ANALYSIS OF IOT BOTNETS USING MACHINE LEARNING TECHNIQUE

Raihana Syahirah Abdullah[1], Helwa Nabilah[1] , Nur Fadzilah Othman[1], Syarulnaziah Anawar[1] and Zakiah Ayop[1]

[1]Fakulti Teknologi Maklumat dan Komunikasi,
Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.

Corresponding Author's Email: [1]raihana.syahirah@utem.edu.my

Article History: Received 14 December 2021; Revised 20 February 2022; Accepted 12 May 2022

ABSTRACT: Internet of Things (IoT) botnets have been used to bring down some of the biggest services on the Internet. The spread of Internet of Things (IoT) botnets like those utilizing the Mirai malware was successful enough to the most powerful DDoS attacks. Particularly, behavioral-based approaches suffer from the unavailability of the benchmark datasets and this lead to lack of precise results evaluation of botnet detection systems, comparison, and deployment which originates from the deficiency of adequate datasets. This project used machine learning as an algorithms program that learn to collect data. There are various data mining tools available to analyze data related IoT botnets detection. However, the problem arises in deciding the most appropriate machine learning techniques or algorithm on particular tools to be implemented on IoT botnet data. This research is focusing only on classification techniques. Hence, the objective of this research is to identify the best machine learning technique or algorithm on selected tool for IoT botnets detection. Five techniques: Random Forest, J48, JRip, Naïve Bayes and BayesNet. are selected and applied in selected tools namely Weka. The expected output of this project is to provide the machine learning techniques for effective detection of IoT botnets flows that have high predictive accuracy. This result provides an option for the researcher on applying technique or algorithm on selected tool when analyzing IoT botnets data.

KEYWORDS: *IoT; IoT Botnets; Machine Learning; Data Mining; Weka*

1.0 INTRODUCTION

IoT of Things (IoT) known as the advance transformative that can possibly influence our lifestyles to be more convenient and also make our lives simpler. According to [1] stated that the IoT device means physical devices connect to Internet-based on traditional telecommunications with address could search and communicate each other. IoT devices represent a general concept for the ability of network devices to sense and collect data from the world around us, and then share that data across the Internet where it can be processed and utilized for various interesting purposes. The one particularly dangerous part of cybercrime is the threat forced by IoT botnet. Based on [2] report, total malware files discovered has been growing in year 2018. The number of malicious files detected daily reflects the average activity of cybercriminals involved in the creation and distribution of malware.

According to the Kaspersky Lab [3], the amount of malware targeting IoT devices more than doubled in 2020. Based on Kaspersky Lab report, The Top 10 regions by number of botnet C&C servers underwent some significant changes. Top spot went to the US with almost half of all C&C centers (44.75% against 29.32% in Q1). South Korea (11.05%) sank from first to second, losing nearly 20 p.p. China also dropped significantly (from 8.0% to 5.52%). Its place was taken by Italy, whose share climbed from 6.83% in the previous quarter to 8.84%. The Top 10 saw the departure of Hong Kong, but was joined for the first time since our records began by Vietnam, whose 3.31% was good enough for seventh place

In fact, the large number of uncertain devices with high computation power make them an easy and attractive target for attackers seeking to compromise these devices and use them to create large-scale IoT botnet by [4]. According to [5] stated that users are often unaware of their system being infected, as infected devices will stay idle until they receive commands from their commander to start an attack. IoT botnet is known as a set of hijacked Internet-connected devices and each of the devices will be affected by threats. Without the knowledge of the device's rightful owner, this process can allow an attacker to remote unsecured device. Based on Felix report describe that the data privacy leaks because of the security issues in IoT devices.

According to [6], the Mirai IoT botnet are not new. In order to form these attacks, the hackers have been using botnet by gaining access to unsecured IoT devices. The main purpose of IoT botnet attack is for spamming, identity theft, information stealing, reputation theft, botnet hosting services, click fraud, manipulating online polls and also attacking bank computers by [7].

2.0 RELATED WORK

2.1 Machine Learning

Machine learning was introduced in the late 1950's as a technique for artificial intelligence (AI) by [8]. Machine Learning is an algorithms program that learn to collect data. The different algorithms that exist to learn from multiple data by using the Machine Learning algorithm. According to [9], there are four types of machine learning techniques for IoT botnet detection. The Machine Learning classifier consists of RandomForest, J48, JRip, Naive Bayes and BayesNet. An explanation of the machine learning is given in the first place, then this project also provides an analysis of results obtained based on the accuracy and false alarm rate.

2.2 Classification Techniques

Classification techniques is data mining function that assign data in a collection to target categories or classes. The goal of classification is to accurately predict the target class for each case in the data. In data mining techniques, classification is one of the most popular techniques. There are seven classification techniques or algorithms: Naïve Bayes (NB), Bayesian Network (BN), Support Vector Machine (SVM), Random Forest (RF), Adaboost, K-Nearest Neighbour (KNN) and Neural Network (NN). However, in this research, only five classification techniques are applied which are Random Forest, J48, JRip, Naïve Bayes and BayesNet since it provides significant result for comparison.

Random Forest is a collection or ensemble of decision trees. Random forest builds multiple decision trees and merges them together to get a more accurate and stable prediction [10]. Random forests is an idea of the general technique of random decision forests that are an ensemble

learning technique for classification, regression and other tasks. [10] also stated that in a random forest, every node is split using the best among the subset of predicators randomly chosen at that node. Random Forests are considered general purpose vision tools and considered as efficient. Besides high prediction accuracy, Random Forest is efficient, interpretable and non-parametric for various types of datasets.

J48 algorithms are effective in that they provide human-readable rules of classification [9]. Based on [10], stated that J48 is a renowned, relatively simple classifier. It is a popular classifier since it is easy to interpret and explain. The decision is made based on whether a record of data belongs to a branch or not. A J48 is constructed from nodes which represent circles, and the branches are represented by the segments that connect the nodes. According to [9], J48 technique was the best at distinguishing between botnet and normal network traffic.

JRip is also a well-known algorithm for supervised data classification. It is a rule set is easy to understand and usually better than decision tree learners. In ripper classifiers training data is randomly distributed into growing set and pruning set. Classes are examined in increasing size and an initial set of rules for the class is generated using incremental reduced-error pruning by [9]. Each rule keeps on growing until no information gain is possible further. In JRip instances of the dataset are evaluated in increasing order, for given dataset of threat a set of rules are generated. JRip algorithm treats each dataset of given database and generates a set of rules including all the attributes of the class. Then next class will get evaluated and does the same process as previous class, this process continues until all the classes have been covered.

NaïveBayes algorithm is used also in machine learning systems to conclude the new data or testing data. According to [9][10], it is a simple probabilistic classifier based on the Bayes theorem with a strong features independence assumption. While this assumption is clearly false in most real-world tasks, naive Bayes often performs classification very well. Because of the independence assumption, the parameters for each attribute can be learned separately and this greatly simplifies learning, especially when the number of attributes is large. Naïve

Bayes models allow each attribute to contribute towards the final decision equally and independently from other attributes, in which it is more computational efficient when compared with other text classifiers. Thus, the present study focuses on employing Naïve Bayes approach as the text classifier for document classification and thus evaluates its classification performance against other classifiers.

Moreover, *Bayesian Network* classifiers are statistical classifiers as stated by [10]. BayesNet can predict class membership probabilities, such as probability that a given tuple belongs to a particular class. It uses various searching algorithms and quality measures based on BayesNet classifier and provide data structure. BayesNet is structured as a combination of a directed acyclic graph of nodes and links and a set of conditional probability tables. Nodes represent features or classes, while links between nodes represent the relationship between them. In BayesNet classifier conditional probability on each node is calculated first and then a Bayesian Network get formed by [11]. The assumption made in BayesNet is, that all attributes are nominal and there are no missing values any such value replaced globally. Moreover, in BayesNet, the output of can be visualized in terms of graph. The power of Bayesian networks as a representational tool stem from this ability to represent large probability distributions compactly. When user have a lot of missing data, BayesNet's can be very effective since modeling the joint distribution by [11].

2.3 Dataset

This research used two types of datasets. The datasets are selected from the VirusShare.com. Table 1 shows the decrypted file name, size of the file and the file type for the selected dataset. The malware samples originated from online sources which are virusshare.com and malwares.com. The malware that will be analyzed in this research is totally non malicious sample focus on IoT botnets. The features used in this dataset is five main duplets on network traffic focus on source IP, destination IP, source port, destination port and protocol. In this project, 9,890 malicious and 465 non-malicious data samples were used.

Table 1: Type of IoT Botnets

Sample	Filename	Size	File Type
Botnet I	VirusShare_7a5751f18c04777727a80d39d4687594d	1,279 KB	.exe
Botnet II	VirusShare_a3968d400aa1fcd833007f87f0c17e68	1,386 KB	.exe

2.4 Measurement Parameter

A confusion matrix is a summary of prediction results on a classification problem. The number of correct and incorrect predictions are summarized with count values and broken down by each class. According to [12][13], the confusion matrix has four categories: True positives (TP) are examples correctly labeled as positives. False positives (FP) refer to negative examples incorrectly labeled as positive. True negatives (TN) correspond to negatives correctly labeled as negative. Finally, false negatives (FN) refer to positive examples incorrectly labeled as negative.

Table 2: Classification Table [22]

Attack	Normal	
TN	FP	Attack
FN	TP	Normal

The measurement parameter used in this research are Accuracy, Detection Rate and False Alarm Rate. From the confusion matrix shown in Table 2, the following measurement are taken to calculate and use for the classifier.

i. Accuracy

According to [12], the classification accuracy metric is to evaluate the effectiveness of the considered features such as detection rate and false positive rate. The accuracy of an IoT botnet attack is measured regarding to detection rate and false alarm rate.

ii. Detection Rate

Refers to the percentage of detected attack among all attack data, and is defined as follows:

$$\text{Detection Rate} = TP/TP+FN \quad [12]$$

iii. False Alarm Rate (FAR)

False alarm rate (FAR): Refers to the percentage of normal data which is wrongly recognized as attack, and is defined as follows

$$FAR = FP/(FP+TN) \quad [12]$$

3.0 METHODOLOGY

The proposed design of experiment for this research is to show the structure of the botnet attack environment. The experiment diagram is shown in Figure 1. At first, download the malicious file from VirusShare.com has been download. Next, extract the file and the malicious file has been run by double clicking the file. The signature and behavior of the malicious file will be active in the Wireshark, a report will be produced.

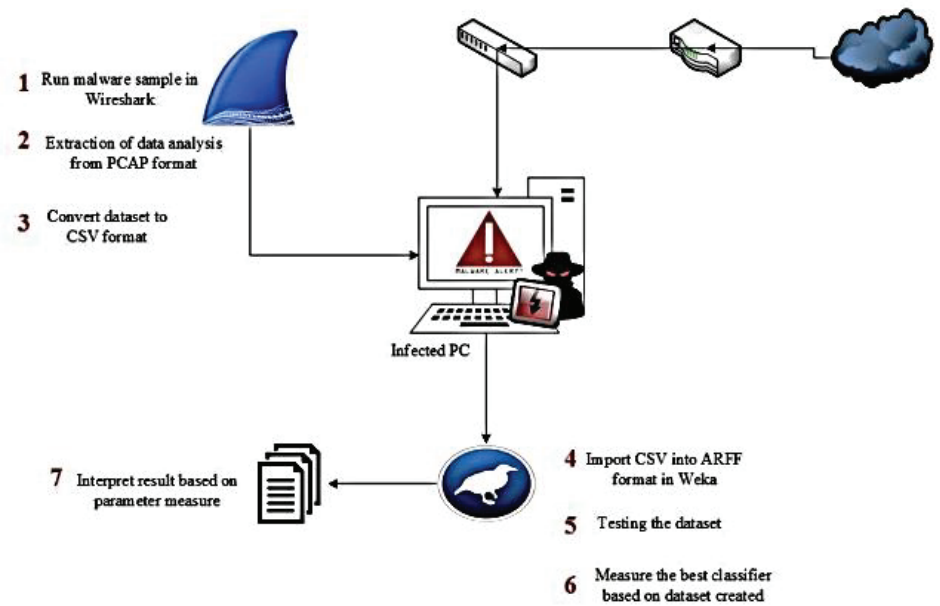

Figure 1: Flow Diagram for Machine Learning Classifier

This research focusing on Windows operating system and use Wireshark as packet analyzer. Before run the file, the downloaded malware file has decrypted from trusted website which is VirusShare.com. In this phase, Wireshark will identify the significant packet for behavior analysis that contains specified flags such as [SYN], [PSH ACK], [FIN ACK], [FIN PSH ACK].

Before the experiment started, the host must be set up to establish the botnet. This project consists of only one item, such as the personal computers (PCs) that installed with the Windows operating system. This project uses the website VirusShare.com that provide samples of

live malicious code. The use of sample bots, scripts or other methods to scrape data from the site, download samples at an excessive rate. When the computer communicates, either on the network or across the internet, they send bits of information called 'packets' to one another.

For this research, an experimental methodology has been used. After going through the deep analysis on IoT botnet's sample, few attributes that can have a great impact on it have been identified. These attributes are here referred as information variables. In this project, all the dataset has been gathered which is then filtered with the help of some dynamic analysis. The filtered data is then converted into the format used by Weka. After monitoring, RAW packet data were passed to sniffer server for calculation and statistics and then output the result into a CSV text file. Weka then analyzes these identified attributes along with the corresponding implementation. After the analysis of the attributes, the machine learning methodology works in the sequence as shown in Figure 2.

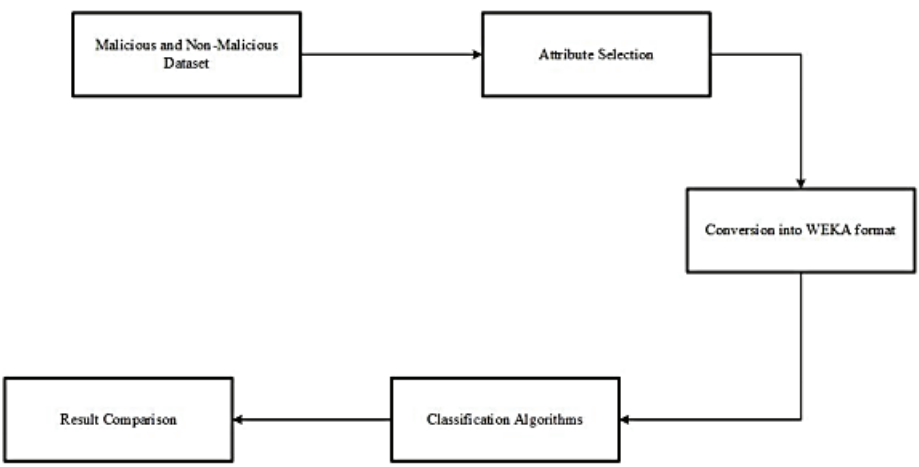

Figure 2: Machine Learning Methodology

For the detection method, Weka is a popular suite of machine learning software written in Java. According to [14] and [15], Weka operates on the predication that the user data is available as a flat file or relation, this means that each data object is described by a fixed number of attributes that usually are of a specific type, normal alpha-numeric or numeric values. Weka contains tools for data pre-processing, classification, regression, clustering, association rules and

visualization. Weka prefers to load data in the ARFF format. It is an extension of the CSV file format where a header is used that provides metadata about the data types in the columns. The training and testing data are already selected and kept in separate files. After loading both the training and testing file, the classifier and its parameters are chosen and the classification is carried out. The classifier is evaluated on how well it predicts the class of a set of instances loaded from a test file.

4.0 RESULT AND DISCUSSION

Figure 3 to Figure 5 respectively show the graph generated by selection data mining on Random Forest, J48, JRip, Naïve Bayes and BayesNet. The result encounter on measurement parameter as below:

4.1 Accuracy Result

The JRip classifiers of cross-validation produced accuracy value of 99.07%. However, the best result in this project was achieved with the Random Forest classifier of training set, with as much as 100%. It was discussed that the 10-fold validation usually produces enhanced results. In this study, the best result of the 10-fold validation is 99.07% while the best result of the training set method is 100%. Therefore, a comparison of accuracy concur that an improvement has been achieved in this research project through selecting the most suitable network traffic features as well as increasing the detection rate respectively.

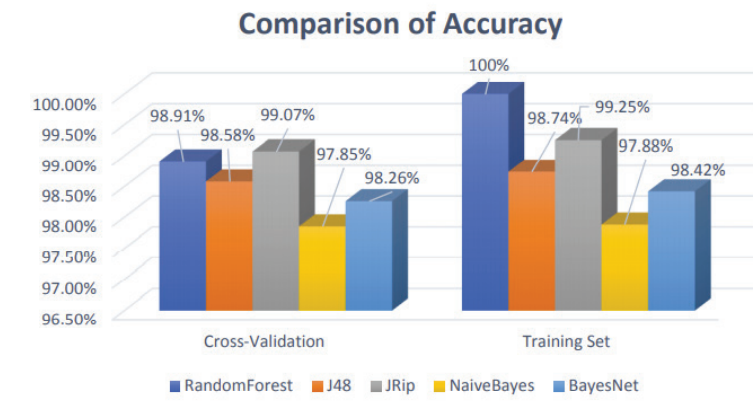

Figure 3: Accuracy Result

4.2 Detection Rate

The results are expressed in terms of performance measurements. Detection rate, also known as a true positive rate (TPR), is the probability of correctly detecting an instance as malware. The higher the Detection Rate, the better the result is. The results of detection rate for different types of attacks are shown in Figure 4. The JRip and Random Forest classifiers produced Detection Rate of 10.90% and 0% respectively. In this project, the best result of the 10-fold validation is 10.90% while the best result of the training set validation is 0%. The lower the value of detection rate, the more the effectiveness of the classifier.

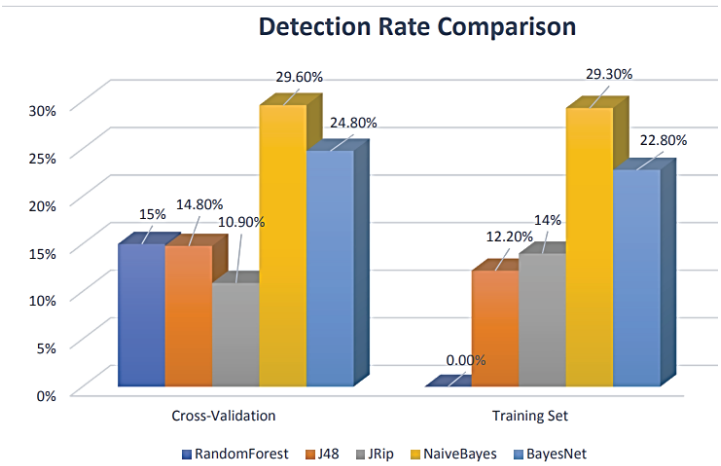

Figure 4: Detection Rate Result

4.3 False Alarm Rate

False alarm rate corresponds to the number of detected attacks but it is in fact normal. The test results are collected and averaged over all folds. This gives the cross-validation estimate of the accuracy. All the statistics results are provided in the figure below. A comparison of false alarm rate of all classifiers is done and finally it has been investigated that JRip technique performs best with lowest value false alarm rate 0.50%. The result from Figure 5 showed that the Random Forest classifier has the capabilities to predict 0% of false alarm rate of the IoT botnet attack. The improvement of overall detections in the signature-based module from classification table in data mining

module are indicated that this signature-based system technically effective for outcome attack detection. Therefore, it can be summarized that Random Forest is more effective classifier than JRip because it can predict 0% of dataset.

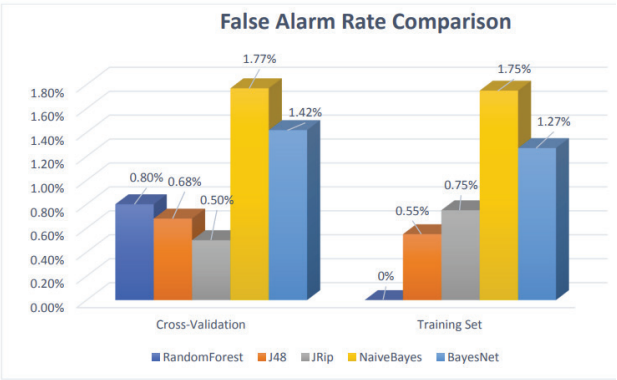

Figure 5: False Alarm Result

Referring to Figure 3 until Figure 5, in Weka tool, the best algorithm chosen is Random Forest and JRip. Hence, it shows that Random Forest and JRip is the best algorithm for Weka tool in IoT botnets data. Both algorithms manage to gain accuracy above 80%. This result provides an option for the researcher on applying technique or algorithm on selected tool when analyzing IoT botnets data. Besides, this research gives the contribution on identify specific IoT botnet attack and its behavior. In future, more machine learning tools and algorithm will be implemented on this dataset to identify the best algorithm or techniques to be used.

5.0 CONCLUSION

In conclusion, this research help user studies the IoT botnet attack by using machine learning classifiers. Besides, this research gives the contribution on identify specific IoT botnet attack and its behavior. In addition, the comparison between the classifiers has been made to improve the time used to train and general the machine learning, as proven in the experiment section. This research also gives contribution on how the machine learning can be used as simple as detection method in the real environment.

proven in the experiment section. This research also gives contribution on how the machine learning can be used as simple as detection method in the real environment.

ACKNOWLEDGMENTS

The authors would like to thank the Information Security Forensics and Computer Networking (INSFORNET), Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka.

REFERENCES

[1] Cyber Security Malaysia, "Trend Report", 130, pp. 28–31, 2017. http://www.cybersecurity.my/data/content_files/13/1713.pdf.

[2] "Malware Trend Report Q4 2015", pp. 1–14, (2017). https://www.redsocks.eu/wpcontent/uploads/2015/12/RedSocks_Malware_Trend_Report_Q4-2015_FINAL.pdf.

[3] Spamhaus Malware Labs, (2018). Available: https://www.spamhaus.org/news/article/772/spamhaus-botnet-threat-report-2017.

[4] S. Shahaboddin et al., "A Study of Machine Learning Classifiers for AnomalyBased Mobile Botnet Detection", vol. 26, no. 4, pp 251-265, 2018.

[5] N. Hoque, D.K. Bhattacharyya, and J.K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges", vol. 17, no. 4, pp. 2242–2270, 2015.

[6] D. Antonioli, G. Bernieri, and N.O. Tippenhauer, 'Taking Control: Design and Implementation of Botnets for Cyber-Physical Attacks with CPSBot", 2018.

[7] Y. Ohsita, "Detecting Distributed Denial-of-Service Attacks by analyzing TCP SYN packets statistically", pp. 2043–2049, 2004.

[8] S. Garg et al., "Behaviour analysis of machine learning algorithms for detecting P2P botnets", 15th International Conference on Advanced Computing Technologies (ICACT), 2017, pp. 1–4.

[9] W. Shahzad, S. Asad and M.A. Khan, "Feature subset selection using association rule mining and JRip classifier", vol. 8, no. 18, pp. 885–896, 2013. doi: 10.5897/IJPS2013.3842.

[10] A.K. Mishra, and B.K. Ratha, "Study of Random Tree and Random Forest Data Mining Algorithms for Microarray Data Analysis", pp. 5–7, 2018.

[11] F. V. Alejandre, N. C. Cortes and E. A.Anaya, "Feature selection to detect botnets using machine learning algorithms", 2017 International Conference on Electronics, Communications and Computers (CONIELECOMP), pp. 1–7, 2017.

[12] E. B. Beigi, "Towards effective feature selection in machine learning-based botnet detection approaches", 2014 IEEE Conference on Communications and Network Security, CNS 2014, pp. 247–255, 2014.

[13] F. Haddadi, "Botnet behaviour analysis using IP flows: With http filters using classifiers", Proceedings - 2014 IEEE 28th International Conference on Advanced Information Networking and Applications Workshops, IEEE WAINA 2014, 2014, pp. 7–12.

[14] N. C. Cortes and E. A. Anaya, "Feature selection to detect botnets using machine learning algorithms", 2017 International Conference on Electronics, Communications and Computers (CONIELECOMP), 2017, pp. 1–7.

[15] D. C. Le, A. N. Zincir-Heywood and M. I. Heywood, "Data analytics on network traffic flows for botnet behaviour detection", 2016 IEEE Symposium Series on Computational Intelligence, 2016.