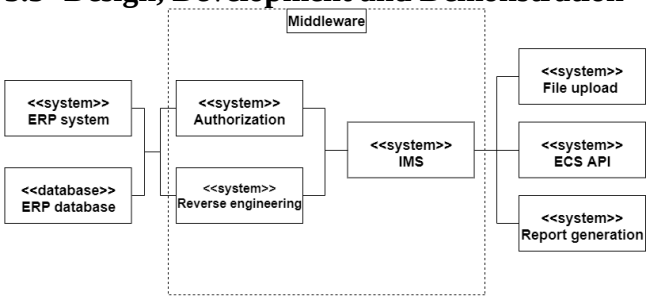


Figure 1. The context model of proposed middleware.

We illustrate the context model to decide the boundaries of the proposed middleware as Figure 1. The context models normally show the connected systems in the environment. Also, we used an activity diagram to show the business process of the proposed context model in Figure 2.

Reverse engineering system: The purpose is analyzing the ERP database schema. Before all else, there are two kinds of authentication should implement, one is for the database management system, the other is for the ERP system. For confirming the logic of authentication in the ERP system, we apply the Data Profiler to display all the executed statements from the database. While the user logins into the ERP system, the Data Profiler will display all the statements, and we can document the

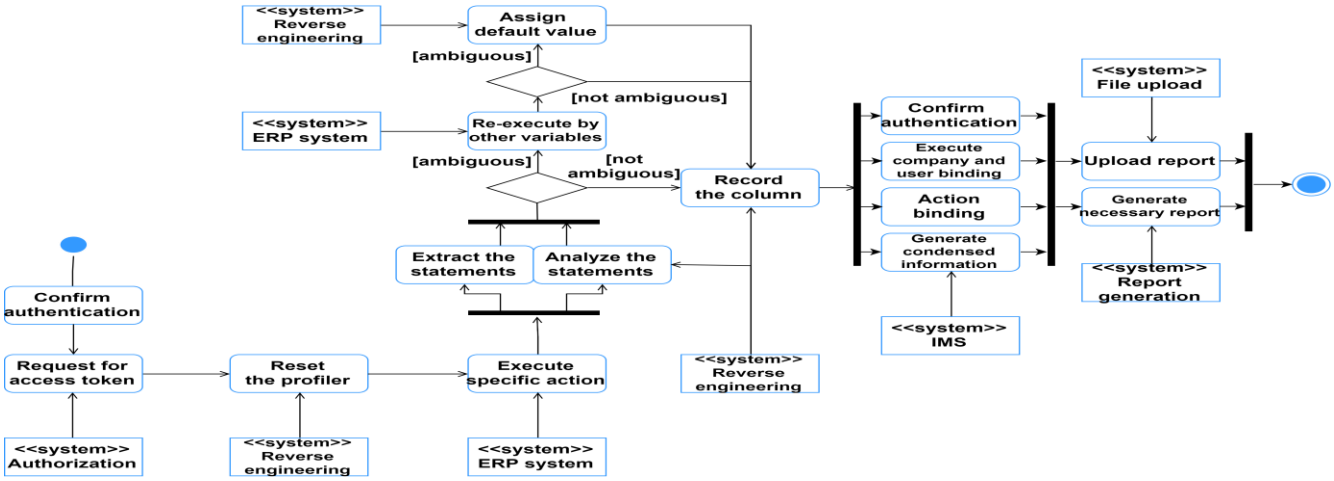


Figure 2. The activity diagram of the proposed context model.

related tables and attributes from the statements. According to our experiments in multiple ERP systems, we summarize two common cases from the schema of authentication as in Table 3.

Table 3. The cases of the authentication

1.	An ERP system might comprise multiple companies, and each company will have a standalone database to store all the information and apply a table to store authentication data.
2.	An ERP system might comprise multiple companies, and each company will have a standalone database to store all the information except authentication, they define the authentication table in an isolated database.

The backbone of the ERP system is its database. Hence, most ERP vendors will intentionally blur the database schema that the user unable to complete well in hand.

To overcome it, we carried out the operations (such as to request order process or purchase order process) in the ERP system and the executed statements will display on the Data Profiler. Based on the statements, we can confirm the related tables and estimate the logic behind the operation. However, you need to carry out the operation by different variables to confirm the schema repeatedly sometimes, such as duplicate attributes in a table. To our knowledge, duplicate cases usually arisen by currency attributes.

Authorization system: The purpose of the system is to verify the login information delivered from the IMS. If it acknowledges the request, it will return the auth token to the IMS. Therefore, the IMS able to communicate with the ERP system by token and identification.

Information middleman system (IMS): We apply the Model-View-Viewmodel (MVVM) architecture to establish this system. With the request order process which comprises initiation, login, user binding, company binding, create order and submit order modules. And we use a standard format including activity diagram, use case, and the sequence diagram to help designers identify objects in this system and give them an understanding of the intention. In Figure 3, go through the use case to describe what a user expects from the system in that integration. The sequence diagram provides the detail of the sequence of interactions and the summarized data as we described in Figure 4.

You can read the sequence diagram by the following descriptions:

- Using the instance AS to check the system's permission.
- The instance RE receives a request from the system to gain related schema from instance D. The system receives the schema and instance RE acknowledges receipt of this request.
- Both instances D and E receive a request for gaining data including items list, currency list, tax categories, warehouses, rule of order primary key and critical parameters of ECS, etc. Here we don't describe critical parameters one by one since it's case by case. However, the parameters for both company and user binding are necessary.
- Instance D receives a request for user binding by specific identification, in our case, we used an email address as identification for the user binding. Instance E returns the corresponding user to instance D and returns to the system for user binding.
- With company binding, it is like the user binding, and we treat the tax id number as the specific identification key.
- About the precise information, we encode the data into the HTML format string. It can deliver multiple purposes to implement, meanwhile, the user design and customized it depend on their case. Instance D receives query statements for executing the request order process. After confirmed the query statements successfully completed, instance D will receive the statements for adjusting inventory and carry out the request order process.

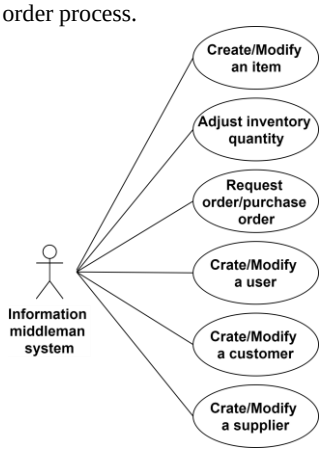


Figure 3. Use case involving the IMS.

From the above, we conclude the shortcomings of ERP from literature and knowledge and confirmed the explicit objectives of

solutions. We show the evaluation and discussion in the following section.

4. RESULT AND EVALUATION

We pick up one of the popular ECS in Taiwan, and through our artifact to integrate with the ECS and multiple ERP systems. The SuccMail (https://www.succmail.com) can access through its website and login by email address.

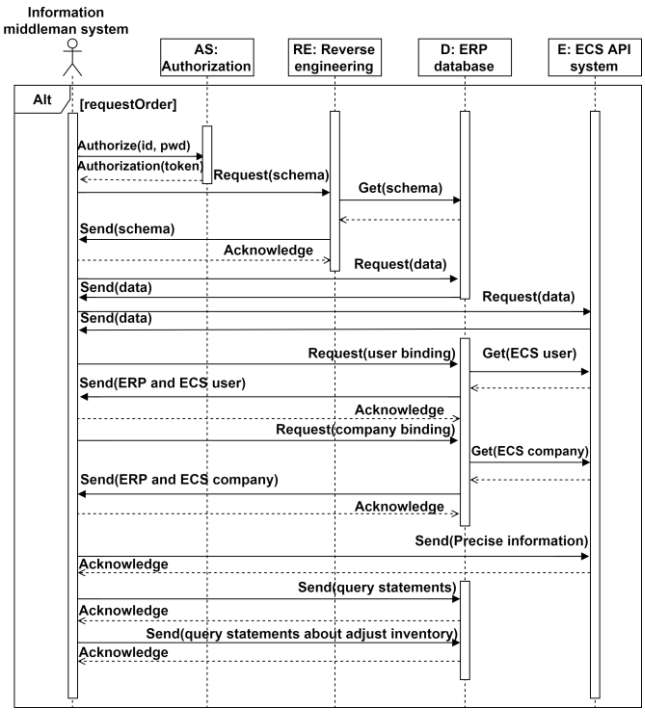


Figure 4. The sequence diagram of use case.

A maximum unit of the SuccMail is a company, and the participant can join multiple companies by one email address. A minimum unit is an event that comprises one subject and multiple replies to form a working item, and participants can go through putting the comment or confirm the informed message to achieve the purpose of communication. To verify that our method is workable and easy to design, we apply the metrics to discuss and test the artifact as described below.

$\eta_1 = the\ number\ of\ distinct\ operators$

$\eta_2 = the\ number\ of\ distinct\ operands$

$\mathrm{N}_1 = the\ total\ number\ of\ operators$

$\mathrm{N}_2 = the\ total\ number\ of\ operands$

Program vocabulary: $\eta = \eta_1 + \eta_2$

Program length: $\mathrm{N} = \mathrm{N}_1 + \mathrm{N}_2$

Halstead difficulty: $D = \mathrm{N} \times \log_2 \eta$

Halstead volume: $V = \frac{\eta_1}{2} \times \frac{\mathrm{N}_2}{\eta_2}$

Besides that, we apply Cyclomatic Complexity(G) to count the number of independent paths through the source code, and the Maintainability Index (MI) is an index value between 0 and 100. The MI between 20 and 100 indicate the program has good maintainability, between 10 and 19 indicate the program is moderately maintainable and between 0 and 9 indicate low maintainability.

$$MI = MAX(0, (171 - 5.2 \times \ln(V) - 0.23 \times G - 16.2 \times \ln(Lines\ of\ Code)) \times 100 / 171)$$

The abbreviation of the following metrics described in Table 4, and we summarize the metrics about six modules in Table 5. McCabe recommends developers should calculate the Cyclomatic complexity of the modules, and split into smaller modules while the value is larger than 10 [11]. Sometimes, the restriction may be permit modules with complexity as high as 15, however, it should provide a written explanation for exceeding limitation [19].

Table 4. The abbreviation of the metrics

P_loc	Physical lines of code
L_loc	Logical lines of code
M_pc	Mean parameter count
G	Cyclomatic complexity
G_density	Cyclomatic complexity density
M_index	Maintainability index
D	Halstead difficulty
V	Halstead volume

In our artifact, both the Create and Submit order module are greater than the threshold. We provide the following functions for each module, and further explanation is shown in Table 6 and Table 7.

Among the functions in the module of creating order, the highest Cyclomatic complexity value is 3, and most of the functions are used to detect changes in the user's operation base on ERP table structure. However, if we use the Halstead complexity for testing, the Halstead Difficulty is lower than the threshold value 30 and the Halstead Volume is also lower than the threshold value of 1500. According to the results, we find our artifact reduces the complexity of the ERP database structure.

Table 5. The metrics of each component in the information middleman system

Module	P_loc	L_loc	M_pc	G	G_density	M_index
Initiation	54	26	0.6	2	7.6923%	49.0113
Login	109	41	0.8571	6	14.6341%	41.4067
User binding	101	52	0.4444	8	15.3846%	39.4538
Company Binding	170	54	2	4	7.4074%	37.4294
Create order	583	236	0.9642	11	4.6610%	19.7719
Submit order	392	190	0.4	22	11.5789%	20.5823

Table 6. The functions in the module of creating order

No.	Function	P_loc	L_loc	G	G_density	D	V
1	constructor	13	10	1	10%	10.5	388.9735
2	generateERPIP	17	11	3	27.2727%	6.5625	192.718
3	onPriceChange	15	4	3	75%	6	147.1486
…	…	…	…	…	…	…	…
28	onRemarkChange	9	5	2	40%	4.1999	51.8914

Table 7. The functions in the module of submitting order

No.	Function	P_loc	L_loc	G	G_density	D	V
1	constructor	13	10	1	10%	10.5	388.9735
2	calculateTax	53	38	15	39.4736%	17.0526	801.4149
3	validateSheet	18	17	4	23.5294%	11.4287	334.4573
…	…	…	…	…	…	…	…
15	submitSheet	53	32	2	6.25%	10	1782.7837

*the calculateTax function is used for calculating the Value-added tax for each order.

*the submitSheet function is used for defining and generating precise information to the ECs.

The calculateTax function is the most complex one in the submit order module. However, the tax calculation is a very important part of the ERP system, even it is complex but necessary. In the same way, we did an assessment of the Halstead complexity and both difficulty and volume are lower than threshold too. In the submitSheet function, the Halstead Volume is higher than the threshold, it is because of the ECS defined multiple parameters to combine and merge the data to form the precise information. It mainly depends on the number of precise information.

5. CONCLUSION

In this paper, we highlight the contributions as below:

- We believe that this is the first research to construct a post-implementation and customization between ERP system and ECS using a complete methodology.
- Instead of providing case studies, we present a complete process for investigating the structure of various ERP systems. It will make our research results widely available to the development of communication between different ERP systems and ECS.
- We use design science as the basis for a research method and provide a more efficient and trustworthy way to develop through software engineering related definitions, models, flowcharts, etc.
- Finally, through a series of complexity indicators. It explains the function of the module whose complexity greater than the threshold. Based on the measurement, the subsequent researcher, developer and manager can catch the relevant details.

6. REFERENCES

[1] Abietar Lopez, M. et al. 2018. Professionals supporting employment: training and accompaniment in Work Integration Enterprises. *Ciriec-Espana Revista De Economia Publica Social Y Cooperativa*. 94, (Dec. 2018), 155–183. DOI:https://doi.org/10.7203/CIRIEC-E.94.12698.

[2] Aboulafia, M. 1991. *Philosophy, social theory, and the thought of George Herbert Mead*. SUNY Press.

[3] Almajali, D.A. et al. 2016. Antecedents of ERP systems implementation success: a study on Jordanian healthcare sector. *Journal of Enterprise Information Management*. 29, 4 (2016), 549–565.

[4] Babaei, M. et al. 2015. Challenges of Enterprise Resource Planning implementation in Iran large organizations. *Information Systems*. 54, (2015), 15–27.

[5] Botta-Genoulaz, V. et al. 2005. A survey on the recent research literature on ERP systems. *Computers in industry*. 56, 6 (2005), 510–522.

[6] Chou, H.-W. et al. 2014. Knowledge sharing and ERP system usage in post-implementation stage. *Computers in Human Behavior*. 33, (2014), 16–22.

[7] Huang, S.-M. et al. 2004. Assessing risk in ERP projects: identify and prioritize the factors. *Industrial management & data systems*. 104, 8 (2004), 681–688.

[8] Jiwasiddi, A. and Mondong, B. 2018. Analysing ERP Implementation Critical Success Factors for SME: A Study of SAP One Implementation in Jakarta. *Pertanika Journal of Social Science and Humanities*. 26, (Apr. 2018), 139–146.

[9] Lee, A. 2000. Systems Thinking, Design Science, and Paradigms: Heeding Three Lessons from the Past to Resolve Three Dilemmas in the Present to Direct a Trajectory for Future Research in the Information Systems Field,"Keynote Address. *Eleventh International Conference on Information Management, Taiwan* (2000).

[10] Maditinos, D. et al. 2012. Factors affecting ERP system implementation effectiveness. *Journal of Enterprise information management*. (2012).

[11] McCabe, T.J. 1976. A complexity measure. *IEEE Transactions on software Engineering*. 4 (1976), 308–320.

[12] Motiwalla, L. and Thompson, J. 2008. *Enterprise systems for management*. Prentice Hall Press.

[13] Nicoletti Junior, A. et al. 2018. Erp Implementation Project in a Brewing Manufacturer: The Quality Attribute as a Performance Differential. *Brazilian Journal of Operations &*

Production Management. 15, 4 (Dec. 2018), 517–527. DOI:https://doi.org/10.14488/BJOPM.2018.v15.n4.a5.

[14] Peffers, K. et al. 2007. A design science research methodology for information systems research. *Journal of management information systems*. 24, 3 (2007), 45–77.

[15] Rouhani, S. and Ravasan, A.Z. 2013. ERP success prediction: An artificial neural network approach. *Scientia Iranica*. 20, 3 (2013), 992–1001.

[16] Shaul, L. and Tauber, D. 2013. Critical success factors in enterprise resource planning systems: Review of the last decade. *ACM Computing Surveys (CSUR)*. 45, 4 (2013), 55.

[17] Simon, H.A. 2019. *The sciences of the artificial*. MIT press.

[18] Von Alan, R.H. et al. 2004. Design science in information systems research. *MIS quarterly*. 28, 1 (2004), 75–105.

[19] Watson, A.H. et al. 1996. *Structured testing: A testing methodology using the cyclomatic complexity metric*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Virtue Ethics as a Solution to the Privacy Paradox and Trust in Emerging Technologies

Adil Bilal
University of Canterbury
Christchurch
New Zealand, 8041
+6433693975
adil.bilal@pg.canterbury.ac.nz

Stephen Wingreen
University of Canterbury
Christchurch
New Zealand, 8041
+6433693975
stephen.wingreen@canterbury.ac.nz

Ravishankar Sharma
University of Canterbury
Christchurch
New Zealand, 8041
+6433692267
ravishankar.sharma@canterbury.ac.nz

ABSTRACT
Despite concerns over the collection of personal information by technologies, society's use of such has increased rapidly. This attitude is termed the privacy paradox. This research-in-progress explores the root causes of this privacy paradox, the role of personal information privacy threats on trust in emerging technologies, and the influence of unconscious decision-making (based on virtue ethics traditions) on conscious decision-making. To understand the duality and subjectivity embedded in the above issues, this study applies Q-methodology for data collection, analysis, and interpretation. The study proposes that virtue ethics is the best approach to solve such subjective issues. This study enhances our understanding, on the basis of prior literature, of the importance of virtue ethics as a solution to the privacy paradox.

CCS Concepts
• Security and privacy→Social aspects of security and privacy.

Keywords
Personal information privacy threats; emerging technologies; data ethics; virtue ethics; privacy paradox; unconscious-decision making; conscious decision making.

1. INTRODUCTION
Technological developments in modern times have driven the world to the verge of the fourth industrial revolution. This revolution is the outcome of different artificial intelligence (AI)-based emerging technologies (ETs), the Internet of Things (IoTs), Big Data, Augmented Reality, and Blockchain [34]. Unlike the prior industrial revolutions, this fourth one does not seem to bring along the passion people felt for new developments in the past. The ultimate reason for this lack of passion is "the great uncertainties and vicissitudes of technosocial life that lie ahead" [55]. Cath, Wachter, Mittelstadt, Taddeo, and Floridi [14] have observed that with the increase in the maturity of information societies, the impact of AI based technologies is increasingly rendered opaque. They have further asserted that "we are fragile entities, delicate systems, vulnerable individuals and AI can easily become the elephant in the crystal room, if we do not pay attention to its development and application." It is very important to understand the sociomateriality of this situation [41]. To do so, the first question that needs to be answered is: What are the factors that contribute to these growing concerns of techno-pessimists about the possible threats posed by AI based ETs?

There could be many conceivable factors behind this dilemma, but one possible factor is surveillance and the intrusion of these ETs; for example, assemblage of heretofore uncollectible information [38]. This information is thereafter likely to be used by the technologies' developers for machine learning. They will use it to develop powerful algorithms to predict human decision-making behaviour, in order to develop the AI's decision-making capability to be on par with humans [47]. This massive amount of data collection by ETs poses serious threats to the personal information privacy (PIP) of the ETs' users [28]. Vulnerabilities in ETs and lack of transparent, flexible, and culturally adaptable data protection rules have made this situation worse. In addition, lack of regulations [54] and data ethics [24] add to the difficulties of the present situation.

Privacy is a human requirement and a core value of our society [23]. As such, it should be protected at any cost. Surprisingly, previous research has shown that society's use of new technologies has been increasing over time [5], despite the fact that their concerns over the loss of privacy that comes with these new technologies is also increasing. These concerns stem from the increasing instances of data breaches, and distribution of users' personal information to third parties by the technology giants. This trend of increased technology use despite mounting concerns over privacy loss is known as the "privacy paradox" or, to be more accurate, the "information privacy paradox" [31]. Previous studies have found that the reason behind the privacy paradox is the users' risk-benefit calculus-based decision-making [3, 16]. If we look into the users' logic behind these decision-making calculations, we will find that it is a whole decision science, not merely a paradox. When users find themselves in a situation where they have to decide whether or not to use or trust ETs, or whether to relinquish their PIP or not, they encounter a decision-making dilemma. Our research will show that during this crucial moment, users' decision-making skills, which they have honed throughout their lives, could help them solve this dilemma. The majority of the previous studies have tried to solve this paradox in the light of deontological and consequentialist ethical theories, also known as ethics of conduct theories [55]. On the other hand, there are scarce few studies that have tried to find the answer in light of the virtue ethics theory, also known as ethics of character theory. Advocates of virtue ethics argue that our decision-making

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388196

process is the outcome of our character dispositions and habits, which we have cultivated on the basis of our prior decisions and experiences [39]. If any decision is taken by a virtuous person – who while making a decision, primarily focuses on his character dispositions with wisdom based on the situation – then that decision will be a good decision [9]. But today, the technologies' users lack such dispositions and habits of a virtuous person. There are many reasons behind this problem. This decision-making fallibility is not merely a behaviour science issue. Instead, it is an ethical issue that should be reinterpreted through this lens, accordingly. This study will examine and address this issue in the light of virtue ethics theory.

2. THEORETICAL BACKGROUND

2.1 Emerging Technologies and PIP Threats

Ziegeldorf et al. [62] have described seven different types of PIP threats that ETs pose: identification, tracking, profiling, violating interactions and presentations, lifecycle transitions, inventory attacks, and information linkage. As yet, there is no known solution that can be used to guard against these PIP threats [3]. This is due to the vulnerable characteristics of the ETs, which might be potentially misused by hackers; such characteristics include the collectability of heretofore uncollectible information [15], invasiveness [28], invisibility [2], mobility [59], programmability [15], simplicity [10], ubiquity [26], network of networks, interconnectedness, and wireless network accessibility [61]. And this situation will worsen when these ETs become available small in size and large in numbers [63].

2.2 Trust in Emerging Technologies and Privacy Paradox

If potential PIP threats are posed by ETs, then how will people develop trust in ETs? To develop trust in ETs under such PIP threats means to relinquish on PIP. There are very limited number of studies that have addressed the issue of trust in technology and the privacy paradox. Surprisingly, the majority of these studies address the issue of trust in people (e.g., trust in technology providers, manufacture, developers etc.) in the name of trust in technology. Trust in technology means specifically trust in technology artefacts [37]. Further, in the case of trust in ETs, studies are scarce. Recently, Mazey [36] has addressed this issue in the light of PIP threats. There is another qualitative study by Lewan [32], which explains the views of different IT professionals regarding trust in ETs. The situation is similar in the case of privacy paradox research related to ETs.

Mcknight et al. [37] have compared the trust in people and the trust in technology constructs. They argue that in the case of trust development in people, the trustor's expectation from the trustee are: competence, benevolence, and integrity; while in the case of trust development in technology, the trustor's expectations from the trustee are: technology's functionality, helpfulness, and reliability. Furthermore, Mcknight et al. [37] have found, based on the empirical evidence, that technology artefact's features are the basic reasons behind the trust development in technology by technology users. They further argue that during the initial stages of trust development in technology, people analyses technology and its features through a calculus-based trust mechanism, along with the institution-based trust factors. When people find technologies more beneficial to use, they start to develop trust in technology. Mazey [36] found that similar propositions are true in the case of trust in ETs. Before extending trust relationships with ETs, people assess ETs' functionality, helpfulness, and reliability along with the other available second-hand knowledge in the market and on the internet. If this is, in fact, the case, how do people develop trust in technologies in the presence of PIP threats? Why they do not seem to care about PIP threats? Do they not have enough knowledge about what PIP threats are and how they can affect them? Previous research shows that people do care about their PIP and they have enough knowledge. But still, despite having PIP concerns, people like to use new technologies and this pattern of behaviour is growing over time [8].

2.3 Privacy Paradox and Calculus-based Decision-making

Smith & Lewis [49] define paradox as "contradictory yet interrelated elements that exist simultaneously and persist over time. Such elements seem logical when considered in isolation but irrational, inconsistent, and even absurd when juxtaposed." Similarly, previous research shows that the enthusiasm of society about acquiring and using new technologies is growing overtime, which adds motivation to technology giants to invest more in the technology sector, particularly in new technologies. At the same time, previous research shows, society has also raised its concerns regarding the intrusion of new technologies into privacy. When we compare and interpret the findings from these studies, we observe an illogical relationship between trust in new technologies and PIP concerns [11].

Many studies have discussed the reasons behind this paradox. These reasons include risk-benefit based privacy calculus [3, 20, 28, 29, 42, 43, 57]; under- or overestimation of the benefits and risks of using technologies [22]; immediate gratifications [1, 5, 30, 45, 46, 57]; the difference between the judgments of risks and benefits of using technologies [22]; habits [18]; privacy valuation failure [11, 33, 40, 52, 60]; and knowledge deficiency due to incomplete information [1, 5, 13, 19, 22, 35]. Additionally, some studies have identified different biases and heuristics which affect technology users' risk-benefit calculus-based decision making [1, 19, 22, 27, 44, 53, 60].

All these studies and theories have described the reasons behind the privacy paradox, but no one study is able to delineate a comprehensive solution to overcome this paradox. These studies simply explain and enhance the theoretical understanding of the privacy paradox. If someone tried to solve the paradox, he has ignored the instability and duality embedded in it, which causes the paradox to "lose its processual edge and its dynamic, time-sensitive, and path-dependent properties" [17]. Trust in technologies, relinquishing on PIP, and privacy paradoxes are critical issues that have been analyzed through epistemological lenses. These issues are subjective phenomena that require more close and in-depth attention if we are to understand them. Additionally, it has been observed that these issues have not been analyzed from an ethical perspective. As trust in technologies, relinquishing PIP, and the privacy paradox are the decision-making issues, Morris [39] believes that decision-making is not just rule-following or performing rational cost-benefit analysis. Instead, it is a process that consists of our beliefs, values, the nature of the problem, how we perceive the problem, prior decisions, availability of alternative options etc. Thus, to develop trust in ETs in the presence of PIP threats and the privacy paradox are decision-making fallibilities.

2.4 Virtue Ethics, Privacy Paradox and Trust in Emerging Technologies

Generally, ethical theories can be divided into two main categories: the ethics of character and the ethics of conduct. The

ethics of character centers on what sort of people we should be (i.e., virtue ethics), while the ethics of conduct focuses on what sort of actions we should perform (i.e., Kantianism) or what sort of rules we should follow (i.e., Utilitarianism). If we look back, all the studies that have attempted to solve the privacy paradox or tried to explain how users develop trust in existing/ETs, have solely followed Kantianism or Utilitarianism. Surprisingly, no one has focused on how these new technologies are impacting on an individual's personal values and their personal decision-making capability. This study proposes that if we want to live well with AI based ETs and retain our freedom, we must understand the trust in ETs in the presence of PIP threats and the privacy paradox phenomenon from a virtue ethics perspective instead of the Utilitarianism or Kantianism perspectives. Utilitarianism and Kantianism pay more attention to conscious decision-making while virtue ethics pays more attention to unconscious decision-making. As discussed above, a majority of the studies delineate the reason behind this privacy paradox as the individuals' rational calculus-based decision-making or conscious decision-making. Barth & De Jong [6] recommended, after conducting an in-depth literature review on the privacy paradox, that it is time to focus on unconscious decision-making along with rational conscious decision-making, to further understand the theoretical underpinnings and the other hidden elements behind the privacy paradox. The research on unconscious decision-making is becoming popular in the fields of psychology, social, behavioral, and information sciences [7, 8, 31, 48, 58]. The study by Becker et al. [8] is the only one that has heeded the call of Barth & De Jong [6] to research the role of unconscious decision-making in the privacy paradox. Becker et al. [8] have found that distractions affect unconscious decision-making and generate stimulus (i.e., mental shortcuts), which in turn influence the actual behavior of individuals, causing them to disclose their personal information. In the case of trust in technologies, particularly ETs, it is hard to find any study that has described the role of unconscious decision-making on trust in technologies in the presence of the privacy paradox. While Barth & De Jong's [6] call for research on unconscious decision-making is not new, it is a novelty in the area of privacy paradox and trust in technologies research. The focus of this study is to fill this research gap, using this novel concept

Several philosophers and psychologists have already worked on virtue ethics in the general context. They include Anscombe [4], Berberich & Diepold [9], Blasi [12], Ess [21], Frankl [25], Morris [39], Sjåstad & Baumeister [48], Stets & Carter [51], Vallor [55]. As discussed above, during the last three centuries, society, particularly Western society, was heavily influenced by Kantianism and Utilitarianism. The consequences of these ethical philosophies can be seen in every part of life, such as individuals' usage of conscious decision-making in regular undertakings. This could be the reason behind researchers' enormous focus on rational calculus-based or conscious decision-making process, instead of on unconscious decision-making process.

3. RESEARCH METHODOLOGY

This study is unique in a sense that it is going to shed a light on the privacy paradox and trust in ETs from a subjectivity (quantum) world view. Previously, the majority of studies have tried to understand the privacy paradox and trust in ETs purely from an objectivity viewpoint, but all were incapable of explaining why individuals disclose their personal information despite having PIP concerns and being well informed about increasing trends in data breach incidents. All studies have focused on conscious decision-making, which perfectly fit in the objectivity perspective but ignored the unconscious decision-making, which deals with subjectivity. Therefore, this study is going to use Q-methodology to understand the duality and subjectivity hidden in the aforesaid issues. Q-methodology helps to understand the subjective judgement of individuals and focus on the debate and contestation happening around the topic of research interest. Moreover, it helps to understand hidden structures based on the expression of individuals' personal view points [56]. Furthermore, Q-methodology naturally helps to investigate the community sensemaking phenomenon as it is rooted in concourse theory of communication, which deals in subjective communicability [50]. Nine scenarios have been designed to conduct the Q-methodology's ranking experiment.

4. EXPECTED CONTRIBUTION

This study seeks to contribute to the body of knowledge in multiple ways. Firstly, this study is the first of its kind to address the linkage between the privacy paradox and the trust in ETs through the theoretical lens of virtue ethics. Previous studies have mostly tried to understand these issues from the perspective of conscious decision-making, whereas this study focuses on unconscious decision-making. Secondly, the findings of this study will help psychologists, ethicists, and philosophers to understand how technologies are affecting character strengths and virtues of individuals, as well as how emerging technologies can offer opportunities to cultivate virtues and become virtuous. Thirdly, privacy regulation laws, though often framed in terms of protecting the users, are generally undermined by the same users' behaviour [8]. This study could help privacy legislative efforts. Understanding the reasons behind the privacy paradox and issues of trust in ETs by relinquishing on PIP through virtue ethics theory could help society, businesses, technology manufacturers, and governments in establishing acceptable regulations and data ethics. Hopefully, this will also provide guidance on redesigning ETs.

5. REFERENCES

[1] Acquisti, A. and Grossklags, J. 2005. Privacy and rationality in individual decision making. IEEE security & privacy. 3, 1 (2005), 26–33.

[2] Adams, M. 2017. Big Data and Individual Privacy in the Age of the Internet of Things. Technology Innovation Management Review. 7, 4 (2017), 13.

[3] Ahituv, N., Bach, N., Birnhack, M., Soffer, T. and Luoto, L. 2014. New Challenges to Privacy due to Emerging Technologies and Different Privacy Perceptions of Younger Generations: The EU PRACTIS Project. (2014), 001–023.

[4] Anscombe, G.E.M. 1958. Modern moral philosophy. Philosophy. 33, 124 (1958), 1–19.

[5] Bandara, R., Fernando, M. and Akter, S. 2018. Is the Privacy Paradox a Matter of Psychological Distance? An Exploratory Study of the Privacy Paradox from a Construal Level Theory Perspective. (2018).

[6] Barth, S. and De Jong, M.D. 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and Informatics. 34, 7 (2017), 1038–1058.

[7] Barth, S., de Jong, M.D., Junger, M., Hartel, P.H. and Roppelt, J.C. 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with

technical knowledge, privacy awareness, and financial resources. Telematics and Informatics. (2019).

[8] Becker, M., Klausing, S. and Hess, T. 2019. Uncovering the Privacy Paradox: The Influence of Distraction on Data Disclosure Decisions. Research-in-Progress Papers. (May 2019).

[9] Berberich, N. and Diepold, K. 2018. The Virtuous Machine-Old Ethics for New Technology? (2018).

[10] Birnhack, M. and Ahituv, N. 2013. Privacy Implications of Emerging and Future Technologies. (2013), 49.

[11] Blank, G., Bolsover, G. and Dubois, E. 2014. A New Privacy Paradox: Young People and Privacy on Social Network Sites. SSRN Electronic Journal. (2014). DOI=https://doi.org/10.2139/ssrn.2479938.

[12] Blasi, A. 1984. Moral Identity: Its Role in Moral Functioning, in edited by Kurtines, W. M. and Gewirtz, J. L. (Eds.), Morality, Moral Behavior and Moral Development (pp. 128–139). John Wiley & Sons, New York.

[13] Buck, C., Horbel, C., Germelmann, C.C. and Eymann, T. 2014. The unconscious app consumer: Discovering and comparing the information-seeking patterns among mobile application consumers. (2014).

[14] Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M. and Floridi, L. 2017. Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. Science and Engineering Ethics. (Mar. 2017). DOI=https://doi.org/10.1007/s11948-017-9901-7.

[15] Conger, S., Pratt, J.H. and Loch, K.D. 2013. Personal information privacy and emerging technologies. Information Systems Journal. 23, 5 (2013), 401–417.

[16] Culnan, M.J. and Armstrong, P.K. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science. 10, 1 (1999), 104–115.

[17] Cunha, M.P. e and Putnam, L.L. 2019. Paradox theory and the paradox of success. Strategic Organization. 17, 1 (Feb. 2019), 95–106. DOI=https://doi.org/10.1177/1476127017739536.

[18] Debatin, B., Lovejoy, J.P., Horn, A.-K. and Hughes, B.N. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of computer-mediated communication. 15, 1 (2009), 83–108.

[19] Deuker, A. 2009. Addressing the privacy paradox by expanded privacy awareness–the example of context-aware services. IFIP PrimeLife International Summer School on Privacy and Identity Management for Life (2009), 275–283.

[20] Dinev, T. and Hart, P. 2006. An extended privacy calculus model for e-commerce transactions. Information systems research. 17, 1 (2006), 61–80.

[21] Ess, C.M. 2010. Trust and New Communication Technologies: Vicious Circles, Virtuous Circles, Possible Futures. Knowledge, Technology & Policy. 23, 3 (Dec. 2010), 287–305. DOI=https://doi.org/10.1007/s12130-010-9114-8.

[22] Flender, C. and Müller, G. 2012. Type indeterminacy in privacy decisions: the privacy paradox revisited. International Symposium on Quantum Interaction (2012), 148–159.

[23] Floridi, L. 2016. On Human Dignity as a Foundation for the Right to Privacy. Philosophy & Technology. 29, 4 (Dec. 2016), 307–312. DOI=https://doi.org/10.1007/s13347-016-0220-8.

[24] Floridi, L. and Taddeo, M. 2016. What is data ethics? Phil. Trans. R. Soc. A. 374, 2083 (Dec. 2016), 20160360. DOI=https://doi.org/10.1098/rsta.2016.0360.

[25] Frankl, V.E. 1992. By Viktor E. Frankl - Man's Search for Meaning. Beacon Press.

[26] Galvez, R. and Gurses, S. 2018. The Odyssey: Modeling Privacy Threats in a Brave New World. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (London, Apr. 2018), 87–94.

[27] Gambino, A., Kim, J., Sundar, S.S., Ge, J. and Rosson, M.B. 2016. User disbelief in privacy paradox: Heuristics that determine disclosure. Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (2016), 2837–2843.

[28] Hoehle, H., Aloysius, J.A., Goodarzi, S. and Venkatesh, V. 2018. A nomological network of customers' privacy perceptions: linking artifact design to shopping efficiency. European Journal of Information Systems. (Jul. 2018), 1–23. DOI=https://doi.org/10.1080/0960085X.2018.1496882.

[29] Kehr, F., Wentzel, D. and Kowatsch, T. 2014. Privacy paradox revised: Pre-existing attitudes, psychological ownership, and actual disclosure. (2014).

[30] Kim, D.H., Sung, Y.H., Lee, S.Y., Choi, D. and Sung, Y. 2016. Are you on timeline or news feed? the roles of facebook pages and construal level in increasing ad effectiveness. Computers in Human Behavior. 57, (2016), 312–320.

[31] Kokolakis, S. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security. 64, (2017), 122–134.

[32] Lewan, M. 2018. The role of trust in emerging technologies. The Rise and Development of FinTech. Routledge. 111–129.

[33] Lutz, C. and Strathoff, P. 2014. Privacy concerns and online behavior–Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. Viewing the Privacy Paradox Through Different Theoretical Lenses (April 15, 2014). (2014).

[34] Maple, C. 2017. Security and privacy in the internet of things. Journal of Cyber Policy. 2, 2 (May 2017), 155–184. DOI=https://doi.org/10.1080/23738871.2017.1366536.

[35] Martin, K.E. 2015. Ethical issues in the big data industry. MIS Quarterly Executive. 14, (2015), 2.

[36] Mazey, C.H.L. 2018. Initial Trust in Emerging Technologies and the effect of threats to Privacy. University of Canterbury.

[37] Mcknight, D.H., Carter, M., Thatcher, J.B. and Clay, P.F. 2011. Trust in a Specific Technology: An Investigation of Its Components and Measures. ACM Trans. Manage. Inf. Syst. 2, 2 (Jul. 2011), 12:1–12:25. DOI=https://doi.org/10.1145/1985347.1985353.

[38] Minkkinen, M., Auffermann, B. and Heinonen, S. 2017. Framing the future of privacy: citizens' metaphors for privacy in the coming digital society. European Journal of

Futures Research. 5, 1 (Dec. 2017). DOI=https://doi.org/10.1007/s40309-017-0115-7.

[39] Morris, T. 1998. If Aristotle Ran General Motors. Holt Paperbacks.

[40] Oetzel, M.C. and Gonja, T. 2011. The Online Privacy Paradox: A Social Representations Perspective. CHI '11 Extended Abstracts on Human Factors in Computing Systems (New York, NY, USA, 2011), 2107–2112.

[41] Orlikowski, W.J. 2006. Material knowing: the scaffolding of human knowledgeability. European Journal of Information Systems. 15, 5 (Oct. 2006), 460–466. DOI=https://doi.org/10.1057/palgrave.ejis.3000639.

[42] Pentina, I., Zhang, L., Bata, H. and Chen, Y. 2016. Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. Computers in Human Behavior. 65, (2016), 409–419.

[43] Poikela, M., Schmidt, R., Wechsung, I. and Möller, S. 2015. FlashPolling privacy: The discrepancy of intention and action in location-based poll participation. Adjunct Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2015 ACM International Symposium on Wearable Computers (2015), 813–818.

[44] Pötzsch, S. 2008. Privacy awareness: A means to solve the privacy paradox? IFIP Summer School on the Future of Identity in the Information Society (2008), 226–236.

[45] Puaschunder, J.M. 2017. Towards a Utility Theory of Privacy and Information Sharing and the Introduction of Hyper-Hyperbolic Discounting in the Digital Big Data Age. SSRN Electronic Journal. (2017). DOI=https://doi.org/10.2139/ssrn.3082060.

[46] Quinn, K. 2016. Why we share: A uses and gratifications approach to privacy regulation in social media use. Journal of Broadcasting & Electronic Media. 60, 1 (2016), 61–86.

[47] Rosenfeld, A. and Kraus, S. 2018. Predicting Human Decision-Making: From Prediction to Action. Synthesis Lectures on Artificial Intelligence and Machine Learning. 12, 1 (Jan. 2018), 1–150. DOI=https://doi.org/10.2200/S00820ED1V01Y201712AIM036.

[48] Sjåstad, H. and Baumeister, R.F. 2019. Moral self-judgment is stronger for future than past actions. Motivation and Emotion. (Apr. 2019). DOI=https://doi.org/10.1007/s11031-019-09768-8.

[49] Smith, W.K. and Lewis, M.W. 2011. Toward a Theory of Paradox: A Dynamic equilibrium Model of Organizing. Academy of Management Review. 36, 2 (Apr. 2011), 381–403. DOI=https://doi.org/10.5465/amr.2009.0223.

[50] Stephenson, W. 1978. Concourse theory of communication. Communication. 3, 1 (1978), 21–40.

[51] Stets, J.E. and Carter, M.J. 2011. The Moral Self: Applying Identity Theory. Social Psychology Quarterly. 74, 2 (Jun. 2011), 192–215. DOI=https://doi.org/10.1177/0190272511407621.

[52] Stutzman, F., Vitak, J., Ellison, N.B., Gray, R. and Lampe, C. 2012. Privacy in interaction: Exploring disclosure and social capital in Facebook. Sixth International AAAI Conference on Weblogs and Social Media (2012).

[53] Sundar, S.S., Kang, H., Wu, M., Go, E. and Zhang, B. 2013. Unlocking the privacy paradox: do cognitive heuristics hold the key? CHI'13 extended abstracts on human factors in computing systems (2013), 811–816.

[54] Taddeo, M. and Floridi, L. 2016. The Debate on the Moral Responsibilities of Online Service Providers. Science and Engineering Ethics. 22, 6 (Dec. 2016), 1575–1603. DOI=https://doi.org/10.1007/s11948-015-9734-1.

[55] Vallor, S. 2016. Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting. Oxford University Press.

[56] Watts, S. and Stenner, P. 2012. Doing Q Methodological Research: Theory, Method & Interpretation. SAGE Publications Ltd.

[57] Wilson, D. and Valacich, J.S. 2012. Unpacking the privacy paradox: Irrational decision-making within the privacy calculus. (2012).

[58] Wu, D., Huang, H., Liu, N. and Miao, D. 2019. Information processing under high and low distractions using eye tracking. Cognitive processing. 20, 1 (2019), 11–18.

[59] Yan, Z. and Holtmanns, S. 2008. Trust modeling and management: from social trust to digital trust. Computer security, privacy and politics: current issues, challenges and solutions. IGI Global. 290–323.

[60] Zafeiropoulou, A.M., Millard, D.E., Webber, C. and O'Hara, K. 2013. Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? Proceedings of the 5th Annual ACM Web Science Conference (2013), 463–472.

[61] Zhou, W., Zhang, Y. and Liu, P. 2018. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. (Jan. 2018), 11.

[62] Ziegeldorf, J.H., Morchon, O.G. and Wehrle, K. 2014. Privacy in the Internet of Things: threats and challenges, Security and Communication Networks. 7, 12 (Dec. 2014), 2728–2742. DOI=https://doi.org/10.1002/sec.795.

[63] 2017. Mitigating Risks in the Innovation Economy. World Economic Forum.

On Possible Electromagnetic Precursors to a Significant Earthquake (Mw = 7.0) Occurred in JiuZhaiGou (China) on 8 August 2017

Zhicheng Qiu
Earthquake Monitoring and Prediction Technology Research Center, Peking University Shenzhen Graduate School Shenzhen, China
(+86)15952022951
1701213583@pku.edu.cn

Shanshan Yong
Earthquake Monitoring and Prediction Technology Research Center, Peking University Shenzhen Graduate School Shenzhen, China
yongss@pkusz.edu.cn

Xin'an Wang
Earthquake Monitoring and Prediction Technology Research Center, Peking University Shenzhen Graduate School Shenzhen, China
anxinwang@pkusz.edu.cn

ABSTRACT
This paper reports an attempt to use low-frequency electromagnetic data (ED) from the Multi-component Seismic Monitoring System (AETA) in the study of earthquake precursors in China. The data from 5 AETA stations deployed within 200 km of the epicenter have been analyzed in the search for possible precursors to a strong earthquake that occurred JiuZhaiGou, (China) on 8 August 2017, with magnitude Mw = 7.0 and focal depth = 20 km. By calculating the correlation between the electromagnetic signals of every 2 AETA stations, an attempt is made to extract relatively weak electromagnetic anomaly information from a strong interference background. The analysis is based on a new method of calculating correlation, called local correlation tracking (LCT) method. Comparing with the classical correlation method, the proposed method can better extract the weak difference of this kind of electromagnetic signal. The electromagnetic data of AETA was analyzed by LCT method. It was found that the correlation coefficient showed an abnormality within one week before the earthquake, which indicated that the weak anomaly in the electromagnetic signal was found. It is concluded that this may be the electromagnetic precursor anomaly signal caused by the significant earthquake, so we hope that this will be helpful to the study of earthquake prediction.

CCS Concepts
• **Applied computing→Environmental sciences.**

Keywords
Electromagnetic data (ED); AETA; earthquake monitoring; local correlation tracking (LCT); electromagnetic precursor.

1. INTRODUCTION
In China, earthquakes occur frequently, with a wide range of influences and great destructiveness. Seismic monitoring is to detect abnormal changes of various types of seismic signals before and after the earthquake [1~8], and to study the relationship between these signals and earthquakes to predict the occurrence of earthquakes. In the past few decades, significant progress has been made in the field of electromagnetic phenomena associated with earthquakes, the so-called seismic electromagnetics [9~15]. A large number of earthquake events show that during the earthquake seismogenic process, different degrees of electromagnetic radiation appear in the seismic source area and its surrounding areas. These radiated electromagnetic fields will appear in advance or in synchronization with seismic signals [16~18]. Since electromagnetic disturbance is one of the most sensitive precursors of short-term seismic reflection, it is also a good method to capture short-term anomalies of earthquakes and has become an important seismic monitoring method [19~24]. For the sake of detect electromagnetic disturbance in real time in a huge area, the Key Laboratory of Integrated Micro-systems Science and Engineering Applications developed AETA.

For many years, scientists have been exploring methods that can effectively capture electromagnetic precursors associated with earthquakes and used them for earthquake prediction [11, 25~27]. However, the precursor anomalies generated by various electromagnetic effects are inconsistent in time, and are also affected by the intensity of the earthquake in space, resulting in very complex features of the anomalies. At present, anomaly detection of electromagnetic data is mainly based on direct analysis of data, rather than through the correlation between multiple electromagnetic data [9~27]. Verma et al. used the LCT method to capture the process dynamics of solar activity, and achieved good results [28]; and Li et al. also used the LCT method to observe possible earthquake precursors in seismic electromagnetic signal extraction and analysis [29]. Therefore, we calculate the correlation of ED between different stations based on the LCT method. Within a certain range, there is a certain correlation between the electromagnetic signal changes brought by the earthquake, that is, there may be a certain relationship between multiple electromagnetic data, which is related to the location, magnitude and depth of the earthquake. In order to study the possible electromagnetic precursors of earthquakes, the correlation of multiple electromagnetic data in a certain range of the epicenter is calculated, and then the electromagnetic signal anomalies related to the earthquake are studied from the anomalies of correlation.

In this paper, the local correlation tracking method is used to process and analyze the electromagnetic data observed by the AETA station before the earthquake. Firstly, the method is based

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388202

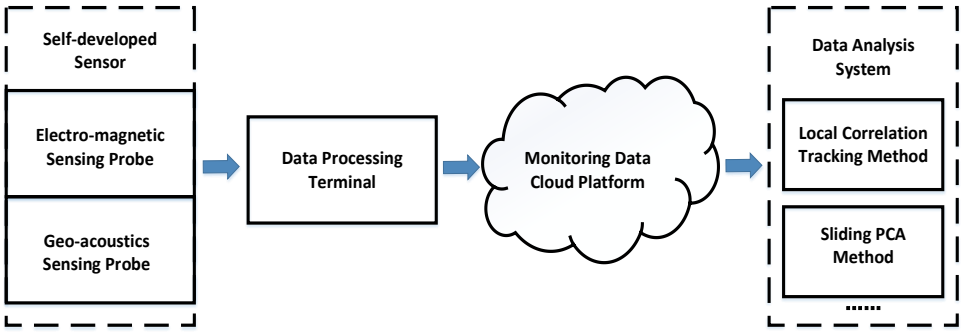


Figure 1. Block diagram of AETA system.

on the calculation of the correlation of electromagnetic signals between stations. By contrast with the classical correlation method, the local correlation method is more suitable for the processing of non-stationary transient signals than the classical correlation method, and has certain Noise resistance. Then, by studying the correlation anomalies between multiple stations within a certain range, possible earthquake-related precursors were discovered.

2. THE MULTI-COMPONENT SEISMIC MONITORING SYSTEM

2.1 AETA

The multi-component seismic monitoring system AETA is a system composed of observing stations and clouds that can observe large-area, high-density observations of earthquake precursors [30]. The monitoring system consists of a data processing terminal, a geo-acoustics sensing probe, an electromagnetic sensing probe, a monitoring data cloud platform and a data analysis system, shown as Figure. 1. Perceive electromagnetic disturbance and geo-acoustics, collect data in real time and transmit data to cloud platform for subsequent storage, feature extraction and abnormal analysis through Internet (wired or wireless) network.

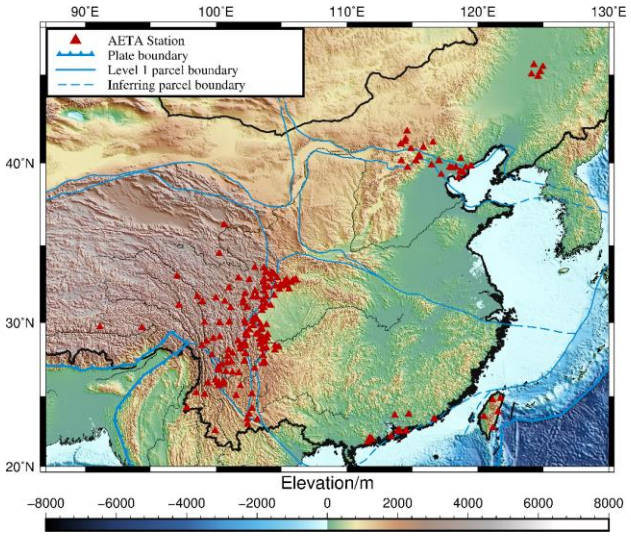


Figure 2. The distribution circumstance of AETA in China.

AETA monitors the very low dynamic range of the very low frequency and ultra-low frequency electromagnetic band (0.1 Hz ~ 10 kHz, 0.1 ~ 1000 nT), sensitivity > 20 mV / nT @0.1 Hz ~ 10 kHz. Specifically, for the 0.1~200Hz frequency band, the sampling frequency is 500Hz with 18-bit resolution; for 0.1Hz~10 kHz, the sampling frequency is 30k Hz with 18- bit resolution. Up to now, with the support of the China Earthquake Administration, the AETA system has been installed more than 200 stations nationwide, covering Hebei, Sichuan, Yunnan, Tibet, Guangdong and Taiwan, shown as Figure. 2. The number of equipment deployed in Sichuan has reached 111, covering the entire key areas of Sichuan.

3. IMPLEMENTATION OF ELECTROMAGNETIC DATA CORRELATION ANOMALY DETECTION METHOD

First, we need to introduce our electromagnetic data (ED). In the AETA system, each station produces 480 frames of low-frequency ED per day, and each frame contains 3 minutes of signal. For each data frame, we can further calculate the characteristic data of the 3-minute signal, including the mean, ringing count and peak frequency. In the experiments described later, we use the mean characteristic data of low-frequency ED.

The anomaly detection method proposed in this section can be divided into two parts: the method of calculating the correlation of ED from AETA stations by classical correlation method and local correlation tracking method respectively.

3.1 Calculating the Correlation of the ED by Classical Correlation Method

In signal analysis, traditional classical correlation refers to the linear or interdependent relationship between variables. When analyzing the correlation between the measured time series $x(t)$ and $y(t)$, the common equation (1) is used to solve the correlation coefficient:

$$r_{xy}(k) = C_{xy} / \sigma_x \sigma_y = \frac{\sum_{i=1}^{n-k}(x(t)-\bar{x})(y(t+k)-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x(t)-\bar{x})^2}\sqrt{\sum_{i=1}^{n}(y(t)-\bar{y})^2}} \quad (1)$$

In equation (1), σ_x and σ_y are the mean square deviations of $x(t)$ and $y(t)$, respectively; $\bar{x}$ and $\bar{y}$ are the mean values of $x(t)$ and $y(t)$, respectively; $C_{xy}(k)$ is the covariance of two time series at time delay k; $r_{xy}(k)$ is the number of correlations

between two time series under time delay t; n is the length of the time series.

3.2 Calculating the Correlation of the ED by Local Correlation Tracking Method

The local correlation tracking method is an improvement on the general linear correlation method. The difference in this method is that it compares the local covariance matrices corresponding to each time of two time series.

A time window $x_{t,\omega}$ is introduced, and then the local covariance matrix of each time series at time t is obtained. For the time t, all the windows $x_{t,\omega}$ in the $(1 \leqslant \tau \leqslant t)$ time period are used, the time window is multiplied by the weighting factor $\beta^{t-\tau}$, the weighting coefficient near time t is large, and the weighting coefficient away from time t is exponentially decayed. Given a time series X, the local covariance matrix at time t is defined as:

$$\hat{\Gamma}_t(X,\omega,\beta) := \sum_{\tau=1}^{t} \beta^{t-\tau} X_{\tau,\omega} \otimes X_{\tau,\omega} \tag{2}$$

Then, the singular value decomposition is performed on the local covariance matrices of the two time series at time t:

$$\hat{\Gamma}_t = \mathbf{U\_X\Sigma V\_X}^{\mathrm{T}} \tag{3}$$

$$\hat{\Gamma}_t = \mathbf{U\_Y\Sigma V\_Y}^{\mathrm{T}} \tag{4}$$

According to the actual demand, the number of "principal components" k to be retained is selected by the energy threshold to obtain the "main eigenvector" matrix which can reflect the original time series features to the greatest extent:

$$\mathbf{U}_X = \mathbf{U}_k\left(\hat{\Gamma}_t(\mathbf{X})\right) = \mathbf{U\_X}(:,1:k) \tag{5}$$

$$\mathbf{U}_Y = \mathbf{U}_k\left(\hat{\Gamma}_t(\mathbf{Y})\right) = \mathbf{U\_Y}(:,1:k) \tag{6}$$

The eigenvectors can capture critical aperiodic, oscillating trends, and even short-term non-stationary sequences of non-stationary time series, using the "primary eigenvector" matrix to pick up local features of the original time series.

Finally, the feature vectors u_x and u_y corresponding to the maximum eigenvalues of the local covariance matrices $\hat{\Gamma}_t(X)$ and $\hat{\Gamma}_t(Y)$ are respectively used to right-multiply the "main feature vector" matrices $\mathbf{U}_Y$ and $\mathbf{U}_X$. $\mathbf{U}_Y^{\mathrm{T}}u_x$ and $\mathbf{U}_X^{\mathrm{T}}u_y$ correspond to the projections of the eigenvectors u_x and u_y corresponding to the largest eigenvalue of the local covariance matrix on the "subspaces" $span(\mathbf{U}_Y)$ and $span(\mathbf{U}_X)$ formed by the "main eigenvector" matrix, and their angles θ are:

$$\begin{aligned} \theta_1 &\equiv \angle\left(u_x, \mathrm{span}\,\mathbf{U}_Y\right) = \angle\left(u_x, \mathbf{U}_Y^{\mathrm{T}}u_x\right) \\ \theta_2 &\equiv \angle\left(u_y, \mathrm{span}\,\mathbf{U}_X\right) = \angle\left(u_y, \mathbf{U}_X^{\mathrm{T}}u_y\right) \end{aligned} \tag{7}$$

Obviously, if the two time series X and Y to be analyzed are locally correlated, then for the maximum eigenvalues of the local covariance matrix of each time series corresponding to the eigenvectors u_x and u_y, they should "belong" to the subspaces $span(\mathbf{U}_Y)$ and $span(\mathbf{U}_X)$ formed by the columns of the main eigenvectors of another time series local covariance matrix. That is, the angles θ_1 and θ_2 should both be close to 0. At this time, the absolute values $|\cos\theta_1|$ and $|\cos\theta_2|$ of the corresponding cosine values should be close to 1:

$$\begin{aligned} |\cos\theta_1| &= \left\|\mathbf{U}_Y^{\mathrm{T}}u_x\right\| / \|u_x\| = \left\|\mathbf{U}_Y^{\mathrm{T}}u_x\right\| \to 1 \\ |\cos\theta_2| &= \left\|\mathbf{U}_X^{\mathrm{T}}u_y\right\| / \|u_y\| = \left\|\mathbf{U}_X^{\mathrm{T}}u_y\right\| \to 1 \end{aligned} \tag{8}$$

Therefore, define the local similarity score (LSS) as:

$$\begin{aligned} \ell_t &= \frac{1}{2}\left(\left|\cos\angle\left(u_y, span\mathbf{U}_X\right)\right| + \left|\cos\angle\left(u_x, span\mathbf{U}_Y\right)\right|\right) \\ &= \frac{1}{2}\left(\left\|\mathbf{U}_X^{\mathrm{T}}u_y\right\| + \left\|\mathbf{U}_Y^{\mathrm{T}}u_x\right\|\right) \end{aligned} \tag{9}$$

Using this method to track the relationship between two time series: when the local correlation between the original time series is strong, the local similarity score (also called the local correlation coefficient) should be close to 1; When this related steady state relationship is broken, the local similarity score will be smaller than 1.

4. EXPERIMENTAL RESULTS AND ANALYSIS

4.1 Experimental Area

The experiment analyzed 5 stations within 200 km from the epicenter of the Jiuzhaigou 7.0 earthquake, and selected data from July 14, 2017 to August 13, 2017 for 30 days. The earthquake occurred at the geographic coordinate (33.20° N, 103.82° E) on August 8, 2017. 21:19:46.

As shown in Figure. 3, the 5 AETA stations within 200km of the epicenter are: No. 121 Jiuzhaigou Earthquake Mitigation Bureau (JZG), No. 129 Songpan Earthquake Station (SP), No. 116 Pingwu Earthquake Mitigation Bureau (PW); No. 43 Qingchuan Earthquake Mitigation Bureau (QC); No. 90 Maoxian Measuring Station (MX). The information of these stations is shown in Table 1.

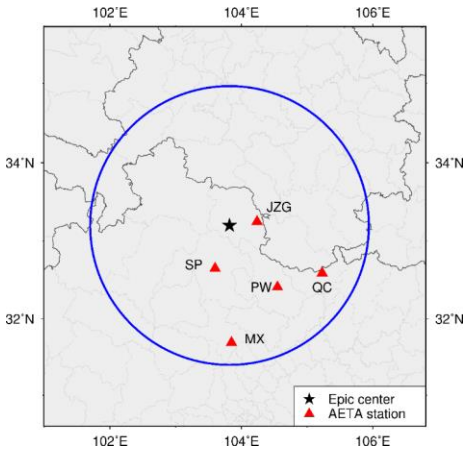


Figure 3. Map of the study AETA stations. The circle on the figure represents a range of 200 km from the epicenter.

Table 1. Location information of the study AETA stations

Station ID	Station Name	Abbreviation	Latitude	Longitude	Epicentral distance
121	Jiuzhaigou Earthquake Mitigation Bureau	JZG	33.25 ℕ	104.24 𝔼	40 km
129	Songpan Earthquake Station	SP	32.65 ℕ	104.03 𝔼	64 km
116	Pingwu Earthquake Mitigation Bureau	PW	32.41 ℕ	104.55 𝔼	120 km
43	Qingchuan Earthquake Mitigation Bureau	QC	32.59 ℕ	105.23 𝔼	147 km
90	Maoxian Measuring Station	MX	31.69 ℕ	103.85 𝔼	170 km

4.2 Experimental Result and Analysis

Taking the JZG station as an example, Figure. 4(a) shows the ED collected by the station from July. 14th, 2017 to Aug. 13rd, 2017, in which the missing data was blanked. The ED shown in Figure. 4(a) is processed using a normalization operation to obtain Figure. 4(b). The red line in Figure. 4 indicates the Jiuzhaigou 7.0 earthquake.

In order to calculate the direct correlation of stations, try to use the classical correlation method and the local correlation tracking method. First, select the ED of No. 90 MX station and No. 75 QW station to calculate the classic correlation coefficient and the local correlation coefficient. The data period is from July 14, 2017 to August 13, 2017. It turns out that the latter has a better processing effect on non-stationary signals. It can be seen from the results of Figure. 5 that the classical correlation method cannot reasonably reflect the correlation between the electromagnetic signals of the two stations. It is difficult to extract effectively when the signal of a certain station is abnormal; however, local correlation tracking is used. The method can well show the correlation between the two stations, and can effectively pick up when a station has a weak anomaly. From this comparison, in the analysis below, we use the LCT method to calculate the correlation between stations.

The correlation analysis was performed using the local correlation tracking method for the ED of 5 AETA stations within 200 km from the epicenter. The ED of the 5 AETA stations is shown in Figure. 6. Among them, the ED of the No. 43 QC station has a large fluctuation in magnitude from July 15 to July 25.

For these 5 AETA stations, the LCT coefficients are calculated for each of the 2 stations, and there are a total of 10 sets of results. It was found that all group correlations were abnormal about one week before the earthquake, as shown in the green box in Figure. 7. Due to the fluctuation of the ED of the No. 43 QC station, the LCT coefficient related to QC is abnormal before July 25, as shown in the red box in the Figure. 7.

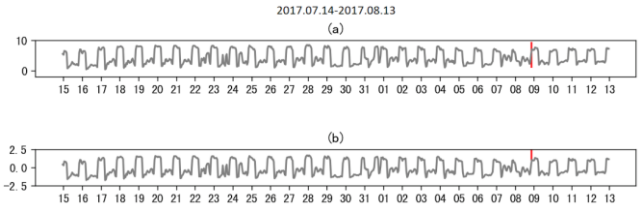


Figure 4. (a) ED raw data of JZG station. (b) ED norm data of JZG station.

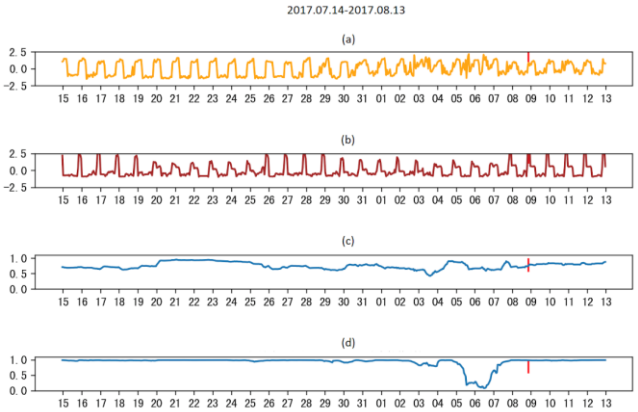


Figure 5. (a) ED norm data of MX station. (b) ED norm data of QW station. (c) and (d) are the correlation between MX station and QW station calculated by classical correlation method and local correlation tracking method, respectively.

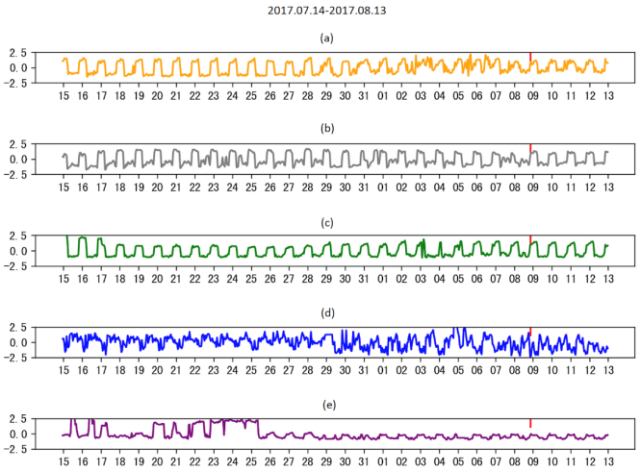


Figure 6. (a) ED norm data of MX station. (b) ED norm data of JZG station. (c) ED norm data of SP station. (d) ED norm data of PW station. (e) ED norm data of QC station.

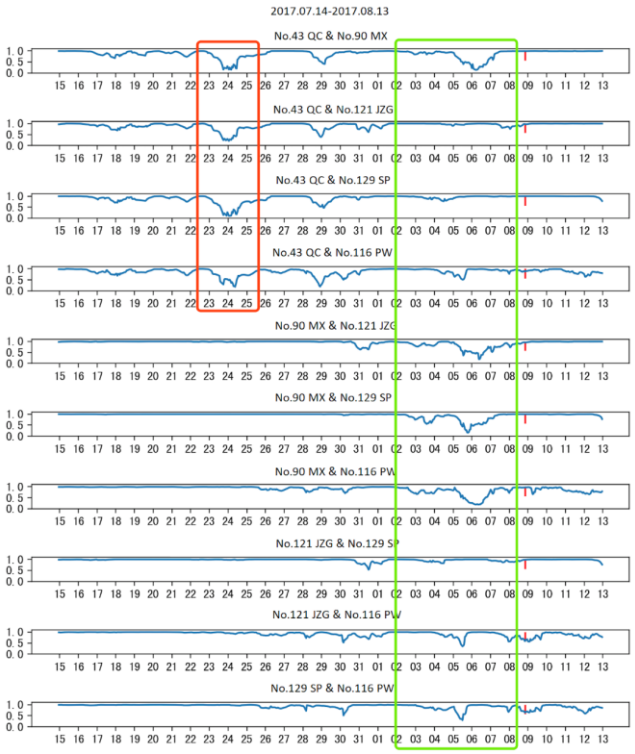


Figure 7. 5 AETA stations use the LCT method for a total of 10 results.

According to the above experiments, when the LCT processing of the electromagnetic signals of 5 stations in the epicenter is carried out, it is found that there is a good spatial correlation between the stations before the earthquake, that is, the number of local correlations between the electromagnetic signals of the stations is close to 1. Further, in the week before the earthquake occurred, the spatial correlation between the inherent electromagnetic signals between the stations was broken, so the corresponding correlation coefficient was less than 1.

It can be inferred that the local correlation tracking method is applied to the ED correlation analysis, and the correlation anomaly is detected within one week before the earthquake, that is, the electromagnetic precursor anomaly related to the earthquake is found.

5. CONCLUSIONS

This paper presents a method for detecting possible electromagnetic precursors to a significant earthquake by calculating electromagnetic data correlation. The proposed LCT method has better applicability and robustness than the classical correlation method, and can extract relatively weak anomalies. Experiments on the ED of the AETA station within 200 km of the Jiuzhaigou earthquake show that the anomaly detected by the LCT method has a certain ability to reflect earthquakes. Today, the understanding of seismic electromagnetic phenomena is still very limited. We hope that the AETA electromagnetic precursor anomaly detection method for calculating LCT anomalies can provide some useful exploration for earthquake prediction. In the further research in the future, I will use this method as the basis, hoping to build a complete and effective earthquake prediction model.

6. ACKNOWLEDGMENTS

This work is supported by the fundamental research project of Shenzhen science and technology application demonstration project under Grant No.KJYY20170721151955849.

7. REFERENCES

[1] E. E. Brodsky and L. Thorne, “Geophysics. Recognizing foreshocks from the 1 April 2014 Chile earthquake,” Science, vol. 344, no. 6185, pp. 700–2, 2014.

[2] A. Skelton et al., “Changes in groundwater chemistry before two consecutive earthquakes in Iceland,” Nature Geoscience, vol. 7, no. 10, pp. 752–756, 2014.

[3] H. W. Green, C. Wang-Ping, and M. R. Brudzinski, “Seismic evidence of negligible water carried below 400-km depth in subducting lithosphere,” Nature, vol. 467, no. 7317, pp. 828–831, 2010.

[4] Eisner, Leo, et al. "Uncertainties in passive seismic monitoring." *The Leading Edge* 28.6 (2009): 648-655.

[5] Lumley, David E. "Time-lapse seismic reservoir monitoring." *Geophysics* 66.1 (2001): 50-53.

[6] Lumley, David. "4D seismic monitoring of CO 2 sequestration." *The Leading Edge* 29.2 (2010): 150-155.

[7] Rickett, J. E., and D. E. Lumley. "Cross-equalization data processing for time-lapse seismic reservoir monitoring: A case study from the Gulf of Mexico." *Geophysics* 66.4 (2001): 1015-1025.

[8] Helmstetter, Agnes, and St éphane Garambois. "Seismic monitoring of S échilienne rockslide (French Alps): Analysis of seismic signals and their correlation with rainfalls." *Journal of Geophysical Research: Earth Surface* 115.F3 (2010).

[9] Nagao, T., et al. "Electromagnetic anomalies associated with 1995 Kobe earthquake." *Journal of Geodynamics* 33.4-5 (2002): 401-411.

[10] Eftaxias, K., et al. "Signature of pending earthquake from electromagnetic anomalies." *Geophysical Research Letters*28.17 (2001): 3321-3324.

[11] Hayakawa, Masashi, et al. "ULF electromagnetic precursors for an earthquake at Biak, Indonesia on February 17, 1996." *Geophysical Research Letters* 27.10 (2000): 1531-1534.

[12] Liu, J. Y., et al. "Seismo‐ionospheric signatures prior to M≥ 6.0 Taiwan earthquakes." *Geophysical research letters* 27.19 (2000): 3113-3116.

[13] Omori, Y., et al. "Anomalous radon emanation linked to preseismic electromagnetic phenomena." *Natural Hazards and Earth System Science* 7.5 (2007): 629-635.

[14] Kalimeris, A., et al. "Multi-spectral detection of statistically significant components in pre-seismic electromagnetic emissions related with Athens 1999, M= 5.9 earthquake." *Journal of Applied Geophysics* 128 (2016): 41-57.

[15] Donner, Reik V., et al. "Temporal correlation patterns in pre-seismic electromagnetic emissions reveal distinct complexity profiles prior to major earthquakes." *Physics and Chemistry of the Earth, Parts A/B/C* 85 (2015): 44-55.

[16] Contoyiannis, Y. F., et al. "Critical features in electromagnetic anomalies detected prior to the L’Aquila

earthquake." *Physica A: Statistical Mechanics and its Applications* 389.3 (2010): 499-508.

[17] Minadakis, George, et al. "Linking electromagnetic precursors with earthquake dynamics: an approach based on nonextensive fragment and self-affine asperity models." *Physica A: Statistical Mechanics and its Applications* 391.6 (2012): 2232-2244.

[18] Potirakis, Stelios M., et al. "On Possible Electromagnetic Precursors to a Significant Earthquake (Mw= 6.3) Occurred in Lesvos (Greece) on 12 June 2017." *Entropy* 21.3 (2019): 241.

[19] Eftaxias, Kostas, et al. "Detection of electromagnetic earthquake precursory signals in Greece." *Proceedings of the Japan Academy, Series B* 76.4 (2000): 45-50.

[20] ZHAO, Guo-ze, Xiao-bin CHEN, and Jun-tao CAI. "Electromagnetic observation by satellite and earthquake prediction [J]." *Progress in Geophysics* 3 (2007).

[21] Uyeda, Seiya, Toshiyasu Nagao, and Masashi Kamogawa. "Short-term earthquake prediction: Current status of seismo-electromagnetics." *Tectonophysics* 470.3-4 (2009): 205-213.

[22] Huang, Q. "Rethinking earthquake-related DC-ULF electromagnetic phenomena: towards a physics-based approach." *Natural Hazards and Earth System Sciences* 11.11 (2011): 2941-2949.

[23] H. Chen, D. Yang, Q. Li, R. Zhu, C. Jiang, and J. Wang, “Observation and Research on Seismic Precursor Information of Electromagnetic Emissions,” Earthquake Research in China, vol. 24, no. 2, pp. 180–186, 2008.

[24] Rabinovitch, Avinoam, Vladimir Frid, and Dov Bahat. "Use of electromagnetic radiation for potential forecast of earthquakes." *Geological Magazine* 155.4 (2018): 992-996.

[25] Eftaxias, K., et al. "Experience of short term earthquake precursors with VLF–VHF electromagnetic emissions." *Natural Hazards and Earth System Sciences* 3.3/4 (2003): 217-228.

[26] Pulinets, Sergey. "Ionospheric precursors of earthquakes; recent advances in theory and practical applications." *Terrestrial Atmospheric and Oceanic Sciences* 15.3 (2004): 413-436.

[27] Uyeda, Seiya, et al. "Geoelectric potential changes: Possible precursors to earthquakes in Japan." *Proceedings of the National Academy of Sciences* 97.9 (2000): 4561-4566.

[28] Verma, M., M. Steffen, and C. Denker. "Evaluating local correlation tracking using CO5BOLD simulations of solar granulation." *Astronomy & Astrophysics* 555 (2013): A136.

[29] Jiankai, L. I. , and T. Ji . "PRINCIPAL COMPONENT ANALYSIS AND LOCAL CORRELA-TION TRACKING AS TOOLS FOR REVEALING AND ANALYZING SEISMO-ELECTROMAGNETIC SIGNAL OF EARTHQAUKE." Seismology & Geology (2017).

[30] X. Jin, S. Yong, X. Wang, R. Pang, C. Han, and J. Zeng, “Design and Implementation of Signal Processing in Seismic Monitoring System AETA,” Computer Technology and Development, no. 1, pp. 45–50, 2018.

Analysis of Key Criteria for Selecting ERP Systems in Croatian Companies

Ruben Picek
Associate professor
Faculty of Organization and Informatics
Pavlinska 2, Varaždin, Croatia
+38542390859
ruben.picek@foi.unizg.hr

ABSTRACT
Selection of an ERP system is extremely important and complex process about whose outcome directly depends the company's success. The goal of this research is to identify, analyze and classified key criteria for selecting ERP systems and then via study apply those results to Croatian companies. The study is based on the comprehensive literature review, where key criteria for selecting ERP systems were systematized in two categories. Then, the online survey was designed and conducted for two target groups: Croatian companies that have implemented ERP system (Users) and companies that implement ERP systems (Consultant). Survey results gives the perception of the importance of certain key criteria per categories from different perspectives. Also, for Croatian companies that have implemented the ERP system, study analyze the importance of particular defined criteria per additional dimensions: years of experience in using ERP systems, enterprise size and type of business.

CCS Concepts
• **Information systems→Enterprise applications.**

Keywords
Selecting ERP systems; classification of selection criteria; key selection criteria; information systems.

1. INTRODUCTION
Selection of an ERP system is a very challenging task and represents a strategic decision of the organization. When company needs to select an ERP system it is necessary to have very seriously approach that will best fit and meet the needs and requirements of the company. ERP system has to be selected on the base of highly examined and selected criteria, although that can't be guarantee that the most appropriate solution will be selected. Before choosing the criteria for selecting "best" ERP system it is necessary to identify all key goals in order to achieve the real needs of the business with ERP system that will be implement into the company. Each criteria should be evaluated separately, based on real facts, wherever possible, and not on the base of subjective opinions or impressions. Therefore, aim of this paper are *identify*, *analyze* and *classify* key criteria for selecting ERP systems and then via study *apply* those results to Croatian companies. The paper is organized as follows. The second section provides a description of related work and presents a literature review. The third section propose a classification of key selection criteria on the base of that review. The third section presents a research method and the results. Finally, the last section concludes the topic.

ICISS 2020, March 19–22, 2020, Cambridge, United Kingdom

ACM ISBN 978-1-4503-7725-6/20/03…$15.00
https://doi.org/10.1145/3388176.3388203

2. RELATED WORK
This section is a literature review that presents a systematization of selection criteria from different perspectives. Perspectives are academic/theoretic research, industry research, stakeholders, open source ERP systems, vendors, experience in selecting (how many times company done it or doing for the first time), and research that has been repeated or expanded after few years.

Czekster et al [1] identified 40 distinct criteria and then narrowed down to 19 criteria. Those criteria were rank according the number of appearance in analyze research papers. Author grouped the criteria into three aspects according to their characteristics; i.e., general costs were grouped as *Financial* (Acquisition and Maintenance cost, Monthly cost Payment and financial terms), whereas all software related was categorized in *Software* (Customization, System efficiency, Backup/restore capabilities, Easiness of use, Reliability, Warranties, Scalability, Portability, Security, Flexibility, System integration, Feature set, Integration with other systems, Maintainability, Technical requirements) and those connected with ERP's suppliers were assigned to the *Supplier* related group (Implementation time, Reputation and references on market, Support, Business strategy alignment, Documentation, Implementation experience, Training).

Authors Motaki and Kamach [2] list a total of 18 criteria that are grouped into 5 categories: *Adaptability* (Compatibility with the enterprise business processes, Technical constraints, System features, Ability to integrate company platforms and data); *Financial* (Service/support cost, Product license, Implementation cost, Budget of the company); *Simplicity* (Ease of use, Ergonomic software, Complexity system); *Provider services* (Maintainability and Support from provider, Training); *Implementation* (Duration of ERP implementation; Complexity of implementation; Successful references).

Authors Motaki and Kamach expand their research and in paper [3] propose an original vision of criteria (total of 36), based on the stakeholders of ERP implementation project: *Vendor/Product* (Vendor market position, References, Financial position, Reputation in the field, Technical support, Training support, Service & support cost, Product License Cost, Functionality, Implementation of Desired Business Processes, Implementation of Desired Business Processes, Implementation of Desired Business

Processes, The provision of best practices, Latest trends in the IT industry, Latest trends in the IT industry, The ability to integrate different platforms and data, System stability, Flexibility in adjusting demands according to business requirements, Flexibility in adjusting demands according to business requirements), *Integrator/Consultants* (The provision of experienced integrators in the alternative ERP implementation, The implementation methodology adopted by the integrator, Integrator's ERP implementation experience in a similar industry, Implementation cost, Training cost, Development cost, Average duration of alternative ERP implementation, Average duration of alternative ERP implementation), *Client* (Enterprise size, Activity area, Desired Business Processes, Enterprise budget, Technical Infrastructure) and *Partners* (ERP systems used by customers and/or suppliers, Consultant's suggestions, The level of use of the ERP by competing enterprises or enterprises whose business sector is the same, Customer and Supplier Needs).

Fathollahi et al. [4] identify 12 criteria group into 4 categories: *Technology* (Applicable and corresponded with business, Reliability and validity, Easy of maintenance), *Costs* (Total investment, Cost of implementation, Maintenance and improvement cost), *Supplier* (Vendor Credential, Industrial certificate, Implementation approach) and *Time* (Needed time for preparation and installation, Updating, System speed).

Hamidi [5] defines only two distinct class of criteria: *Management Factors* (Implementation time, Cost, Vendor Reputation, Consultancy services, R&D capability) and *Product Factors* (Interoperability, Reusability, User-friendliness, Flexibility, Portability, Functionality, Reliability, Usability, Maintainability, and Efficiency). Total number of criteria are 15.

Wei, Chien, and Wang Wang [6] define 9 criteria in total classified in 2 categories: *Software factors* and *ERP vendor* characteristics. For software, the authors selected next criteria: Total cost, Development time (for improvements after acquisition), Feature set, User-friendliness, Flexibility, and Reliability. For the vendor, the authors define: Experience, Offered services, and Reputation.

Bueno and Salmeron [7], [8] have modeled a practical ERP selection tool and defined the set of 27 ERP selection criteria. Of them 17 are related to *ERP Software* (Possibility of applying industry solutions, Credibility of the system, The capacity to integrate the ERP with the current IS/IT, Trust in the ERP system, Modularity, Adaptation of the ERP to the current system needs, Capability of the ERP system to offer information on time, Intuitiveness of the ERP system Software costs, Consultation costs, Maintenance costs, Hardware requirements, Specialist team requirements, High average implementation time, Parameter complexity, Project planning, Possibility of objectively defining the concepts) and the other 10 to the *Organization* where implementation is performed (Employee continuing education, Average age of the personnel, Continuing education of the decision-making group, Suggestions/recommendations made by the users, Traditional organizational culture, Complexity of the organizational structure, High performance, Number of employees/company size, Traditional organizational strategy, Complexity of organizational processes).

Verville and Halingten [9], also Wei et al. [6] have highlighted the importance of choosing a suitable ERP vendor. Wei draws a clear boundary between ERP selection factors related to the *ERP system* itself and factors related to the *ERP vendor*. In the ERP software selection process, he suggests to take into account six groups of criteria related to increase in the ERP project efficiency, which are: Minimized total cost, Minimized implementation time, Complete functionality, User-friendly interface and operations, Excellent system flexibility, High system reliability. In ERP vendor category, criteria need to be considered are: Vendor reputation, Technical capabilities and Provision of ongoing services [8].

Kilic et al. [10] grouped the criteria into three major groups, *Business criteria*, *Cost criteria*, and *Technical criteria*, where the business criteria included company image and marketing position of ERP, the cost criteria were total cost in implementing, and the technical criteria included functional, non-functional, and reliability of the system.

Spencer in [11] evaluating the real reasons why ERP implementations fail and as a first reason lists "Faulty priorities when selecting software" and identify two groups – those companies who were selecting their first business system and those who had gone through previous system selections. The ranking was significantly different between these two groups. *First-time buyers* ranked their evaluation criteria as follows: 1. Price 2. Ease of implementation 3. Ease of use 4. Software fit to the business 5. Functionality of the software 6. Software compatibility with existing hardware 7. Growth potential of software 8. Level of support provided by experienced implementation partner 9. Quality of documentation 10. Software publisher's track record. *Second-time and subsequent buyers* ranked the selection criteria differently. Assuming that they have learned from their previous selection decisions, their rankings are worth reviewing separately. Experienced buyers ranked their criteria as follows: 1. Level of support provided by experienced implementation partner 2. Software publisher's track record 3. Software fit to the business 4. Growth potential of software 5. Price of software 6. Quality of documentation 7. Functionality of the software 8. Ease of use 9. Ease of implementation 10. Software compatibility with existing hardware.

In this review some industrial research are included. To determine a set of ERP selection criteria Ayağ and Özdemi [3], [8] analyzed a set of companies that have already implemented an ERP system. They observed how companies defined the selection criteria for the adoption of their ERP. According to the authors, the ERP selection criteria can be classified into three determinants that have relationships with each other: (A) Competitive advantage, (B) Productivity, (C) Profitability. Under the three determinants, seven dimensions are listed: System cost (A1: Licence free, Consultant expense, Maintenance cost and Infrastructure cost), Vendor support (B1: Reputation, Consulting performance, R&D capabilities, Technical support and Training performance), Flexibility (C1: Upgrade ability, Easy of integration and Easy of in house development), Functionality (C2: Module completion, Function fitness and Security level), Reliability (C3: Stability and recovery ability), Ease of use (C4: Easy of operation and Easy of learning) and Technology advance (C5: Standardization, Integration of legacy systems and Easy of maintain). Finally, 22 criteria are determined.

Baki and Çakar [3], presented results from a study on ERP package selection criteria in 55 Turkish manufacturing companies from variety of industries, they proposed a criteria list that include fit with parent/allied organization systems, better fit with organizational structure, functionality, system reliability, technical criteria, compatibility with other systems, cost, vision, ease of customization, service and support, market position of the vendor, domain knowledge of vendor, references of the vendor,

methodology of the software and consultancy, cross module integration, implementation time.

Kumar, Kumar and Maheshwari [8], referring to a practical survey of 20 enterprises in Canada, distinguished four groups of ERP selection criteria. The first group consists of *ERP software-related criteria* (Functionality of the system, System reliability, Fitting with parent/ allied organization systems, Cross-modular integration, Best business practices available in the system). All these criteria were mentioned in more than 50% of cases. The second group includes criteria related to the *Implementation project manager* (Project management Skills, Functional experience, Experience in IT management). The third group consists of criteria related to the *Implementation partner*, and the last one is associated with implementation consultants' criteria (Reputation, Experience) [8].

Some research was done in context of open source ERP systems. Tasnawijitwong and Samanchuen in [12] discus about qualitative and quantitative criteria for open source ERP systems selection of SMEs in Thailand. They found that the criteria of open source ERP selection are quite similar to that of proprietary ERP selection and use a list of following criteria: Total Costs, Implementation Time, Vendor Support, Functionality, Flexibility, Reliability and User Friendliness. That list is take over from comprehensive literature research done by Johansson and Sudzina [13].

Some authors stress only one class of criteria and focus only on vendor. Malindzakova and Puskas discus abut criteria for selecting information systems according to suppliers/vendor evaluation and defines 18 criteria distributed in 5 classification categories: *Price* (Price offer, Upgrade price, Service cost), *Software availability* (Duration, Meeting customer requirements), *Service* (Employee training, Guidance, Guidance, Connection with departments), *PC support* (Operation System Compatibility, Package contents, Modules, Data collection, Processing, Retention) and *Security IS* (Responsibility, Cyber-attacks, Data protection) [14].

There are authors that do not group criteria in classes they only list them. Author [15] list 28 criteria: Technical team capability, Coverage of the required functionalities norms/regulations, Vendor references/portfolio, Offered guarantees, Quality: Technical support, documentation, and consultancy services, Training services, Payment/financial terms, Vendor market share/scale, Implementation ability, Vendor financial conditions, OS compatibility, HW requirements, Database engine compatibility, Integration with other platforms, Source code accessibility, User friendliness, Costs: SW licensing, HW/infrastructure, Integration/middleware, Maintenance, Software acquisition and consultancy, Scalability/upgradeability, Stability/recovery capacity, Security issues, Customization.

Haddara [16] has listed 11 major criteria: Functionality, Technical requirements, Costs, Services and support, Supplier reputation, Reliability, Compatibility, Market share, Integration, Deployment methodology and Adherence to the company.

Although different classifications of criteria for selecting an ERP system are found in the literature, in all of them a core - set of the most important criteria, can be identify that can serve as a framework or starting point.

3. CLASSIFICATION OF CRITERIA FOR SELECTING ERP SYSTEMS

In previous section a comprehensive literature review was done and key criteria for selecting ERP systems were identify and analyze. It is clear that diversity of selection criteria complicates their classification in standard classes. Most often, ERP system selection criteria are defined from different perspectives and are usually divided into two, three or four groups [8]. For the purpose of this study, key selection criteria were systematized in two categories: *ERP system* and *ERP vendor*.

Category ERP system has 17 criteria, while category ERP vendor has 10 criteria.

Selected criteria in category *ERP system* are:

- Functionality and quality of the product (S1)
- Consistent and intuitive interface (S2)
- Ease of maintenance (S3)
- Affordability (S4)
- Flexibility of ERP system adaptation to business processes (S5)
- Implementation time (S6)
- ERP system speed (S7)
- Supportive abilities in different languages, organizations and currencies (S8)
- System complexity (S9)
- The ability and ease of integrating different platforms and systems (S10)
- Standard coverage of most business processes (S11)
- Return of investment time (S12)
- Mobility (S13)
- Development path in line with the latest technologies (S14)
- Recommendations from other employers (S15)
- Manufacturer recognition in the market (S16)
- ERP system sales in the last year (S17)

Selected criteria in category *ERP vendor* are:

- Technical support and experience (V1)
- Post-implementation maintenance and upgrade support (V2)
- Position in the market (V3)
- Good reputation in the area (V4)
- Years of experience (V5)
- Partnership network built (V6)
- Support in training users to work with the system (V7)
- Great international brand (V8)
- Financial position (V9)
- Recommendation from other users (V10).

Based on this two categories of criteria for selecting ERP systems, a survey was created and conducted on Croatian companies and the results are presented below.

4. RESEARCH METHOD AND RESULTS

After *identifying*, *analyzing* and *classifying* key criteria for selecting ERP systems the *study* was conducted on Croatian companies. The main objective of research was to examine the importance of the defined key criteria (classified into 2 categories) by conducting survey on Croatian companies, which are divided into two target groups - *Companies users of ERP systems* and *Consulting companies* that implement ERP systems into other companies. The total number of respondents included in this survey were 70 (survey completed 28 companies from the first target group and 40 companies from the second group). The survey instrument was a survey questionnaire that was created, emailed, and later analyzed using the Google Forms.

Let's first get acquainted with the profile of first group of respondents - companies that are ERP users or intend to implement the ERP system in the near future. Of the 28 respondents, 3 are micro (10.7%), 8 are small (28.6%), 10 medium-sized (35.7%) and 7 large companies, or 25%.

Companies are from different business domain, most of them, 10, are from the Retail, or 35.7% of the total number of respondents. Behind Retail is Manufacturing with 7 respondents (25%), then Construction with 5 respondents (17.9%), Services with 3 respondents (10.7%), ICT with 2 respondents (7.1%) and Banking with 1 respondent (3.6%).

Regarding the experience that companies have with ERP systems, 6 have experience less than 5 years (21.4%), 4 companies have experience between 5 and 10 years (14.3%), most respondents 12 of them have experience with ERP systems between 10 and 20 years (42.9%), while 4 have experience over 20 years (14.3%). Two companies that have no experience with the ERP system (7.1%) have also participate in the survey. It should be noted that from total number of respondents, 6 are extremely satisfied with the existing ERP system (21.4%), 13 of them (46.4%), are satisfied and 6 are neutral respondents (21.4%). Only 1 respondent is dissatisfied (3.6%), while 2 respondents have expressed extremely dissatisfaction (7.1%), but these are 2 respondents who have no experience with the ERP system.

Then research was focus to achieve the goals of this paper. Both target groups determined the importance of the criteria for selecting ERP systems in the defined categories: ERP *system* and ERP *vendor*. The results for each category of criteria are presented below.

4.1 Importance of Criteria in Category: ERP System

A comparison of the results obtained for the selection criteria in the category *ERP system* for both target groups (Companies users of ERP systems and Consulting companies) is shown in Figure 1.

Both groups of respondents placed in the top three places the most important criteria for selecting an ERP system: ERP systems speed, Functionality and quality of the product and the Flexibility of ERP system adaptation to business processes. To the respondents, the first two criteria are almost equally important, while for Consultants companies, the Speed of the ERP system is convincing in the first place. Other criteria are equally ordered and important for both groups of respondents. The Manufacturer recognition in the market is in the last place for both groups of respondents, but Consultants companies mark these criteria much less.

As there are no major differences in the importance of the criteria of these two groups of respondents, it is concluded that Companies users of ERP systems think well and are guided by the criteria that experienced consultants in Consulting companies consider most important when selecting an ERP system.

Consulting companies have listed a few other criteria that they consider to be extremely important for the selection of the ERP system, and are not listed in the survey questionnaire. *The independence of the ERP system from one implementation partner* - the ability to change the partner without changing the ERP system, is very important criteria because if the implementation partner is inexperienced, unprofessional or his post implementation support is not on high level, it is desirable that the company has the ability to change the implementation partner.

Also, very important criteria from Consulting companies' perspective is *existence of plan of using IT technologies and information systems / ERP system and alignment with business strategy of the company*.

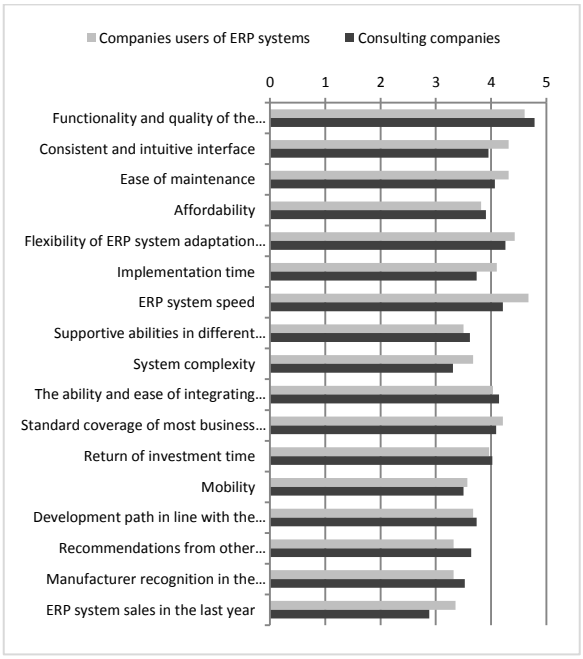


Figure 1. Comparison of criteria in category: *ERP system.*

4.2 Importance of Criteria in Category: ERP Vendor

A comparison of criteria in the category *ERP vendor* for two target groups (Companies users of ERP systems and Consulting companies) are shows in Figure 2.

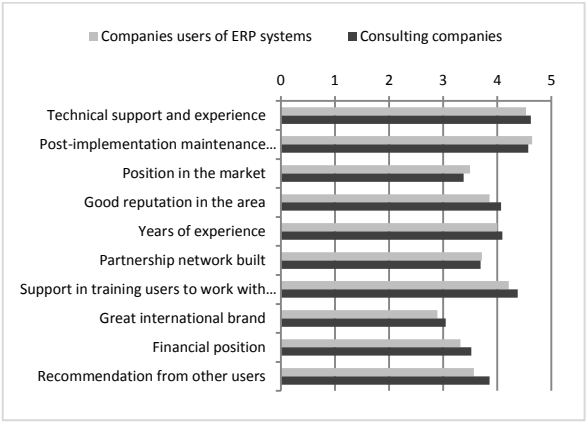


Figure 2. Comparison of criteria in category: *ERP vendor.*

Ranking the first three most important criteria is a little different for those two target groups.

For the *Companies users of ERP systems* in the first place is: Post-implementation maintenance and upgrade support, in second Technical support and experience and in the third place is Support in training users to work with the system. For C*onsultants companies* the first two criteria have switch places and according to them the most important criterion would be Technical support

and experience. Both criteria are at the top of the key criteria for both groups of respondents, which is understandable because of the great importance of maintaining the system and upgrading it, so that all data is up-to-date, and the operations were conducted smoothly and in accordance with all legal regulations.

Both groups of respondents point Great international brand as least important criteria. Much more important for companies is to have long-standing experience and reputation of ERP vendor in the industry in which the company operates, as well as recommendations from other users. It is concluded that Companies users of ERP systems have identified the criteria that even experienced consultants in Consulting companies consider to be the most important when selecting an ERP system.

Consulting companies have listed a few other criteria that they consider to be extremely important for the selection of the ERP system, and are not listed in the survey questionnaire. The first is a *number of experienced ERP system experts*, while the second is related to the *cost of services and vendor response time* (terms defined in the contract/SLA). After comparison of survey results for two target groups of respondents, the focus below is focused only on the first target group *Companies users of ERP systems* and the importance of certain criteria in the defined categories of criteria is looked in new dimensions: experience in working with the ERP system, size of the company and company business.

In dimension "*Experience*", two criteria with the greatest difference in importance between users with less than 10 years of experience and users with more than 10 years of experience are: S15 and S8. Greater importance is given to both criteria by users with greater experience, as with the criteria S14. In dimension "*Company size*", for category ERP system, the analysis found that small companies emphasize the greatest importance to: S7, S1 and S3 while all large companies emphasize S5. All large companies consider that the most important criteria in ERP vendor category are: V1 and V2. In dimension "*Company business*", for category ERP system the biggest differences of opinion were find between Constructing and Manufacturing companies. Other stress criteria: S1, S7 and S5. Constructing and manufacturing companies emphasize ERP vendor criteria V1 and V2.

5. CONCLUSION

The process of selecting an ERP system is extremely important, because if the evaluation of ERP systems is reduced to only a few criteria such as cost, ease of implementation and availability, it is likely that the selected solution will not fully meet the needs of the business, which will lead to weaker overall business results. So, this paper presents a literature review with comprehensive set of criteria that was foundation in identifying key criteria for selecting an ERP systems. Although different authors list different categories of criteria and the number of criteria can be extremely large, for the purposes of this research, 2 categories of criteria have been defined and in each of them the most significant criteria that are either mentioned in the literature or derived from the experience of experts. Aim of this research, conducted on Croatian companies, was ranking the defined criteria as well as to confirm their an implemented the ERP system and consulting companies dealing with the implementation of the ERP system). Detailed analysis of the results shows that the most important criteria for selecting an ERP systems in the category *ERP system* for both target groups are: ERP systems speed, Functionality and quality of the product and the Flexibility of ERP system adaptation to business processes. The research also identifies that the independence of the ERP system from one implementation partner and Existence of plan of using IT technologies and information systems/ERP system and alignment with business strategy of the company criteria should be added to this criteria category. Results of the comparison of criteria in the *ERP Vendor* category, point out that the first three most important criteria for both groups of respondents were: Post-implementation maintenance and upgrade support, Technical support and experience and Support in training users to work with the system. The study identifies some additional criteria that should be added into list of criteria in category ERP Vendor. The first is a number of experienced ERP system experts, while the second is related to the cost of services and vendor response time.

Some interesting findings of importance of certain criteria in the defined categories of criteria are found from the view of additional dimensions: experience in working with the ERP system, size of the company and company business.

6. REFERENCES

[1] R. M. Czekster, T. Webber, A. H. Jandrey, and C. A. M. Marcon, "Selection of enterprise resource planning software using analytic hierarchy process," *Enterp. Inf. Syst.*, vol. 13, no. 6, pp. 895–915, Jul. 2019.

[2] M. Noureddine and N. Oualed, "ERP selection: A step-by-step application of AHP Method," *Int. J. Comput. Appl.*, vol. 176, no. 7, pp. 15–21, Oct. 2017.

[3] M. Noureddine and K. Oualid, "Extraction of ERP Selection Criteria using Critical Decisions Analysis," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 4, 2018.

[4] Soraya Fathollahi, Mohammad Aghaei, Asgar Babapour and Behrooz Pourvali, "Investigation of Criteria's and Selection Efficient ERP System Using AHP Tools in Persian Electronic Commerce Company," *Int. Bus. Manag.*, vol. 10, no. 10, pp. 1958–1964, 2016.

[5] H. Hamidi, "A Fuzzy Decision Making Approach to Enterprise Resource Planning System Selection," *Iran. J. Oper. Res.*, vol. 6, no. 1, pp. 34–52, Mar. 2015.

[6] C.-C. Wei, C.-F. Chien, and M.-J. J. Wang, "An AHP-based approach to ERP system selection," *Int. J. Prod. Econ.*, vol. 96, no. 1, pp. 47–62, Apr. 2005.

[7] S. Bueno and J. L. Salmeron, "Fuzzy modeling Enterprise Resource Planning tool selection," *Comput. Stand. Interfaces*, vol. 30, no. 3, pp. 137–147, Mar. 2008.

[8] D. Ratkevičius, Č. Ratkevičius, and R. Skyrius, "ERP selection criteria: theoretical and practical views," *Ekonomika*, vol. 91, no. 2, pp. 97–116, Jan. 2012.

[9] J. Verville and A. Halingten, "A six-stage model of the buying process for ERP software," *Ind. Mark. Manag.*, vol. 32, no. 7, pp. 585–594, Oct. 2003.

[10] H. S. Kilic, S. Zaim, and D. Delen, "Selecting 'The Best' ERP system for SMEs using a combination of ANP and PROMETHEE methods," *Expert Syst. Appl.*, vol. 42, no. 5, pp. 2343–2352, Apr. 2015.

[11] Diann Spencer, "9 Real Reasons Why ERP Implementations Fail." Western Computer.

[12] S. Tasnawijitwong and T. Samanchuen, "Open source ERP selection for small and medium enterprises by using analytic hierarchy process," in *2018 5th International Conference on Business and Industrial Research (ICBIR)*, Bangkok, 2018, pp. 382–386.

[13] B. Johansson and F. Sudzina, “Choosing Open Source ERP Systems: What Reasons Are There For Doing So?,” in *Open Source Ecosystems: Diverse Communities Interacting*, vol. 299, C. Boldyreff, K. Crowston, B. Lundell, and A. I. Wasserman, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 143–155.

[14] M. Malindzakova, D. Puskas, “The AHP Method Implementation for ERP Software Selection with Regard to the Data Protection Criteria,” *TEM J. Vol. 7 Issue 3 Pages 607-611 ISSN 2217-8309*, Aug. 2018.

[15] M. M. Cruz-Cunha, J. P. Silva, J. J. Gonçalves, J. A. Fernandes, and P. S. Ávila, “ERP Selection using an AHP-based Decision Support System,” *Inf. Resour. Manag. J.*, vol. 29, no. 4, pp. 65–81, Oct. 2016.

[16] M. Haddara, “ERP Selection: The SMART Way,” *Procedia Technol.*, vol. 16, pp. 394–403, 2014.