Applied Information Technology And Computer Science Vol. 2 No. 2 (2021) 219-235
© Universiti Tun Hussein Onn Malaysia Publisher's Office

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

A Comparative Study between Deep Learning Algorithm and Bayesian Network on Advanced Persistent Threat (APT) Attack Detection

Ooi Hui Ni, Nurul Hidayah Ab Rahman*

Faculty of Computer Science & Information Technology,
Universiti Tun Hussein Onn Malaysia, Parit Raja, 86400, MALAYSIA

DOI: https://doi.org/10.30880/aitcs.2021.02.02.015
Received 15 June 2021; Accepted 09 September 2021; Available online 30 November 2021

Abstract: Advanced Persistent Threat (APT) attacks are a major concern for the cybersecurity in digital world due to their advanced nature. Attackers are skilful to cause maximal destruction for targeted cyber environment. These APT attacks are also well funded by governments in many cases. The APT attacker can achieve his hostile goals by obtaining information and gaining financial benefits regarding the infrastructure of a network. It is highly important to study proper countermeasures to detect these attacks as early as possible due to sophisticated methods. It is difficult to detect this type of attack since the network may crash because of high traffic. Hence, in this study, this research is to study the comparison between Multilayer Perceptron and Naïve-Bayes of APT attack detection. Since the APT attack is persistent and permanent presence in the victim system, so minimal false positive rate (FPR) and high accuracy detection is required to detect the APT attack detection. Besides, Multilayer Perceptron algorithm has high true positive rate (TPR) in the detection of APT attack compared to Naïve Bayes algorithm. This means that Multilayer Perceptron algorithm can detect APT attack more accurately. Based on the result, it also can conclude that the lower the false positive rate (FPR), the more accurate to detect APT attack. Lastly, the research would also help to spread the awareness about the APT intrusion where it possibly can cause huge damage to everyone.

Keywords: accuracy, APT attack, Bayesian Network, deep learning algorithm, NSL-KDD dataset

1. Introduction

In recent years, Advanced Persistent Threats (APTs) have become a new security risk for companies and governments. Advanced persistent threat (APT) attack is a broad term used to describe a long-term presence on a network in order to destroy sensitive data [1]. This attack is a high-scale attack and needs a long period of time to be performed by highly skilled and highly motivated people [2]. The APT attackers use small companies as stepping-stones to gain access to large organizations by avoiding all the detection. APT attack is observed as a multi-vector multi stage attack with a continuous strategic

**Corresponding author: hidayahar@uthm.edu.my* campaign [3]. APT attack also is an advanced network attack, with the purpose of long-term espionage or maximal destruction for target systems and networks. It has multiple functionalities that include multiple simultaneous attack vectors with different phases, masquerading as communication data, random changes in execution time intervals, horizontal and vertical connections and mimicking legitimate traffic APTs have been recognized as a threat. The functionalities are developed to avoid detection for as long as possible and are not so highly detecting.

The complexity and variety of cyber attacks are continually increasing [4]. Although virus scanners, firewalls and intrusion detection and prevention systems (IDPSs) have been able to detect and prevent many cyber attacks, there are still many cyber-criminals developed more advanced methods and techniques to intrude into the target's network.

This trend is currently being pushed by cyber warfare and the emergence of the Internet of Things [3]. The annual cost of cyber attacks was $3 trillion in 2015. Besides, it is expected to increase more than $6 trillion per annum by 2021 [5]. Interest in research and investment towards developing new cyber-attacks defence methods and techniques were already caused by high cost.

Moreover, many of the defence approaches against cyber-attacks consider those attacks are targeting random networks. Thus, they assume that the attacker can surrender and move onto an easier target if the company's network is well protected. The assumption is no longer valid with the rise of targeted attacks, Advanced Persistent Threats (APTs), in which both cyber-criminals and hackers are targeting selected organizations and persisting until they achieve their goals from a technical report by Trend Micro.

The APT attack is a persistent, targeted attack on a specific organization and is performed through several steps. The main aim of APT is espionage and then data exfiltration. Therefore, APT is considered as a new and more complex version of multi-step attack. Moreover, the economic damage due to a successful APT attack is significant [6]. The potential cost of attacks is the major motivation for the investments in intrusion detection and prevention systems.

Most of the research like [7] and [6] in the area of APT detection, has focused on analysing already identified APTs, or detecting a particular APT that uses a specific piece of malware. However, they face serious shortcomings in achieving real time detection to detect all APT attack steps. The balance between false positive and false negative rates and the correlating of events spanning over a long period of time. However, the accurate and timely detection of APT remains a challenge.

Deep learning is one of the subsets of machine learning in the field of artificial intelligence. Deep learning allows machines to solve complex problems even when using a data set that is very unstructured and interconnected. The Multilayer Perceptron Neural Network (MLPNN) is one of the deep learning methods used to solve problems that require supervised learning and parallel distributed processing.

Bayesian Network is a classification model in data mining. It represents knowledge about an uncertain domain where each node corresponds to a random variable [6]. Besides, each edge represents the conditional probability for the corresponding random variables. The Bayesian Network model has a graphical scheme that represents prediction variables and their eventual connections using a directed or non-circular signal graph. By comparing two different methods of detection of APT attack, it is possible to get certain types of anomalies and behaviour of APT attack.

This research is carried out with three-fold objectives. First, to study a deep learning algorithm and Bayesian Network for detecting the APT attack. Second, to analyse the accuracy, true positive rate

(TPR) and false positive rate (FPR) of APT attack. Third, to compare between the classification of Naïve Bayes and Multilayer Perceptron for APT detection method by using Weka Software.

This research work aims to compare deep learning algorithms and Bayesian Network which is more accurate to detect the APT attack. The plan is to conduct this research in three phases. In the first phase, NSL-KDD dataset was collected to pass through the classification of Bayesian Network and Deep Learning by using Weka software. The plan proceeds to prove the accuracy of the detection of APT attack. The third phase of this research work is to define a method that can highly detect the APT attack.

The rest of the paper is organized as follows: Section 2 is Literature Review, Section 3 is Methodology, Section 4 is Result and Discussion. Lastly, Conclusions and Future Works are presented in Section 5.

2. Literature Review

2.1 Advanced Persistent Threat (APT)

Advanced Persistent Threat describes malicious, organized, and highly sophisticated cyber operations where an external backing agency was responsible for the strategic goals [8]. The APT attacks consist of two characteristics which are purposes and targets [9]. The purposes of APT attack are to take advantage of vulnerabilities in targeted intelligent information collection systems; to steal data and information and sell confidential or sensitive information to opponents; to sabotage the infrastructure of organizations, governments; to sabotage the credit of the targeted organizations. The targets of APT attacks in sector industries are Military and Aerospace; Finance and banking; IT businesses; Governments and other agencies [10].

The process of APT attack has eight phases which includes (i) target selection, (ii) information gathering, (iii) point of entry, (iv) escalate privileges, (v) command and control communications, (vi) lateral movement, (vii) asset discovery persistent and (viii) data exfiltration. There is a specific target or chosen organization for the APT attack that the attacker is likely to attack. The first phase is target selection which means to find the targeted victim before collecting the information to attack the targets. The victims could be individuals, companies, government sectors, and organizations [7]. In the information gathering phase, the attacker will perform a complete study about the organization. Attackers will gather the information of the operating system used, the models of the computer network, the company profiles, and the nature of business that company runs. Figure 1 shows the anatomy of point of entry to gain access to the system. After collecting information, the process will go through the point of entry for planning to initiate and exploit the network. During the escalate privileges phase, the system has been exploited by the attacker [7]. The APT attack has successfully compromised the network of the organization. Then, the command-and-control communication phase is where the APT infiltrates the systems and communicates with the attacker. This means that C&C communication phase provides ways of attackers to break the system [7]. The APT will gather and steal as much information from the compromise network during this phase. The last phase of APT attack is lateral movement, the attackers must remain in the system before being detected. The attacker needs to remain in the system undetected by moving fast. APT starts reconnaissance, credentials, stealing, and infiltrating others' computers without staying in one place.

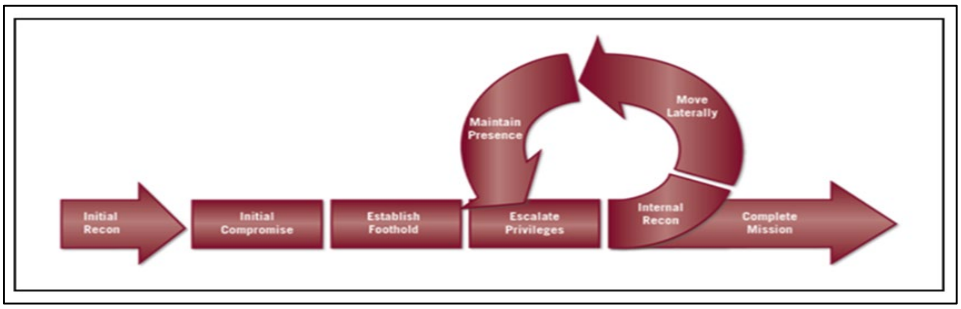


Figure 1: The anatomy of point of entry stages to gain access into the system [7].

2.3 APT Attack Detection

Detecting APT attacks based on intrusion detection systems have three methods such as APT malware, malicious Uniform Resource Locator (URL), and malicious Domain Name System (DNS) detection [8]. These intrusion detection systems to detect APT attacks can be classified into two threads which are Signature-based detection and Behaviour-based detection [8]. Signature-based detection is based on the signatures of malicious code of APT attacks. The efficiency of this strategy is very low. Generally, APT attack exploits zero-day vulnerability to gain the access privilege of the targets. For example, Stuxnet [11] exploited four zero-day vulnerabilities in windows operating system including Windows print spooler (MS10-061), Win32k Keyboard Layout (MS10-073), LNK format (MS10-046), and task scheduler (MS10-092). These exploits are nearly impossible to be detected by signature-based detection. Behaviour-based detection is an advanced strategy to detect new malicious code trends. This technique is focused not only on malicious APT code signatures, but also on APT code activity. This technique leads to higher productivity along with high costs of production [11]. In this research, features of Dos, Probe, U2R, and R2L are used to detect APT attack using behaviour-based detection.

A detailed analysis on the NSL-KDD data set using various machine learning techniques is done in [12] available in the WEKA tool. The inherent drawbacks in the KDD cup 99 dataset [13] has been revealed by various statistical analyses has affected the detection accuracy of many IDS modelled by researchers. It contains redundant records of the complete KDD data set. Thus, NSL-KDD data set provided by knowledge discovery [11] was used because its network communication protocol and attack behaviour patterns remain unchanged. Multilayer Perceptron and Naïve-Bayes classification method were then used for the data set experiments and pass through the training and testing NSL-KDD dataset. The model was then used to establish the APT attack detection system. Detection and defence covered all stages of the APT attack to achieve the best result.

2.4 Deep Learning Algorithm

Deep learning is one of the machine learning types. Deep learning algorithms present to draw similar conclusions as humans would continue to analyse data with a given logical structure. In deep learning, multi-layered deep neural networks are introducing multi-layered learning of the features as the main characteristic [14]. A network is considered as a deep learning network due to it having more than two hidden layers in the neural network.

Multilayer perceptron (MLP) is a back-propagation neural network with high learning accuracy and fast recall under deep learning algorithm. It is a popular neural network that has wide range of applications which are sample identification, bifurcation problems, function simulation, prediction, system control, noise filtering, data compression [14].

Multilayer Perceptron is through $f(\cdot) : Rm \rightarrow Ro$, m is the dimension at input and o is the dimension at output. The algorithm can classify the data using nonlinear approximation or perform regression y by inputting the feature $X = x1, x2, . . . xm$ and the target value Y. Multilayer Perceptron can have many nonlinear layers inserted between the input and output layers.

2.5 Bayesian Network

A Bayesian network stands for the causal probabilistic relationship among a set of random variables. It provides a compact representation of a joint probability distribution [15]. Naive Bayes is under the Bayesian Network and it predicts the results of classification according to the Bayesian theorem. Naive Bayes is mainly used to calculate the data of unknown categories and the probability of its belonging to a category. Bayesian classification achieves least error by analysing probability statistics and calculating the likelihood of a new instance in each category using known category attribute probability values. The probability of each category is compared and the case will be classified as the category with the greatest probability. Assume that event $c_1, c_2, . . ., c_n$ is in n category data collection sample space, an observe quantity $\mathbf{X} = [x_1, x_2, . . ., x_r]^T$ is then given which has an r features parameter. According to the Bayesian theorem, the classification ci belongs to the observe quantity $\mathbf{X}$, and the error probability of classification can be expected to be minimized. The following Equation (1) can be obtained from the Bayesian theorem.

$$P(Ci|X\,) = \frac{P(Ci)P(X|Ci)}{P(X)(12)} \qquad Eq.1$$

2.6 Dataset

In this research, NSL-KDD dataset is used to detect the APT attack (see Table 1). NSL-KDD is a data set suggested to solve the intrinsic problems of the KDD'99 data set [16]. NSL-KDD dataset also consists of only selected records from the complete KDD dataset. It does not suffer from any fault. From McHugh study [17], the standardized genre of the KDD dataset still suffers from some of the problems. Due to the lack of public datasets for network based IDSs, it may not be a perfect illustrative of existing real networks.

Moreover, the number of records in the NSL-KDD train and test sets are reasonable compared to KDD’99 data sets. NSL-KDD dataset is affordable to run the experiments on the complete set without the need to randomly select a small portion. The improvement of the KDD'99 Data Set to the NSL-KDD data set has brought a lot of benefit over the original KDD data set. The following are advantages [18]:

- It has a lower bias value as there is no redundancy of the data or duplicates records in the train set.
- The number of records in the proposed test sets is not duplicate. So, the performance of the learners is not biased by the methods which have better detection rates on frequent records.
- The number of selected records is inversely proportional to the percentage of records in the original KDD dataset.
- It produces better precision in various learning techniques.

Table 1: List of NSL-KDD dataset files and the description [18].

S.NO.	Name of the file	Description
1	KDDTrain+.ARFF	The train set in ARFF with binary labels format.
2	KDDTrain+.TXT	The full NSL-KDD train set including attack-type labels and difficulty level in CSV format.

Table 1: (cont.)

S.NO.	Name of the file	Description
3	KDDTest+.ARFF	The full NSL-KDD test set with binary labels in ARFF format.
4	KDDTest+.TXT	The full NSL-KDD test set including attack-type labels and difficulty level in CSV format.
5	KDDTest-21.ARFF	A subset of the KDDTest+.arff file which does not include records with difficulty level of 21 out of 21.
6	KDDTest-21.TXT	A subset of the KDDTest+.txt file which does not include records with difficulty level of 21 out of 21.

From Table 1, KDDTrain+.ARFF and KDDTest+.ARFF is used to conduct this research. This is because these two datasets do not contain the redundant data. Number of individual records in four types of attacks for both training and testing in Figure 2 and Figure 3.

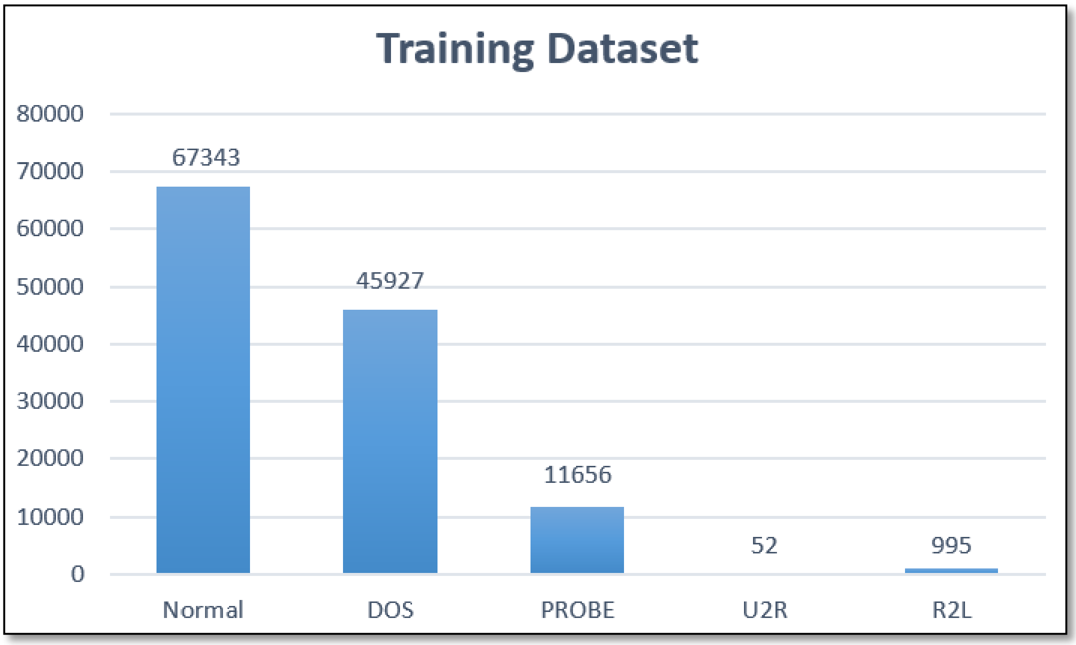


Figure 2: Number of instances in Training Dataset.

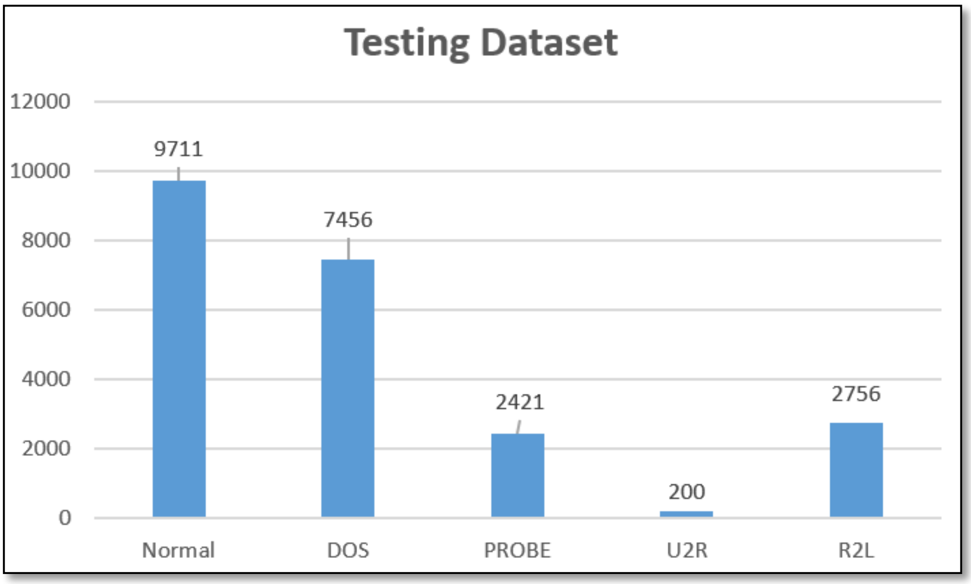


Figure 3: Number of instances in Testing dataset.

3. Methodology

Figure 4 presents the research model that is adopted from the study of author Joloudari [19]. First, an NSL-KDD dataset is collected to analyse the APT detection. The dataset is taken from the official website https://www.unb.ca/cic/datasets/nsl.html which is UNB, Canadian Institute for Cybersecurity. In this research, there are 148517 data samples in this dataset and splitting into 15% testing and 85% training dataset. The number of instances in testing dataset is 22544 while the number of instances in training dataset is 125973.

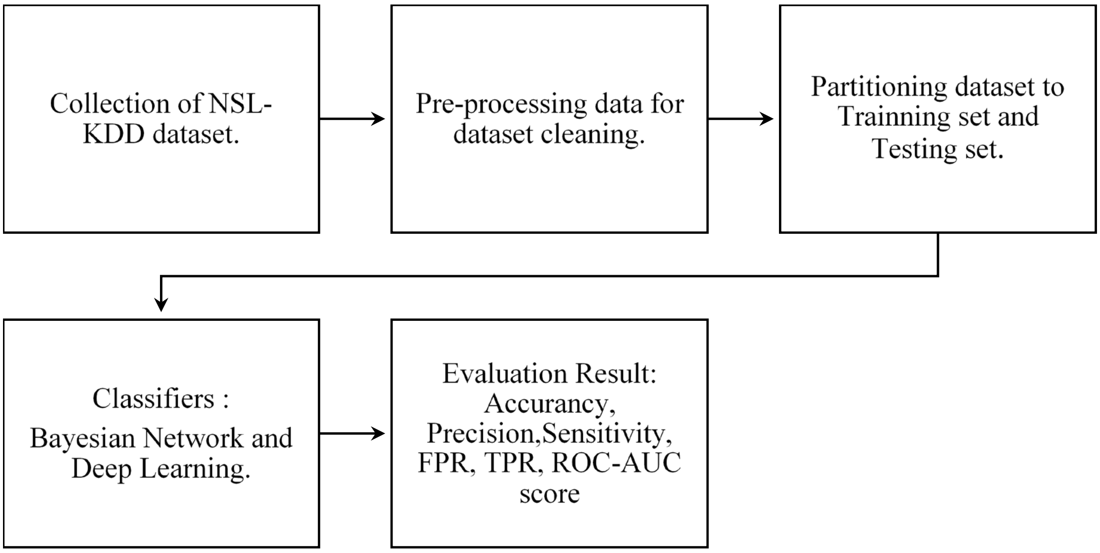

Collection of NSL-KDD dataset.
Pre-processing data for dataset cleaning.
Partitioning dataset to Trainning set and Testing set.
Classifiers :
Bayesian Network and Deep Learning.
Evaluation Result: Accurancy, Precision,Sensitivity, FPR, TPR, ROC-AUC score

Figure 4: Research Model

Secondly, the dataset is pre-processed for data cleaning and data featuring using Weka software. There are forty-two features inside the NSL-KDD dataset. According to the features of this dataset, the data types are categorical, numerical, and nominal data. The data set is then initially pre-processed and normalized to a range 0 -1. This is done as a requirement because certain classifiers produce a better accuracy rate on normalized data set.

Next, the NSD-KDD dataset is split into training data and test data. Classifying the data using the classifiers which are Multilayer Perceptron and Naïve-Bayes algorithm. Bayesian network classification model is according to Bayes' theorem. The philosophy of this model is based on a possible framework to solve the classification problems. This theorem is based on the probability of occurring or not occurring an event so that the probability of an event is calculated. The Bayes' theorem is as follows:

$$P(D|B) = \frac{P(B,D)}{}P(B) \qquad Eq.2$$

$$P(D|\, B) = P(B,D)P(D)/\, P(B) \qquad Eq.3$$

Naive Bayes calculates the posterior probability for each class. Naive Bayes makes a prediction for the class with the highest probability. So, it supports both binary classification and multi-class classification problems.

For the deep learning model, the philosophy is derived from the architecture of biological neural networks in the human brain under artificial neural networks. It is a branch of machine learning and artificial intelligence. In deep learning model, it is a multilayer perceptron is used in this research in the weka. Multilayer perceptron as the main characteristic. These layers are called hidden layers in the neural network, and a network is considered as a deep learning network, when it includes more than two hidden layers.

The experiments were carried out in WEKA. The effectiveness of the classification algorithms in classifying the NSL-KDD data set is also analysed. The accuracy rate in detecting normal and abnormal class is evaluated and discussed in the discussion part. The result is presented in accuracy, precision, sensitivity, False positive rate (FPR), True Positive Rate (TPR). These evaluation methods are discussed in the next section.

3.1 Method Evaluation

In this research, the confusion matrix (see Table 2) is used to evaluate the research model. There are four elements in this matrix which are True Positive (TF), False Positive (FP), True Negative (TN), and False Negative (FN). The basic definitions are as follows [20]:

- TP: It shows that when APT attack is not detected, but it occurs.
- FP: It shows that when APT attack is not detected, but it does not occur.
- TN: It shows that when APT attack is not detected, but it does not occur.
- FN: It shows that when APT attack is not detected, but it occurs.

Table 2: Confusion matrix for APT attack detection

The Actual Class	The Predicted Class	
	Anomaly	Normal
Positive	True Positive	False Positive
Negative	False Negative	True Negative

According to the confusion matrix, there are seven criteria to evaluate Bayesian, and deep learning. The criteria are accuracy, true positive rate (TPR), False Positive rate (FPR)**.** If the algorithm has higher value of accuracy and true positive rate (TPR), this means that the algorithm can detect APT attack more accurately. Besides, the lower the false positive rate (FPR), this means that the algorithm also can detect the APT attack more accurately.

3.2 Hardware And Software

Table 3 presents the hardware and software that were used in this research.

Table 3: Hardware and software

Hardware	Software
● Lenovo Laptop with RAM 4GB ● Processor Intel i5	● Microsoft Windows 10 Operating System ● Weka 3.8.4

4.0 Result and Discussion

During the data collection, the NSL-KDD testing dataset and NSL-KDD training dataset is taken from the authorised source which has been conducted the experiment regarding the detection of APT attack [21].

4.1 Result on NSL-KDD Testing Dataset

From testing dataset, the results in Table 4 showed that Multilayer Perceptron algorithm has a higher accuracy which is 95.95% compared to Naïve Bayes algorithm which has only 80.73%. This means that Multilayer Perceptron algorithm is more easily to detect APT attack compared to Naïve Bayes algorithm [15].

Besides, by comparing the result of true positive rate (TPR) also can know that Multilayer Perceptron algorithm can detect APT attack more accurately due to it has high true positive rate which is 0.945 while Naïve Bayes algorithm only has 0.807 true positive rate (TPR) [22].

On the other hand, the lower the false positive rate, the more accurate of the APT detection [22]. The false positive rate (FPR) in Multilayer Perceptron algorithm is 0.056 which is lower than the false positive rate (FPR) in Naïve Bayes algorithm which is 0.158.

Table 4: Average Result on NSL-KDD Testing Dataset

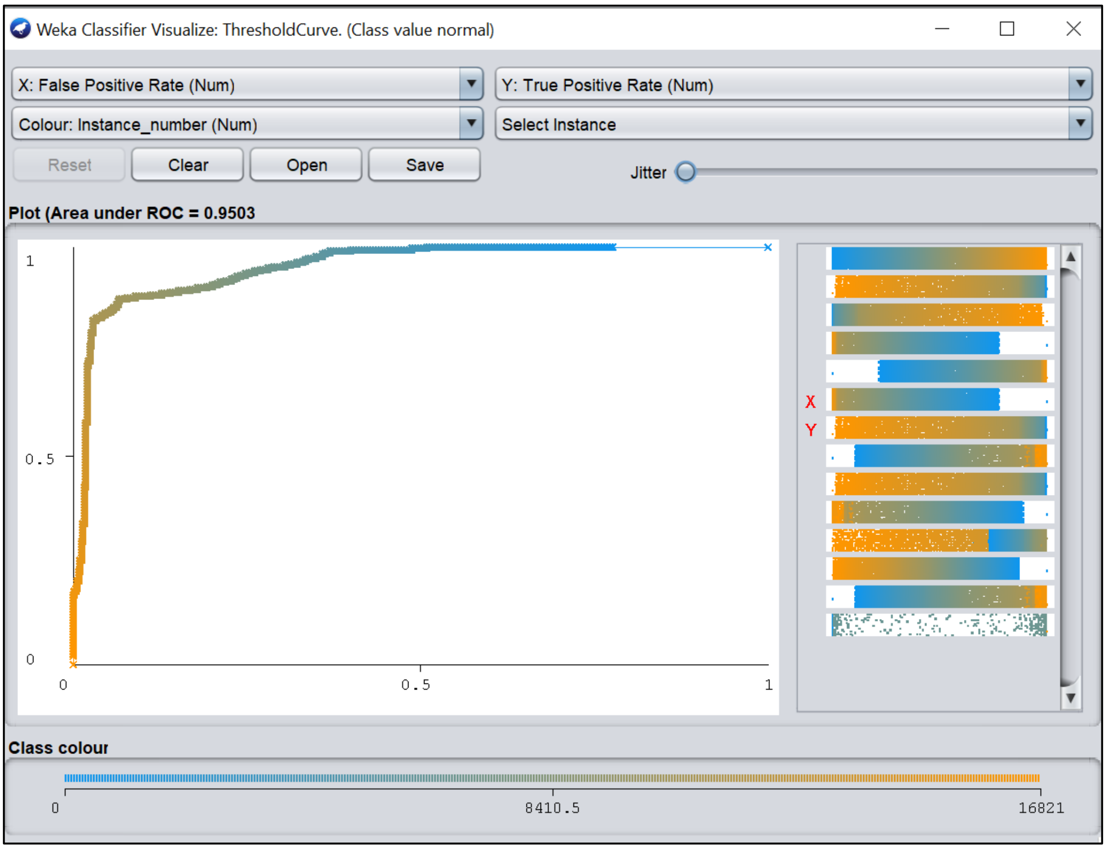
Algorithm	TP Rate	FP Rate	Precision	Recall	F-Measure	ACC %	ROC Area	PRC Area
Naïve Bayes	0.807	0.158	0.844	0.807	0.825	80.73	0.953	0.946
Multilayer Perceptron	0.945	0.056	0.945	0.945	0.945	95.95	0.977	0.974

The ROC-Curve is plotted using false positive rate (FPR) against true positive rate (TPR) to show the performance of a classification model at all classification thresholds. This means that is area of ROC is nearly equal to 1, the more accurate of the detection of APT attack.

Figure 5 and Figure 6 showed the ROC area of Naïve Bayes algorithm in class normal and abnormal using NSL-KDD Testing dataset which are 0.9503 and 0.9485.

Figure 7 and Figure 8 showed the showed the ROC area of Multilayer Perceptron algorithm in class normal and abnormal using NSL-KDD Testing dataset which are 0.9792 and 0.9794.

Based on the result of ROC area obtained, it showed that Multilayer Perceptron algorithm is more accurate to detect APT attack. This is because the ROC area in Multilayer Perceptron algorithm in class normal and abnormal are more nearly to 1 compared to ROC area in Naïve Bayes algorithm [23].


Weka Classifier Visualize: ThresholdCurve. (Class value normal)

X: False Positive Rate (Num)

Y: True Positive Rate (Num)

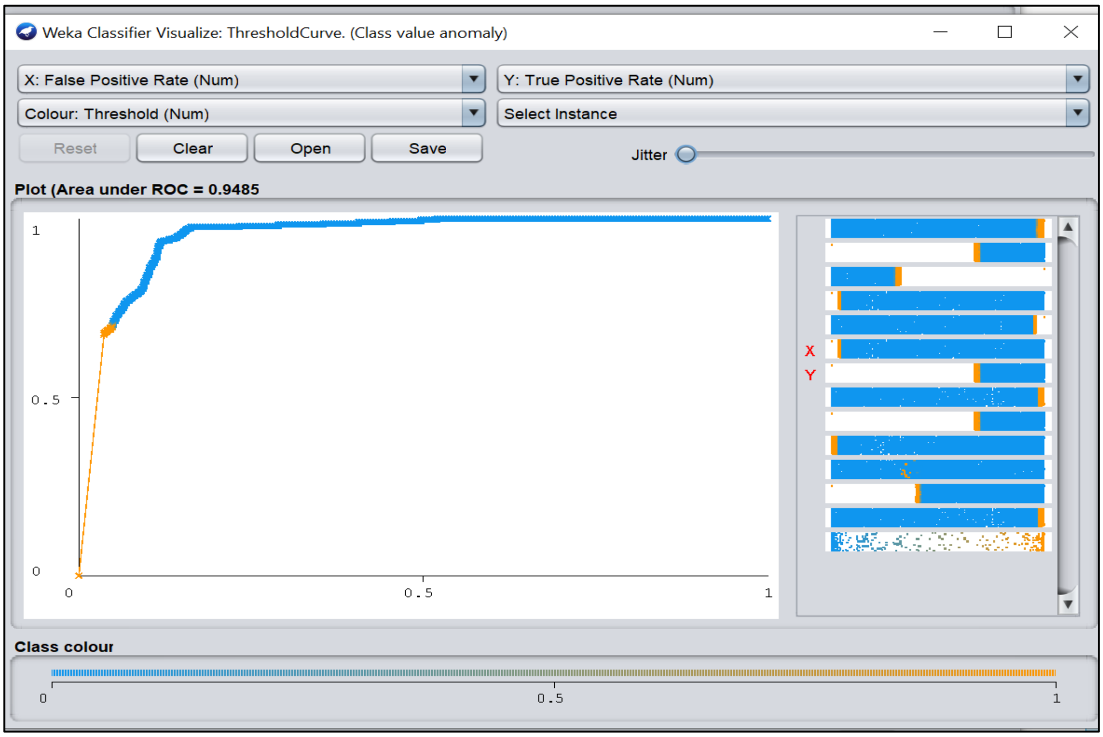
Colour: Instance_number (Num)

Select Instance

Plot (Area under ROC = 0.9503

Class colour

Figure 5: ROC-Curve of Naïve Bayes algorithm in class normal using NSL-KDD Testing dataset.



Weka Classifier Visualize: ThresholdCurve. (Class value anomaly)

X: False Positive Rate (Num)

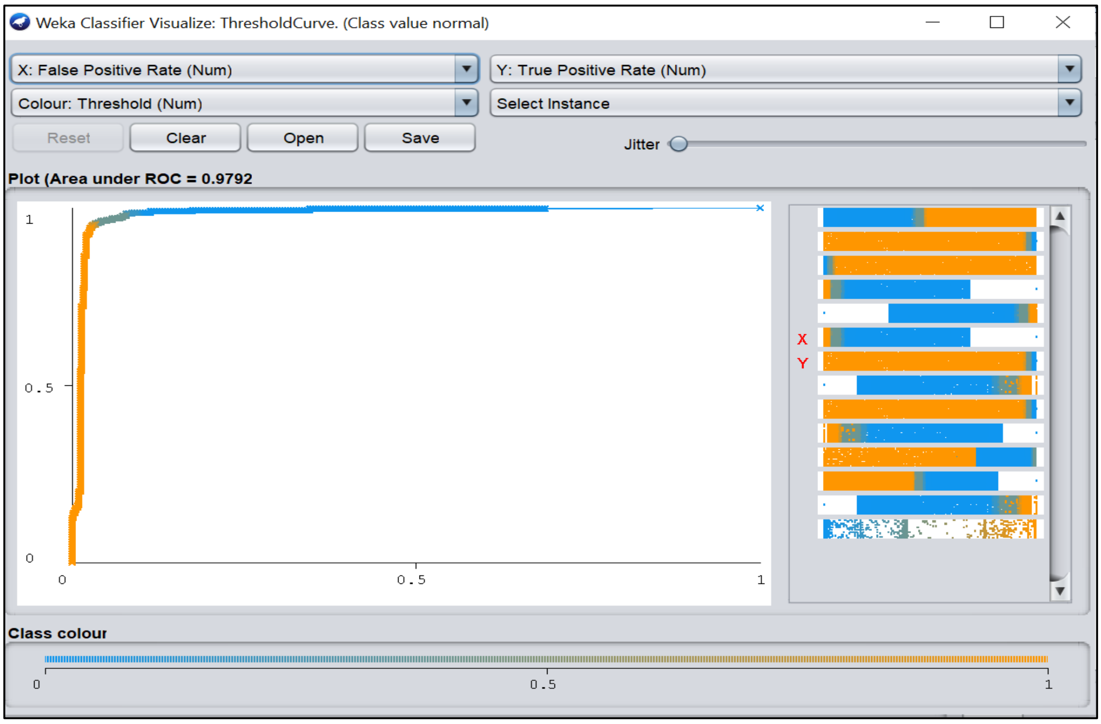
Y: True Positive Rate (Num)

Colour: Threshold (Num)

Select Instance

Plot (Area under ROC = 0.9485

Figure 6: ROC-Curve of Naïve Bayes algorithm in class abnormal using NSL-KDD Testing dataset.



Weka Classifier Visualize: ThresholdCurve. (Class value normal)

X: False Positive Rate (Num)

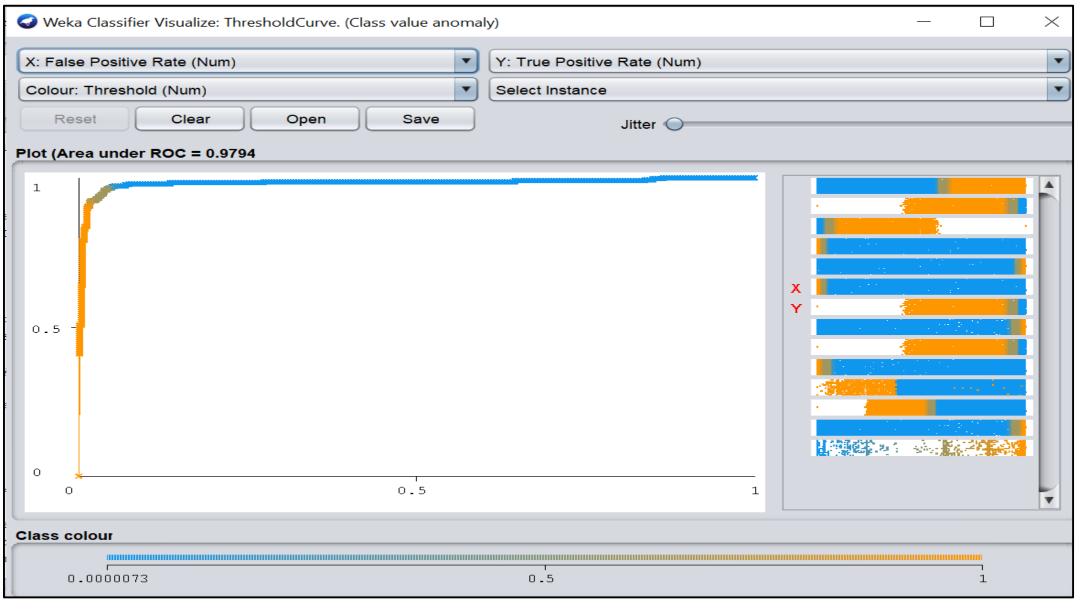
Y: True Positive Rate (Num)

Colour: Threshold (Num)

Select Instance

Plot (Area under ROC = 0.9792

Figure 7: ROC-Curve of Multilayer Perceptron algorithm in class normal using NSL-KDD Testing dataset.



Weka Classifier Visualize: ThresholdCurve. (Class value anomaly)

X: False Positive Rate (Num)

Y: True Positive Rate (Num)

Colour: Threshold (Num)

Select Instance

Plot (Area under ROC = 0.9794)

Class colour

Figure 8: ROC-Curve of Multilayer Perceptron algorithm in class abnormal using NSL-KDD Testing dataset.

Table 5: Performance Matrix Table for Naïve Bayes algorithm in NSL-KDD Testing dataset.

	Normal	Anomaly
Normal	9225	486
Anomaly	3858	8975

4.2 Result on NSL-KDD Training Dataset

From training dataset, the results in Table 6 showed that Multilayer Perceptron algorithm has a higher accuracy which is 98.43% compared to Naïve Bayes algorithm which has only 90.38%. This means that Multilayer Perceptron algorithm is more easily to detect APT attack compared to Naïve Bayes algorithm [24].

Besides, by comparing the result of true positive rate (TPR) also can know that Multilayer Perceptron algorithm can detect APT attack more accurately due to it has high true positive rate which is 0.985 while Naïve Bayes algorithm only has 0.904 true positive rate (TPR) [22].

On the other hand, the lower the false positive rate, the more accurate of the APT detection [22]. The false positive rate (FPR) in Multilayer Perceptron algorithm is 0.016 which is lower than the false positive rate (FPR) in Naïve Bayes algorithm which is 0.101.

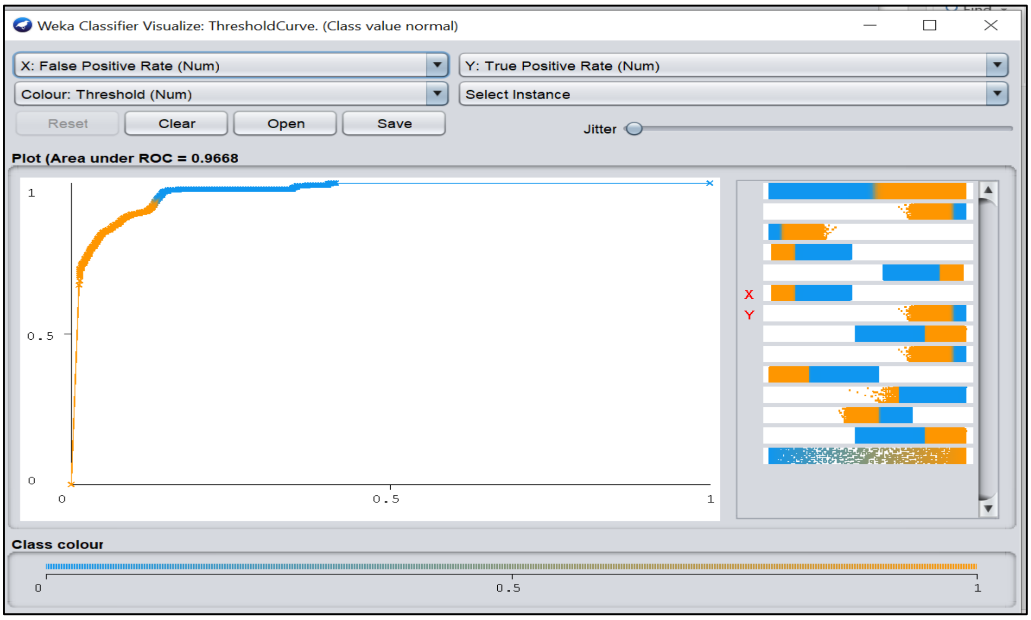
Table 6: Average Result on NSL-KDD Training Dataset

Algorithm	TP Rate	FP Rate	Precision	Recall	F-Measure	ACC %	ROC Area	PRC Area
Naïve Bayes	0.904	0.101	0.905	0.904	0.904	90.38	0.966	0.957
Multilayer Perceptron	0.985	0.016	0.985	0.985	0.985	98.43	0.996	0.995

Figure 9 and Figure 10 showed the ROC area of Naïve Bayes algorithm in class normal and abnormal using NSL-KDD Testing dataset which are 0.9503 and 0.9485.

Figure 11 and Figure 12 showed the showed the ROC area of Multilayer Perceptron algorithm in class normal and abnormal using NSL-KDD Testing dataset which are 0.9792 and 0.9794.

Based on the result of ROC area obtained, it showed that Multilayer Perceptron algorithm is more accurate to detect APT attack. This is because the ROC area in Multilayer Perceptron algorithm in class normal and abnormal are more nearly to 1 compared to ROC area in Naïve Bayes algorithm [15].



Weka Classifier Visualize: ThresholdCurve. (Class value normal)

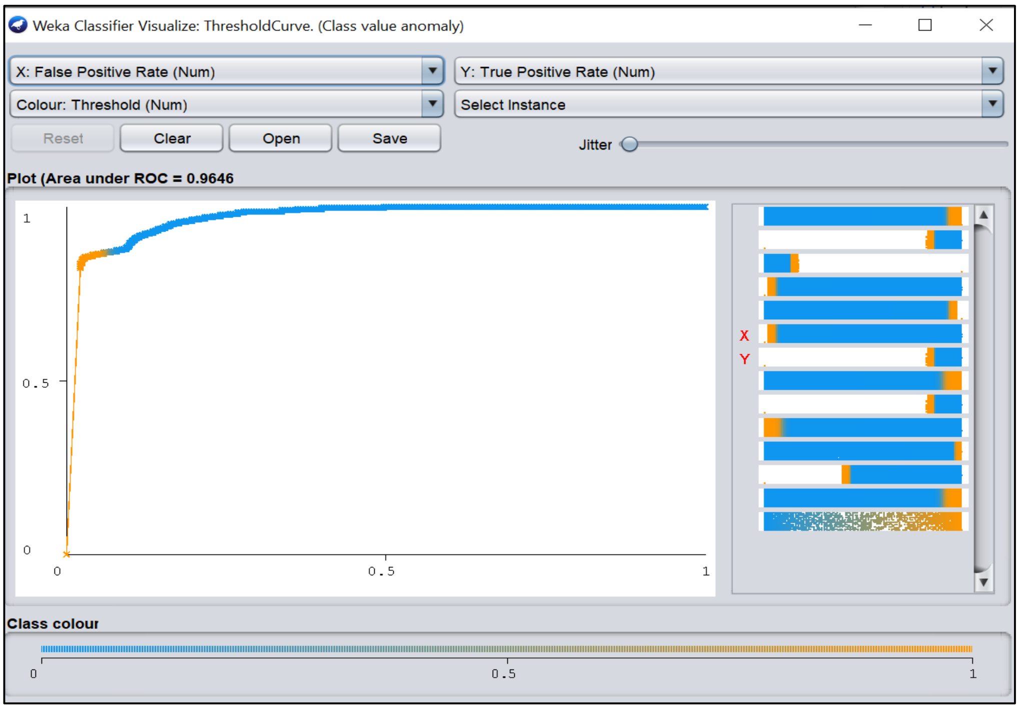
X: False Positive Rate (Num)

Y: True Positive Rate (Num)

Colour: Threshold (Num)

Plot (Area under ROC = 0.9668)

Figure 9: ROC-Curve of Naïve Bayes algorithm in class normal using NSL-KDD Training dataset.



Weka Classifier Visualize: ThresholdCurve. (Class value anomaly)

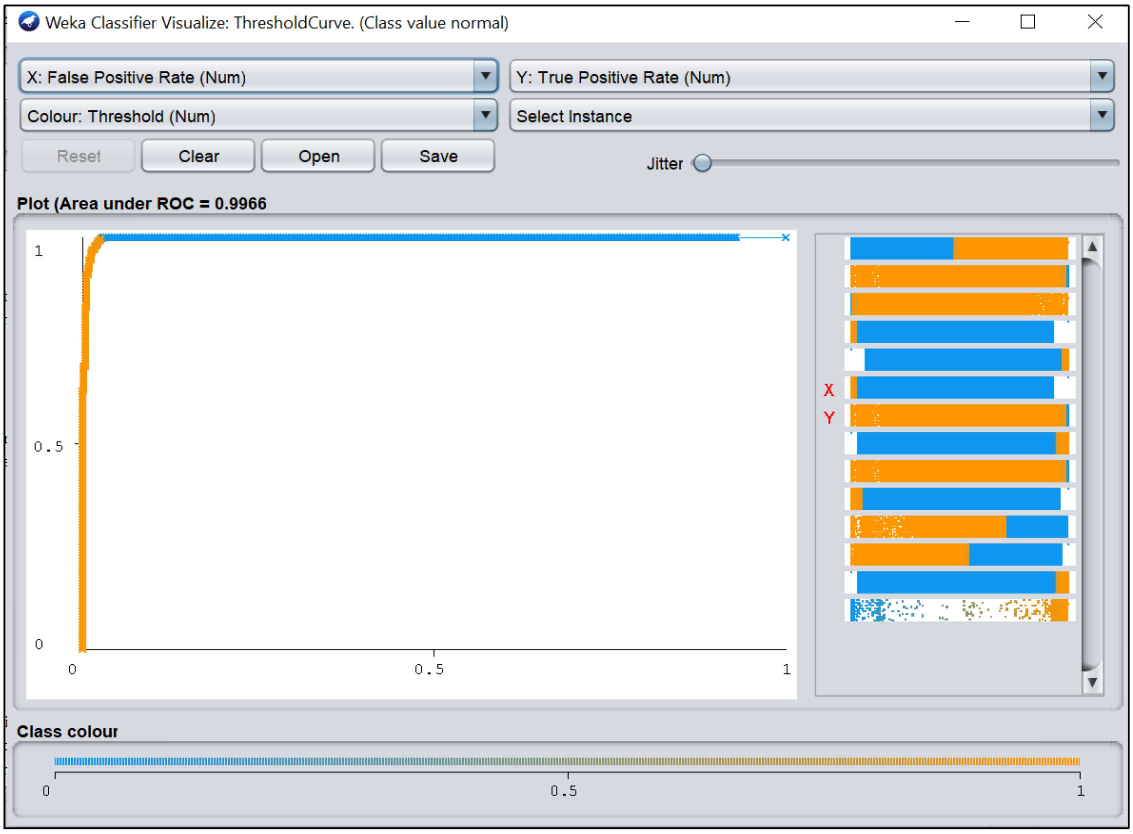
X: False Positive Rate (Num)

Y: True Positive Rate (Num)

Colour: Threshold (Num)

Plot (Area under ROC = 0.9646)

Figure 10: ROC-Curve of Naïve Bayes algorithm in class abnormal using NSL-KDD Training dataset.



Weka Classifier Visualize: ThresholdCurve. (Class value normal)

X: False Positive Rate (Num)

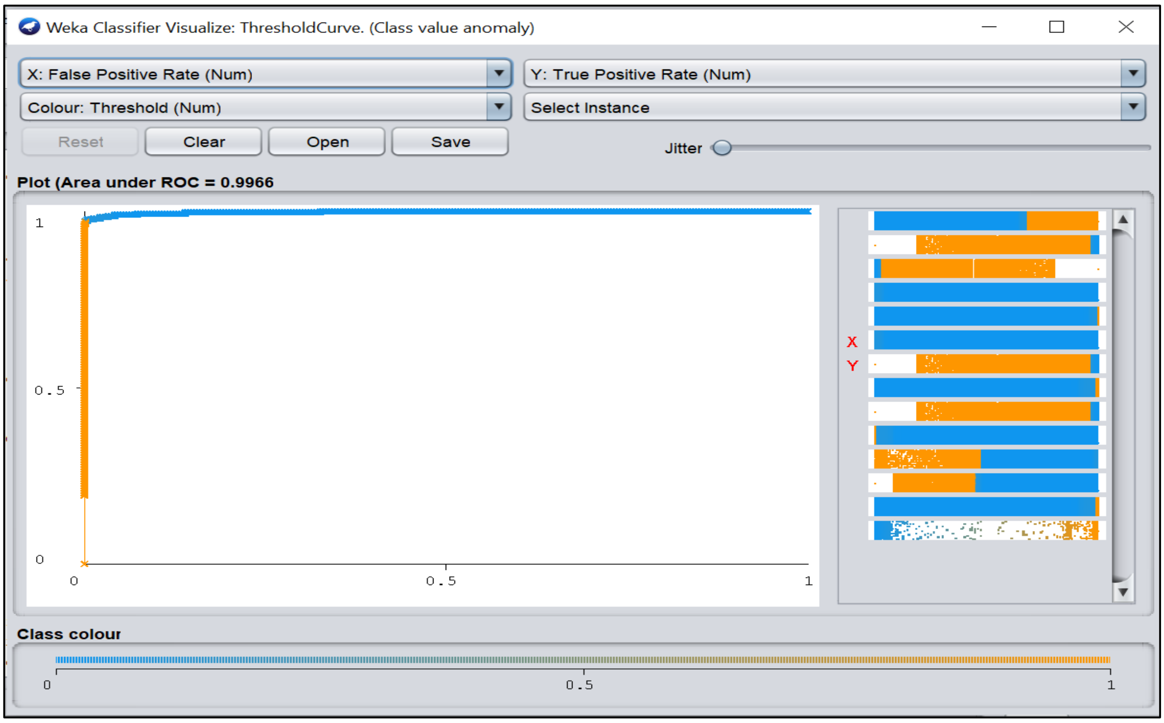
Y: True Positive Rate (Num)

Colour: Threshold (Num)

Select Instance

Plot (Area under ROC = 0.9966

Figure 11: ROC-Curve of Multilayer Perceptron algorithm in class normal using NSL-KDD Training dataset.



Weka Classifier Visualize: ThresholdCurve. (Class value anomaly)

X: False Positive Rate (Num)

Y: True Positive Rate (Num)

Colour: Threshold (Num)

Select Instance

Plot (Area under ROC = 0.9966

Figure 12: ROC-Curve of Multilayer Perceptron algorithm in class abnormal using NSL-KDD Training dataset.

Table 7: Performance Matrix Table for Naïve Bayes algorithm in NSL-KDD Training dataset.

	Normal	Anomaly
Normal	63060	4283
Anomaly	7832	60798

5.0 Conclusion and Future Work

This research is to study the comparison between Multilayer Perceptron and Naïve-Bayes of APT attack detection.

Overall, the detection of Advanced Persistent Threat (APT) attack between Multilayer Perceptron and Naïve-Bayes algorithm has achieved its objectives for research development.

This research had achieved the objectives in this research. First, the classification of Naïve Bayes and Multilayer Perceptron for detecting the APT attack are studied. Second, the accuracy, true positive rate (TPR) and false positive rate (FPR) of APT attack is analysed. Third, the classification of Naïve Bayes and Multilayer Perceptron for APT detection method by using Weka Software are compared.

Since the APT attack is persistent and permanent presence in the victim system, so minimal false positive rate (FPR) and high accuracy detection is required to detect the APT attack detection. Lastly, the research would also help to spread the awareness about the APT intrusion where it possibly can cause huge damage to everyone.

Besides, Multilayer Perceptron algorithm has high true positive rate (TPR) in the detection of APT attack compared to Naïve Bayes algorithm. This means that Multilayer Perceptron algorithm can detect APT attack more accurately. Based on the result, it also can conclude that the lower the false positive rate (FPR), the more accurate to detect APT attack.

The ROC-Curve is plotted using false positive rate (FPR) against true positive rate (TPR) to show the performance of a classification model at all classification thresholds. ROC area in Multilayer Perceptron algorithm in class normal and abnormal are more nearly to 1 compared to ROC area in Naïve Bayes algorithm. This further indicates that Multilayer Perceptron can detect APT attack more accurately.

There are two limitations in this research. The first limitation of the research is the scope of research and discussion. The scope and depth of discussions in this research paper is compromised in many levels compared to the works of experienced scholars since the years of experience of conducting research is short. Second limitation of the research is implementation of data collection method. There may have the chance that the nature of implementation of data collection method is flawed due to do not have an extensive experience in primary data collection.

The recommendation for the future work is to conduct research using a combination of machine learning and deep learning algorithms and implement to NSL-KDD dataset to analyse the APT intrusion accurately. Besides, the researcher also can conduct research at different stage. As APT is a multi-step attacks, detecting a single stage of an APT technique itself does not simply detecting an APT attack as mentioned [9].

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support and encouragement throughout the process of conducting this study.

References

[1] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” Leading Issues in Information Warfare & Security Research, 2011.

[2] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, “BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset,” IEEE Access, vol. 8, pp. 29575–29585, 2020, doi: 10.1109/ACCESS.2020.2972627.

[3] T. Bodström and T. Hämäläinen, “Title: Year: A Novel Method for Detecting APT Attacks by Using OODA Loop and Black Swan Theory,” Lect. Notes Comput. Sci., pp. 498–509, 2018, doi: 10.1007/978-3-030-04648-4_42.

[4] Y. Wang, Q. Li, Z. Chen, P. Zhang, and G. Zhang, “A Survey of Exploitation Techniques and Defenses for Program Data Attacks,” Journal of Network and Computer Applications, vol. 154. Academic Press, Mar. 15, 2020, doi: 10.1016/j.jnca.2020.102534.

[5] Cybersecurity Ventures, “A cybercrime Revelation, 2016 Cybercrime Report, Cybersecurity Ventures.,” 2016.

[6] M. B. Rao and C. R. Rao, “Bayesian networks,” in Handbook of Statistics, vol. 32, Elsevier B.V., 2014, pp. 357–385.

[7] “Anatomy of an APT Attack: Step by Step Approach - Infosec Resources.” https://resources.infosecinstitute.com/topic/anatomy-of-an-apt-attack-step-by-step-approach/ (accessed Dec. 31, 2020).

[8] A. Ahmad, J. Webb, K. C. Desouza, and J. Boorman, “Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack,” Comput. Secur., vol. 86, pp. 402–418, 2019, doi: 10.1016/j.cose.2019.07.001.

[9] I. Ghafir et al., “Detection of advanced persistent threat using machine-learning correlation analysis,” Futur. Gener. Comput. Syst., vol. 89, pp. 349–359, 2018, doi: 10.1016/j.future.2018.06.055.

[10] I. Ghafir et al., “Detection of advanced persistent threat using machine-learning correlation analysis,” Futur. Gener. Comput. Syst., vol. 89, pp. 349–359, 2018, doi: 10.1016/j.future.2018.06.055.

[11] N. Virvilis and D. Gritzalis, “The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?,” 2013, doi: 10.1109/ARES.2013.32.

[12] S. Revathi and A. Malathi, “A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection.” Accessed: Nov. 12, 2020. [Online]. Available: www.ijert.org.

[13] Kaushik, Sapna S., and P. R. Deshmukh, "Detection of attacks in an intrusion detection system." International Journal of Computer Science and Information Technologies (IJCSIT), 2011.

[14] Ngiam, Jiquan, et al. "Multimodal deep learning." ICML, 2011.

[15] D. E. Holmes and L. C. Jain, “Introduction to Bayesian networks,” Studies in Computational Intelligence, vol. 156. Springer, Berlin, Heidelberg, pp. 1–5, 2008, doi: 10.1007/978-3-540-

85066-3_1.

[16] G. Meena and R. R. Choudhary, “A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA,” in 2017 International Conference on Computer, Communications and Electronics, COMPTELIX 2017, 2017, pp. 553–558, doi: 10.1109/COMPTELIX.2017.8004032.

[17] J. Mchugh, “Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory,” ACM Trans. Inf. Syst. Secur., vol. 3, no. 4, pp. 262–294, 2000, doi: 10.1145/382912.382923.

[18] L. Hakim, R. Fatma, and Novriandi, “Influence Analysis of Feature Selection to Network Intrusion Detection System Performance Using NSL-KDD Dataset,” in Proceedings - 2019 International Conference on Computer Science, Information Technology, and Electrical Engineering, ICOMITEE 2019, 2019, pp. 217–220, doi: 10.1109/ICOMITEE.2019.8920961.

[19] J. H. Joloudari, M. Haderbadi, A. Mashmool, M. Ghasemigol, S. S. Band, and A. Mosavi, “Early detection of the advanced persistent threat attack using performance analysis of deep learning,” IEEE Access, vol. 8, pp. 186125–186137, 2020, doi: 10.1109/ACCESS.2020.3029202.

[20] J. H. Joloudari et al., “Coronary artery disease diagnosis; ranking the significant features using a random trees model,” Int. J. Environ. Res. Public Health, vol. 17, no. 3, 2020, doi: 10.3390/ijerph17030731.

[21] Q. Zhu, X. Jiang, Q. Zhu, M. Pan, and T. He, “Graph Embedding Deep Learning Guides Microbial Biomarkers’ Identification,” Front. Genet., vol. 10, 2019, doi: 10.3389/fgene.2019.01182.

[22] Kumar, Vipin, Himadri Chauhan, and Dheeraj Panwar. "K-means clustering approach to analyze NSL-KDD intrusion detection dataset." International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2013.

[23] L. Dhanabal and S. P. Shantharajah, “A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms,” Int. J. Adv. Res. Comput. Commun. Eng., vol. 4, 2015, doi: 10.17148/IJARCCE.2015.4696.

[24] M. Längkvist, L. Karlsson, and A. Loutfi, “A review of unsupervised feature learning and deep learning for time-series modeling,” Pattern Recognit. Lett., vol. 42, no. 1, pp. 11–24, 2014, doi: 10.1016/j.patrec.2014.01.008.