MAHASARAKHAM UNIVERSITY

A Machine Learning Approach for Detecting Distributed Denial of Service Attacks

Tanaphon Roempluk
Master's degree studying
Majoring in Information technology
Faculty of informatics, Mahasarakham University

The 4th International Conference on Digital Arts,Media and Technology and 2nd ECTI Northern Section Conference on Electrical,
Electronics, Computer and Telecommunications Engineering.   ECTI DAMT and NCON 2019 January 30 - February 2, 2019, Nan Thailand

Presentation is Divided Into Five Parts:

First part : Introduction.

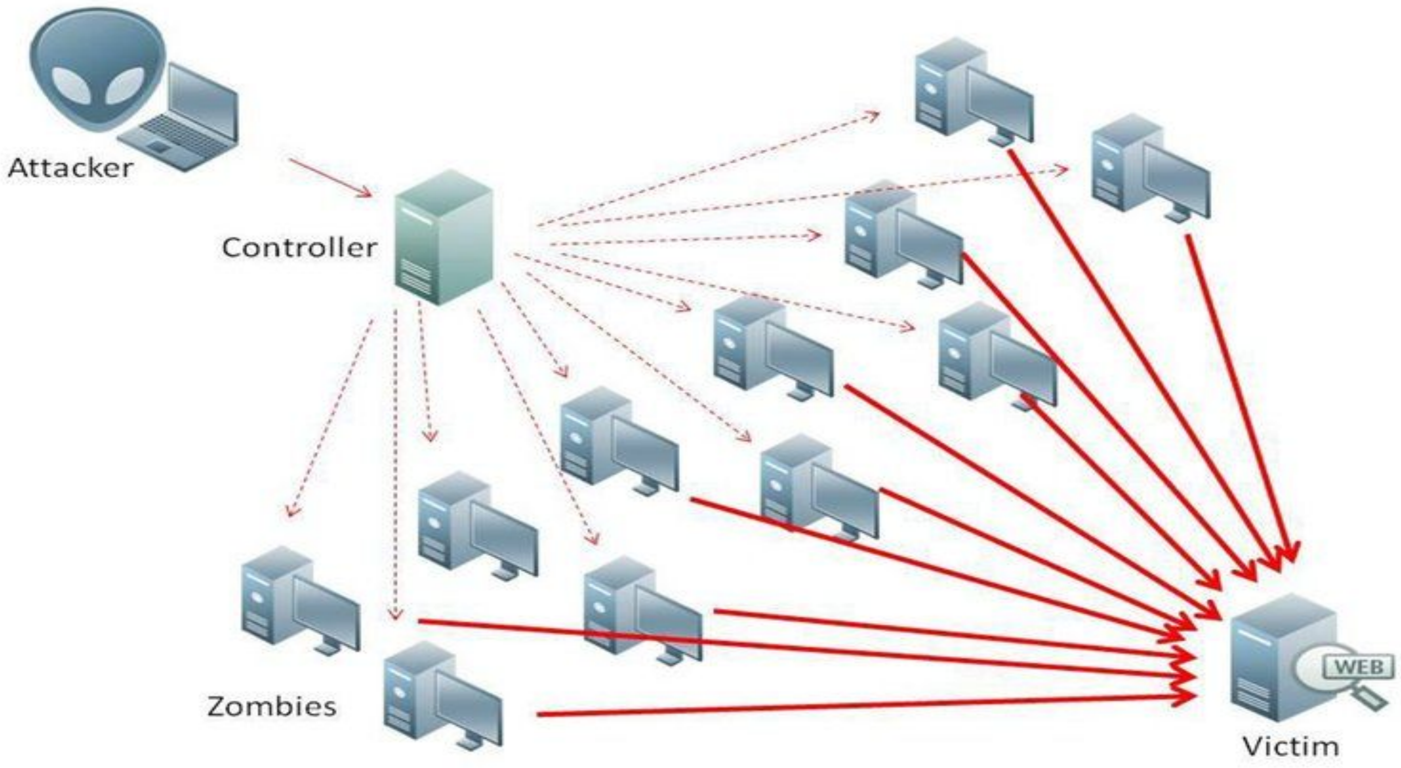
Second part : Method for classifying.

Third part : Describe.

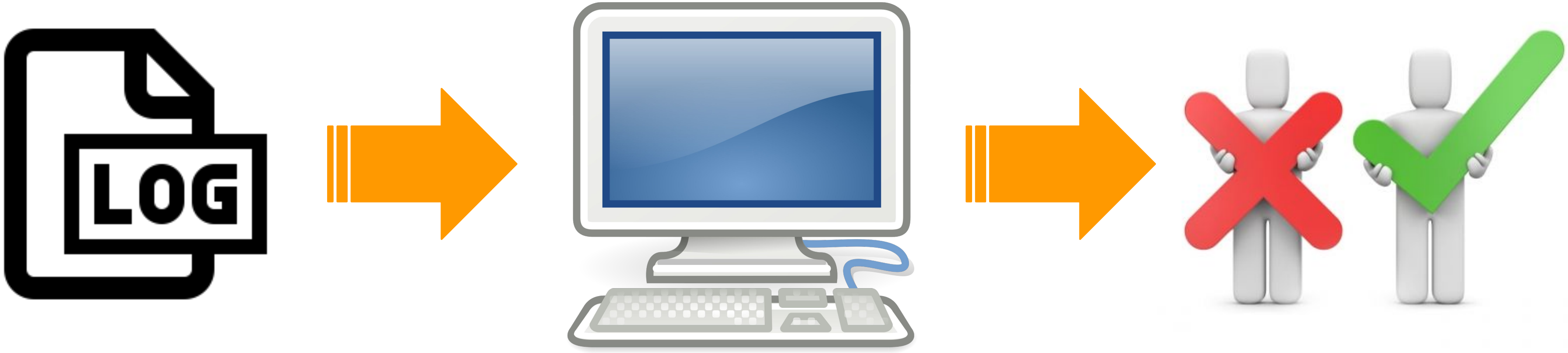
Fourth part : Experience and Results.

Final part : Summarize.

Introduction



Method for Classifying

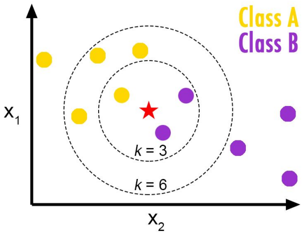


Network Security Information

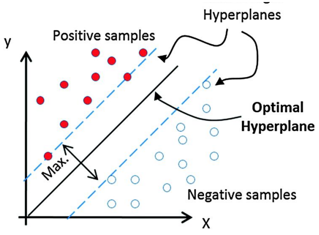
Machine Learning

Classifying DDoS Attack

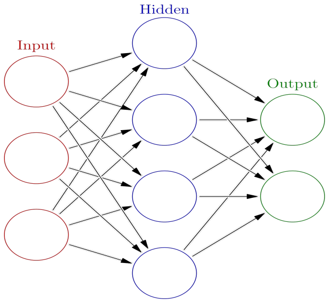
Technique for Classification



The K-Nearest-Neighbor (KNN)



Support Vector Machine (SVM)

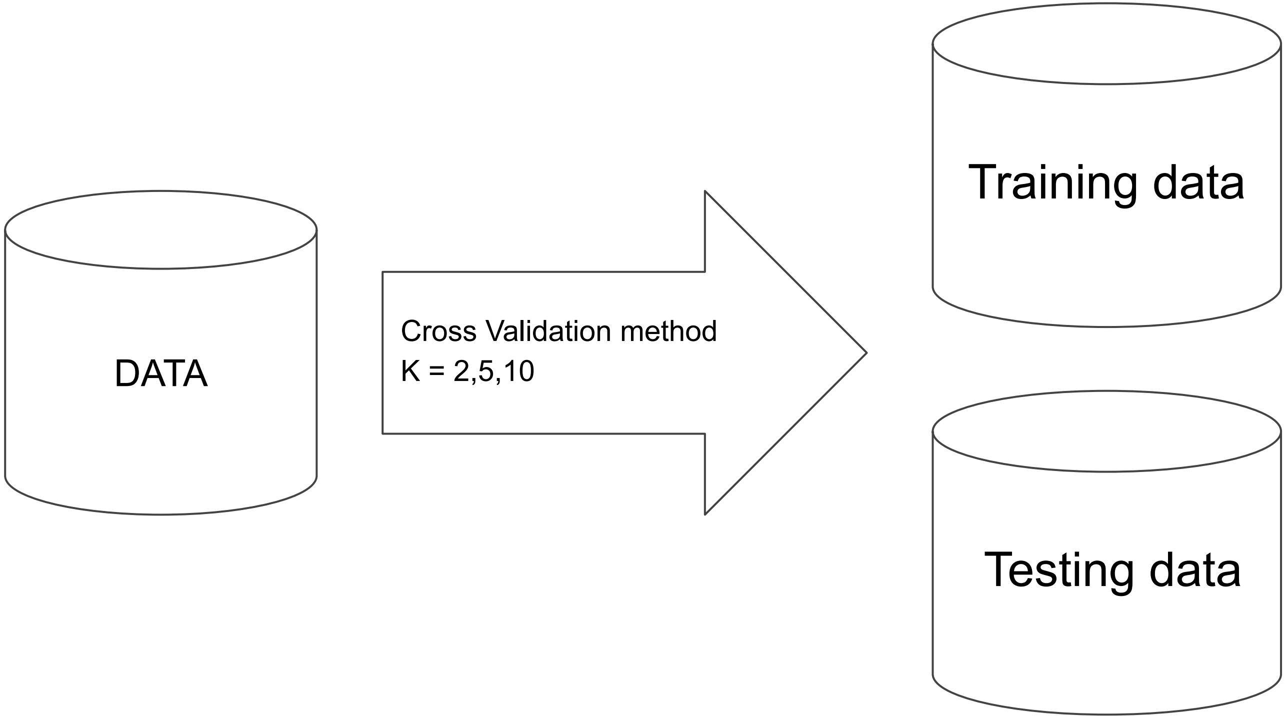


Multi-Layer Perceptron (MLP)

Classification

Accuracy Rate

Cross Validation Method

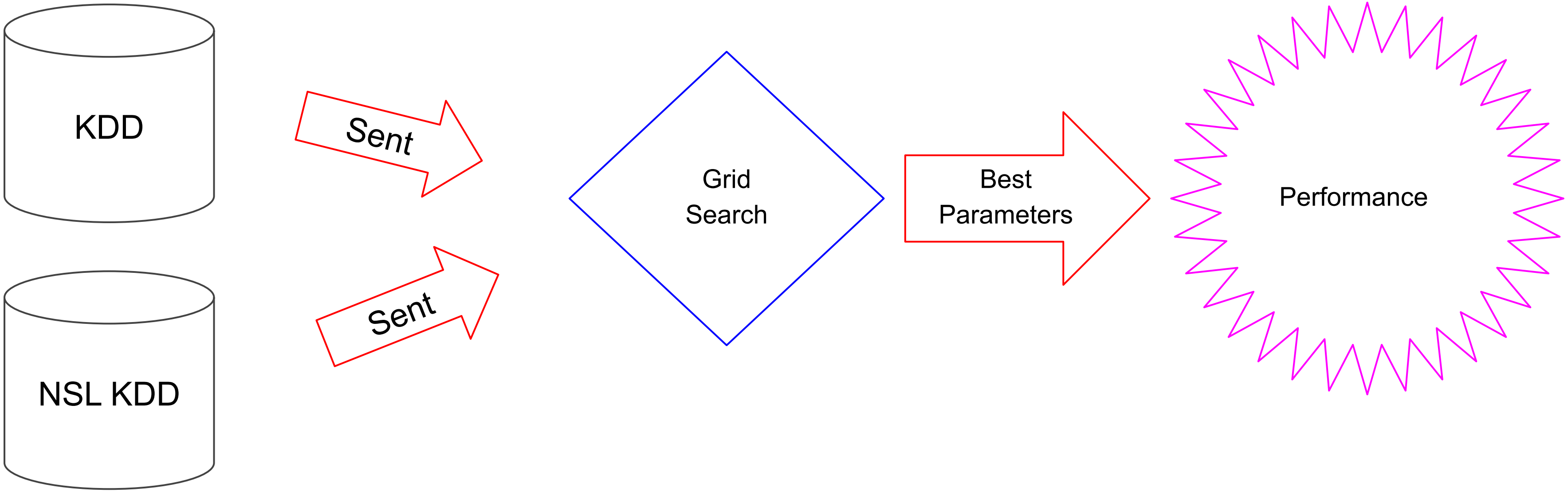

DATA

Cross Validation method
K = 2,5,10

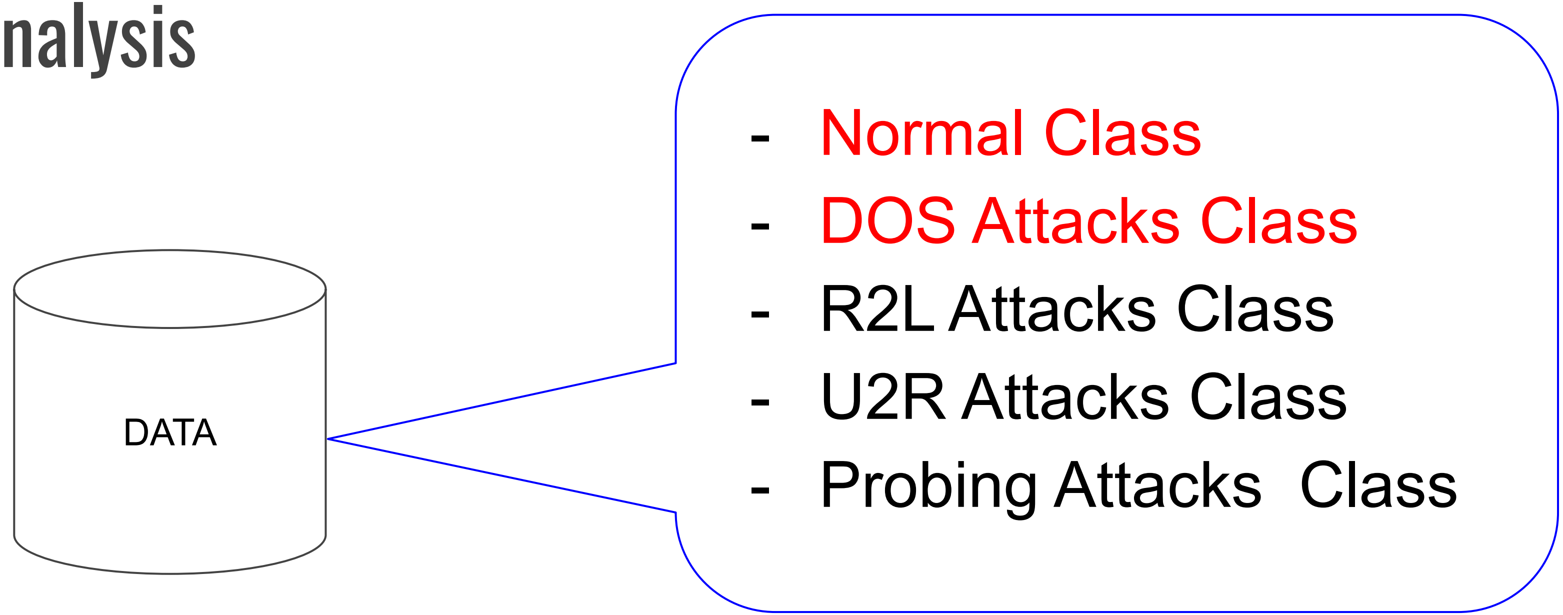
Training data

Testing data

Grid Search Method



Data Analysis

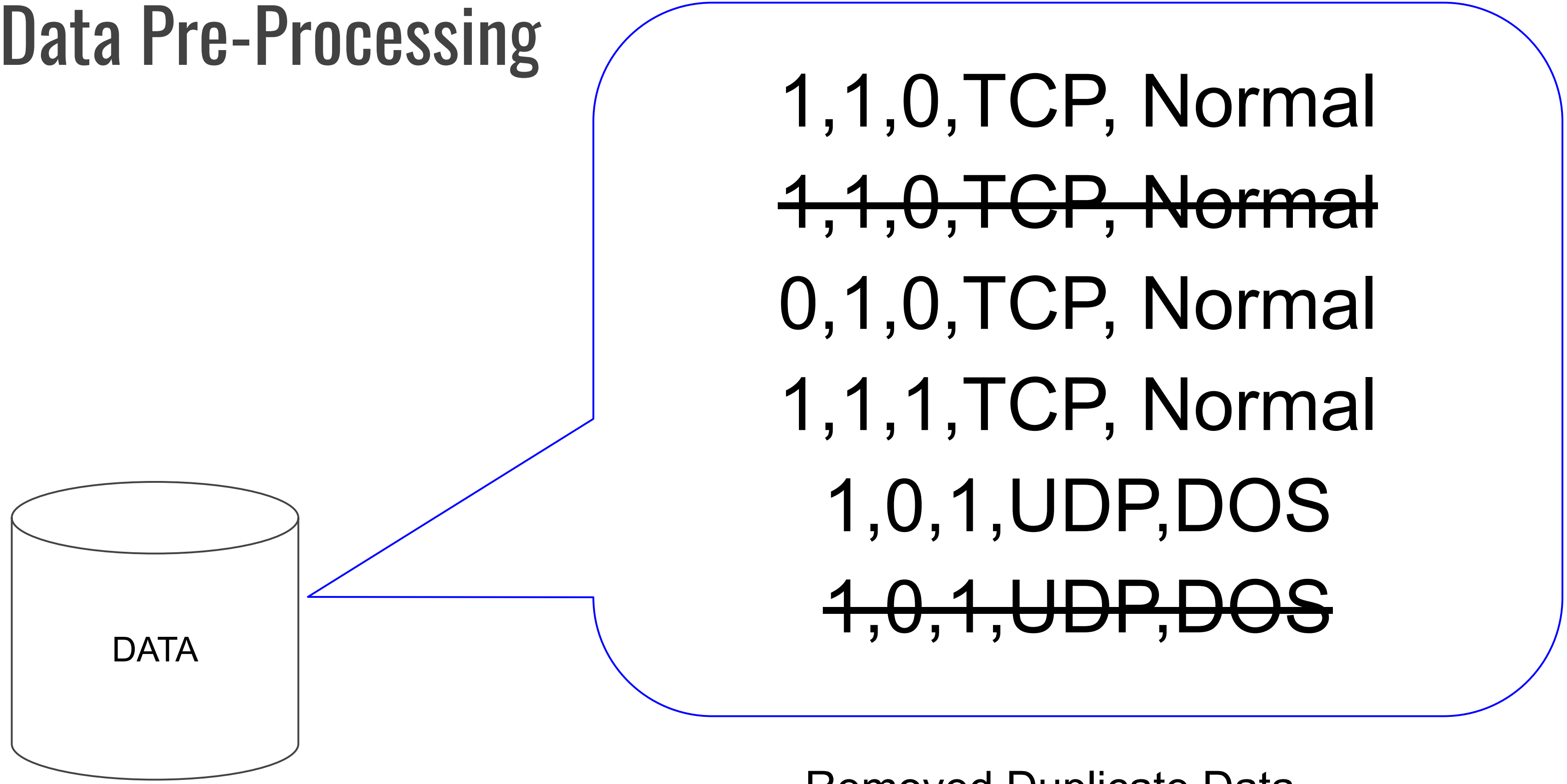


- Normal Class
- DOS Attacks Class
- R2L Attacks Class
- U2R Attacks Class
- Probing Attacks Class

The datasets were divided into Normal Class and 4 features of attack class.

In the dataset of this research, there are 41 features which are selected only normal and DDoS attacks

Data Pre-Processing



1,1,0,TCP, Normal

~~1,1,0,TCP, Normal~~

0,1,0,TCP, Normal

1,1,1,TCP, Normal

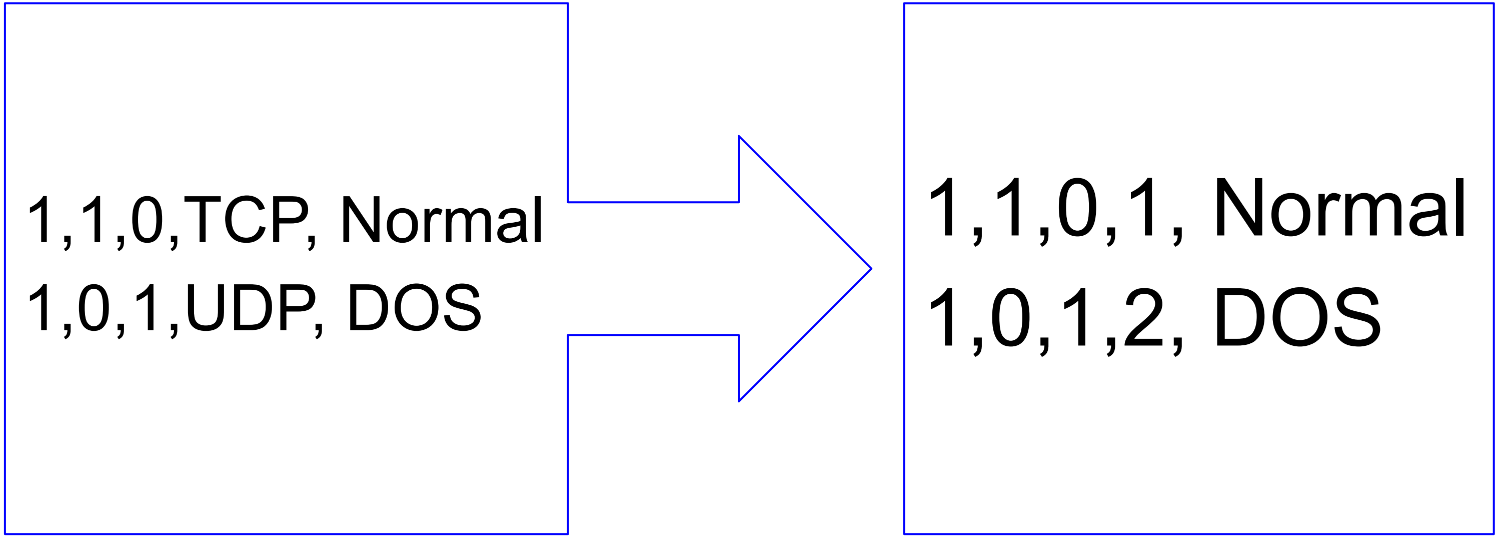
1,0,1,UDP,DOS

~~1,0,1,UDP,DOS~~

Removed Duplicate Data.

Data Pre-Processing

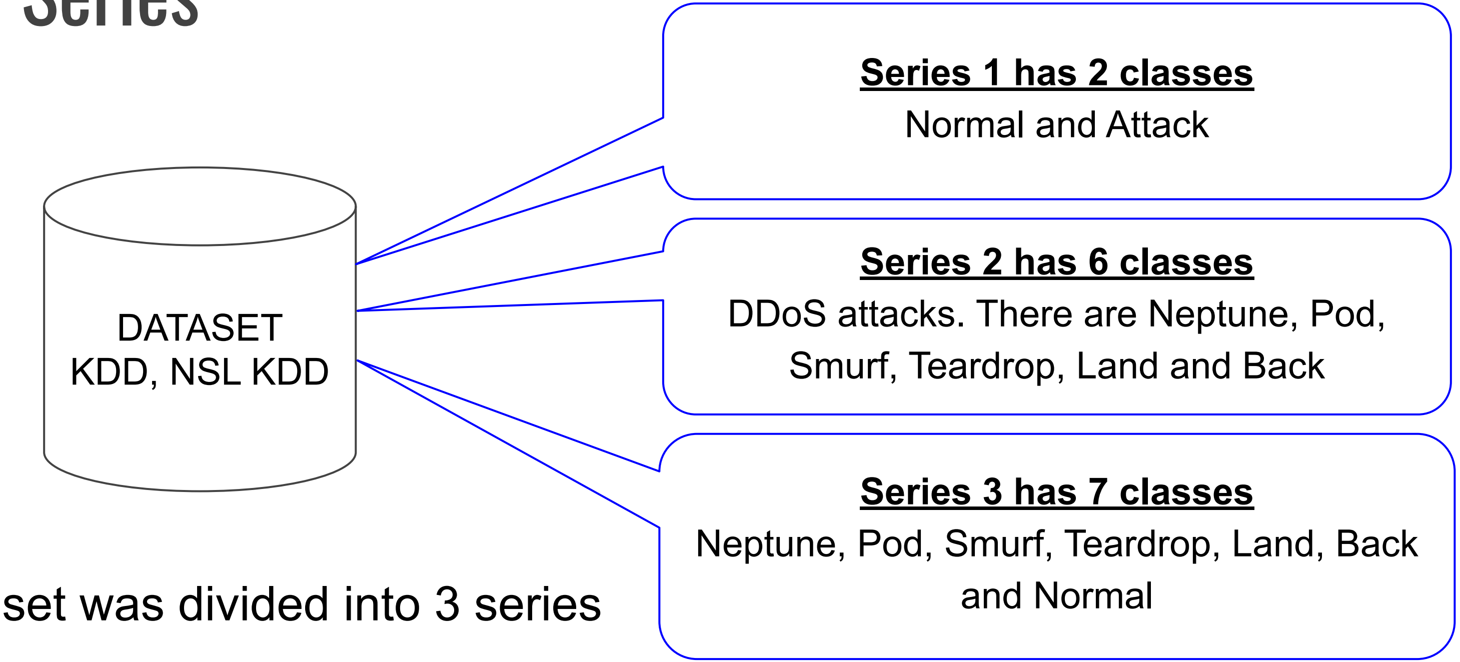
Convert Alphabet to Numeric



1,1,0,TCP, Normal
1,0,1,UDP, DOS

1,1,0,1, Normal
1,0,1,2, DOS

Data Series



DATASET
KDD, NSL KDD

Series 1 has 2 classes

Normal and Attack

Series 2 has 6 classes

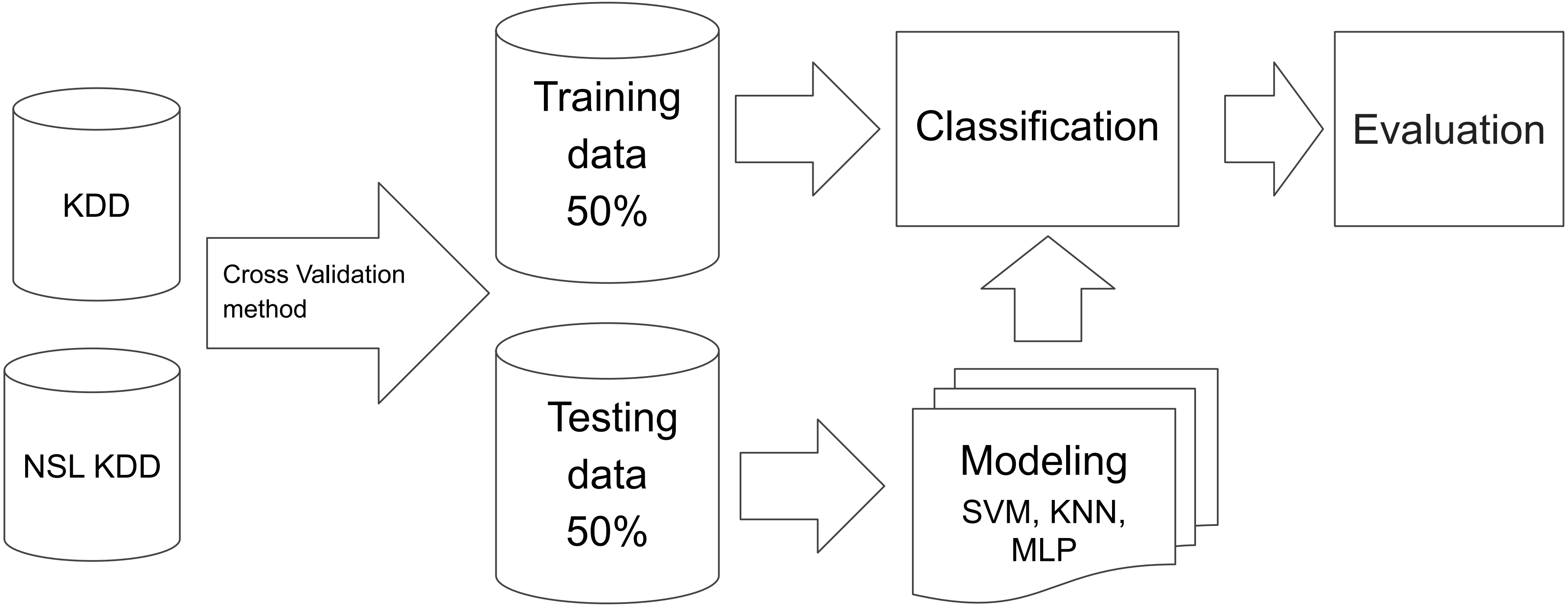
DDoS attacks. There are Neptune, Pod, Smurf, Teardrop, Land and Back

Series 3 has 7 classes

Neptune, Pod, Smurf, Teardrop, Land, Back and Normal

The dataset was divided into 3 series

Modeling of Data for DDoS Attacks Classification



KDD

NSL KDD

Cross Validation method

Training data 50%

Testing data 50%

Classification

Evaluation

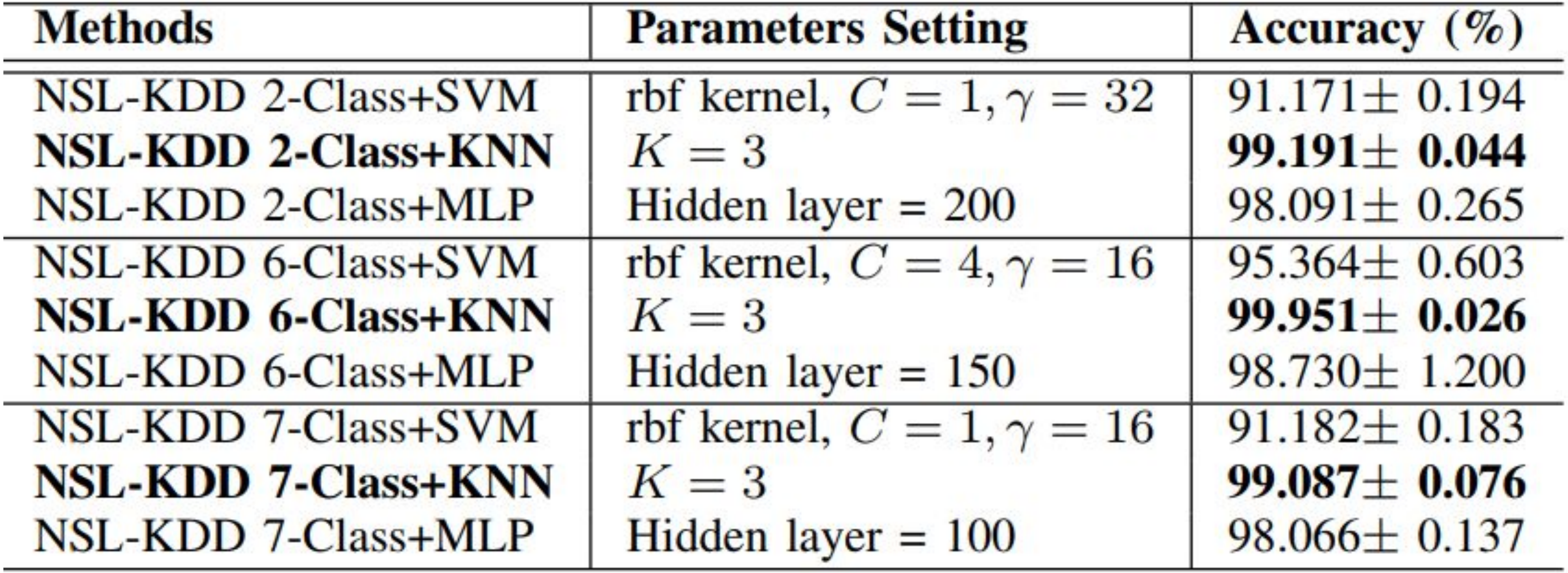
Modeling

SVM, KNN, MLP

TABLE I: Accuracy Results of the KDD Dataset

Methods	**Parameters Setting**	**Accuracy (%)**
KDD 2-Class+SVM	rbf kernel, $C = 8, \gamma = 16$	98.946± 0.022
KDD 2-Class+KNN	$K = 3$	**99.983**± **0.003**
KDD 2-Class+MLP	Hidden layer = 150	98.833± 0.131
KDD 6-Class+SVM	rbf kernel, $C = 8, \gamma = 32$	98.781± 0.020
KDD 6-Class+KNN	$K = 3$	**99.998**± **0.002**
KDD 6-Class+MLP	Hidden layer = 20	99.981± 0.131
KDD 7-Class+SVM	rbf kernel, $C = 4, \gamma = 32$	99.096± 0.027
KDD 7-Class+KNN	$K = 3$	**99.984**± **0.002**
KDD 7-Class+MLP	Hidden layer = 500	99.944± 0.019

TABLE II: Accuracy Results of the NSL-KDD Dataset



Methods	**Parameters Setting**	**Accuracy (%)**
NSL-KDD 2-Class+SVM	rbf kernel, $C = 1, \gamma = 32$	91.171± 0.194
NSL-KDD 2-Class+KNN	$K = 3$	**99.191± 0.044**
NSL-KDD 2-Class+MLP	Hidden layer = 200	98.091± 0.265
NSL-KDD 6-Class+SVM	rbf kernel, $C = 4, \gamma = 16$	95.364± 0.603
NSL-KDD 6-Class+KNN	$K = 3$	**99.951± 0.026**
NSL-KDD 6-Class+MLP	Hidden layer = 150	98.730± 1.200
NSL-KDD 7-Class+SVM	rbf kernel, $C = 1, \gamma = 16$	91.182± 0.183
NSL-KDD 7-Class+KNN	$K = 3$	**99.087± 0.076**
NSL-KDD 7-Class+MLP	Hidden layer = 100	98.066± 0.137

CONCLUSION

- Find a special feature
- Reduce the number of features
- Not reduce the accuracy rate

THANK YOU!