http://dx.doi.org/10.21172/ijiet.143.16

Classification Algorithm Against Different Types of DDoS Attacks Using Hybrid Approach

Mohd Azahari Mohd Yusof[1], Fakariah Hani Mohd Ali[2], Mohamad Yusof Darus[3]
[1] *Faculty of Computing and Multimedia, Kolej Universiti Poly-Tech MARA Kuala Lumpur, Malaysia*
[2,3] *Faculty of Computer & Mathematical Sciences, Universiti Teknologi MARA Shah Alam, Malaysia*

Abstract– We know that today's security tools are still ineffective to detect the type of DDoS attack based on the behavior of incoming packets whether it's normal traffic or DDoS attack. When an attacker launches a DDoS attack, it will result in the target server being interrupted and inaccessible at that time even though we are legitimate users. In this paper, we propose a technique called Packet Threshold Algorithm (PTA) combined with some machine learning algorithms. This combined technique aims to detect incoming packets entering the network environment by classifying whether it is normal traffic or DDoS attack. The technique has been implemented, and it can improve the accuracy of detection while reducing the problem of false positive rate.
Keywords– Distributed Denial of Service (DDoS), Packet Threshold Algorithm (PTA), machine learning, false positive rate.

I. INTRODUCTION

The computer network is a very important communication tool because it offers many advantages and one such is as resource sharing. Computer networks are formed based on a combination of two or more computers to allow users to exchange information. The combination of computer networks with other computer networks formed a technology called the Internet. According to [1], the existence of the Internet brings many advantages such as online games, where it allows users to connect with each other in different places. Also, the internet allows users to communicate through Facebook, Twitter and Instagram, where they are today's most popular social media. Most importantly, the Internet is considered as a highly effective and preferred communication platform as it can be accessed 24 hours a day from everywhere. However, day to day the computer network or the Internet has experienced threats such as DDoS attacks [2].

Based on [3], the computer network was inaccessible at the time it was attacked by DDoS even though they were legitimate users. Typically, the DDoS attack launched by an attacker uses botnet to produce a quick and powerful attack to weaken the target server [4]. There are three categories of DDoS attacks that exist in the world, they are a volume-based attack, protocol attack and application layer attack [5]. The volume-based attack is launched to suppress the server bandwidth under attack so that the server could not handle all requests. The categories of this attack include UDP flood and ICMP flood. Protocol attack is launched to charge servers with excessive use of resources so that the server was unable to respond to every request. The categories of this attack include TCP SYN flood, Ping of Death and Smurf. Finally, application layer attack is launched to disable the target server by botnet, which sends a large request to applications such as databases. The categories of this attack include Slowloris and Zero-day attack.

This paper expresses its primary contribution through the establishment of the DDoS classification algorithm to detect incoming packets, classifying them either normal traffic or DDoS traffic based on the packet threshold that has been set in PTA combined with several machine learning algorithms. Today, DDoS attacks are one of the most popular network or Internet threats that motivate us to design the DDoS classification algorithm. DDoS attacks consist of several types (Holmes, 2016) and only four types of DDoS attacks are discussed on this paper, which are TCP SYN flood, UDP flood, Ping of Death and Smurf traffic. According to [6], the four types of attacks are the top network threat today and the most popular is launched by attackers all over the world. Moreover, the four types of DDoS attacks are very easy to generate because their attack structure is simple, but hard to defend according to [7] and [8]. Apart from that, [9] have said the false positive rate is still unending, where normal traffic incorrectly specified as a DDoS attack. The false positive problem will negatively affect the accuracy of incoming traffic detection.

This paper is structured into several sections. The types of DDoS attacks are described in section II, while in section III, we reviewed some related works. The methodology and evaluation are explained in section IV. The results and discussion are in section V and section VI concludes the paper.

II. TYPES OF DDOS ATTACKS

We know that successful DDoS attacks launched by attackers will cause the network resources to be inaccessible to anyone at that time [10]. There are several types of DDoS attacks that can be generated by the attacker as described in the following subsection.

2.1 UDP Flood

According to [11], UDP flood occurs when the target server receives a lot of UDP packets consistently. This will result in the target server unable to entertain all requests at that time. This type of attack can result in a firewall that protects the target server from working properly. This happens because the firewall paves the way for flooding with the UDP packet continuously without stopping.

2.2 TCP SYN Flood

TCP SYN flood occurs when an attacker generates and sends too many TCP SYN requests to the target server consistently [12]. In the event of this type of attack, the target server could not handle all requests even the user is a legitimate user. Typically, a normal TCP connection involves a three-way handshake, where it involves three standard steps to establish a connection. However, normal TCP connection switches to TCP SYN flood if the target server is flooded with a SYN packet repeatedly without restriction.

2.3 ICMP Flood

ICMP flood occurs when an attacker strikes the target server with ICMP echo or ping [13]. It is also known as ping flood. Typically, attackers use some tools such as hping3 and scapy to generate custom ICMP packets to undermine the target server continuously.

2.4 Smurf

The attacker launched a Smurf attack by generating and sending a large number of ICMP packets to the target server [14]. Typically, this type of attack is done through several steps. It starts with the identification of the target server IP address by the attacker, where the ICMP packet will be sent using broadcast to the network of the target server.

2.5 Ping of Death

This type of attack occurs when the target server receives an ICMP packet of more than 65,535 bytes per second from the attacker [15]. This type of attack could crash, destabilize or freeze the target server by simply generating a simple ping command.

2.6 Slowloris

Slowloris is a DDoS attack software developed by Robert Hansen. The use of Slowloris by an attacker allows a single computer to take down a target server. The obvious advantage of Slowloris is that it can open many connections to the target server, where all connections will always be open. This situation allows the attacker to send a large number of partial HTTP packets consistently.

2.7 Zero-day Attack

Attackers use this type of attack to exploit a vulnerability in hardware or software so that it could not be fixed. Usually, this happens before the vendor realizes there is a problem with the software or hardware. The main purpose of this type of attack is not to provide space for vendors to make improvements to hardware or software which has a problem as complained by the user.

III. RELATED WORK

Attackers will disrupt the target server at any time by generating DDoS attacks. However, there are some solutions that have been designed by previous researchers to reduce the problem of DDoS attacks. This is presented in Table 1.

Multi-Queue Algorithm is a solution that has been proposed by [16] to detect TCP SYN flood and UDP flood. This algorithm is equipped with two techniques called drop tail congestion control algorithm and random early detection algorithm. These algorithms can increase network throughput even though the network environment is being attacked by DDoS. However, these algorithms still could not reach the best level of detection because it does not classify incoming traffic either normal traffic or DDoS traffic.

Cumulative Sum Algorithm has been proposed by [17] to detect the UDP flood. There are two states that fall into this algorithm, they are Not Under Attack (NA) and Attack (A) and include two main functions named DDoS and

ipac. The DDoS function is to determine whether incoming traffic is A or NA. Meanwhile, ipac works to determine the IP address that is captured, whether they are a new IP address or IP address that has been logged. Unfortunately, this algorithm has weaknesses such as high false positive rates as most new IP addresses are always detected as DDoS traffic. Apart from that, both functions, ipac and DDoS take a long time to classify incoming traffic based on normal traffic or DDoS traffic.

The solution proposed by [9] is known as Dynamic Security Level Changing Strategy Algorithm used to detect TCP SYN flood, where it is installed in the server node. This algorithm is loaded into the server to reduce the problem of DDoS attacks against neighboring nodes being attacked. It is also able to classify incoming traffic either normal traffic or DDoS traffic. However, a high false positive rate is the most obvious drawback of this algorithm because of the inaccurate traffic being detected as DDoS traffic and indirectly, it has a very serious impact on the accuracy of detection.

SVM algorithm proposed by [18], works to detect DDoS attacks using the SVM algorithm. They have applied DARPA datasets to classify the form of traffic coming into the network. Also, they have made comparisons with some other machine learning algorithms such as Naive Bayes, Decision Tree and Random Forest. They found that the SVM algorithm gave better results compared to the other algorithms because SVM has produced higher detection accuracy and reduced the false positive rate. Unfortunately, this algorithm could not protect target servers if attackers generate DDoS attacks using actual IP addresses.

A solution called Worldwide SYN Flooding Attack Detection Algorithm works to detect TCP SYN flood has been proposed by [19]. Researchers have introduced eight attack scenarios in their studies with 14 types of SYN flood attacks to determine the strength of their algorithm. The strength of their algorithm can only detect 80 DDoS traffic from 307 incidents and this shows that the algorithm does not succeed in obtaining high detection accuracy.

Modified K-Means Algorithm proposed by [20] is a solution for detecting DDoS traffic based on DARPA datasets. They have loaded a method known as chain initialization over landmark window to process incoming traffic. They have handled a comparison of this altered algorithm with some other algorithms to look at the accuracy of detection and false positive rate. They found that this algorithm needs to be improved to reduce the false positive rate and improve the accuracy of incoming traffic detection.

Hop-Count Filter is a solution that has been proposed by [21] to classify incoming traffic as normal traffic or DDoS traffic. They have set traffic thresholds to detect incoming traffic. If the number of incoming traffic exceeds the number of traffic thresholds, then it is DDoS traffic. Unfortunately, the solution only achieves 93.3% of the detection accuracy and indirectly shows a high false positive rate.

Then, [22] have proposed Density-Based Spatial Clustering and Application with Noise to classify incoming traffic as normal traffic or DDoS traffic. The incoming traffic classification is based on DARPA dataset and uses the entropy method and found that the solution reaches 98.9% detection accuracy after comparison with other methods such as K-Means. If seen on detection accuracy results, it shows that there is still a high false positive rate.

Based on the explanation of some of the solutions shown in Table 1, we found that false positive rate problems still could not be reduced and it affects the percentage of detection accuracy. Apart from that, there is some solution proposed by [18], [21] and [22] which have not detected the DDoS attacks based on the type of attack, either Smurf, TCP SYN flood, Ping of Death, UDP flood or ICMP flood.

Table - 1 The Existing Solution for Detecting DDoS Attacks

Previous Solution	Type of DDoS attack detected									
	TCP SYN Flood	UDP Flood	ICMP / Ping Flood	Ping of Death	Smurf	Slowloris	HTTP Flood	Zero-day Attack	SIDDoS	Not Available
Multi-Queue Algorithm	✓	✘	✘	✘	✘	✘	✘	✘	✘	✘
Cumulative Sum Algorithm	✓	✓	✘	✘	✘	✘	✘	✘	✘	✘
Dynamic Security Level Changing Strategy Algorithm	✓	✘	✘	✘	✘	✘	✘	✘	✘	✘
Support Vector Machine	✘	✘	✘	✘	✘	✘	✘	✘	✘	✓
Worldwide SYN Flooding Attack Detection Algorithm	✓	✘	✘	✘	✘	✘	✘	✘	✘	✘
Modified K-Means Algorithm	✘	✘	✘	✘	✓	✘	✘	✘	✘	✘

Hop-Count Filter	✘	✘	✘	✘	✘	✘	✘	✘	✘	✓
Density-Based Spatial Clustering and Application with Noise	✘	✘	✘	✘	✘	✘	✘	✘	✘	✓

IV. METHODOLOGY AND EVALUATION

In this section, we describe the research methodology used to support this study. Our study is based on four important phases as presented in Figure 1.

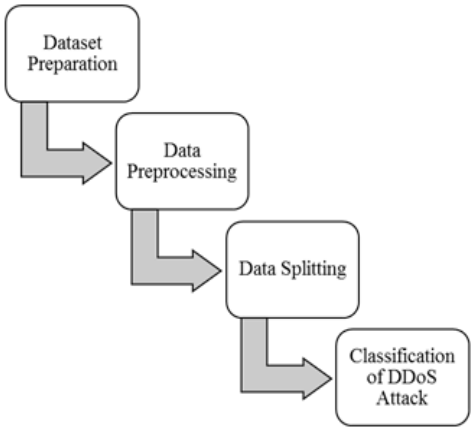

Figure 1 Research Methodology

4.1 Dataset Preparation

The dataset preparation is the first phase of our study, where the dataset contains traffic information that goes into the network environment. This dataset is an open source dataset that has been captured and recorded by [23], as presented in Table 2. This dataset is most appropriate for our study because the information recorded is related to normal traffic and DDoS traffic.

Although there are some datasets that can be attributed to DDoS attacks like KDD Cup 99 and CAIDA, the datasets used in our studies are more realistic and effective. Most important, this dataset is in line with our study as it provides four types of DDoS attacks that we focus on and they are TCP SYN flood, UDP flood, Ping of Death and Smurf. For example, TCP SYN flood occurs when the target server receives multiple SYN packets consistently to make the target server unable to handle any requests [24].

Table - 2 Sample Dataset

Src_Addr	Dst_Addr	Pkt_Type	Pkt_Size	…	Pkt_Class
10.0.34.87	10.0.34.70	TCP	55	…	Normal
10.0.34.70	10.0.34.87	ICMP	65535	…	Ping of Death
10.0.34.87	10.0.34.70	ICMP	1540	…	Smurf
10.0.34.70	10.0.34.87	UDP	1192	…	UDP Flood
10.0.34.70	10.0.34.87	TCP	50310	…	TCP SYN Flood

4.2 Data Preprocessing

Our study is continued with the second phase known as data preprocessing. This phase involves data cleaning and data reduction, where data cleaning is done to ensure data is consistent, correct and has no errors. Meanwhile, data reduction is carried out to reduce the size of the data to a small amount but still contains important information. Both of these methods are implemented because we are aware that the data was originally incomplete, noisy, inconsistent and it came from a variety of sources. Hence, data preprocessing is very important in our study to ensure data is correct, complete and consistent.

4.3 Data Splitting

The third phase of our study is data splitting. The data is separated into two sets. They are the training set and the testing set, this is done since this dataset consists of 240,000 samples and 27 features. Training set and testing set is very important in our study, where data from the training set is used to fit the machine learning algorithm. Meanwhile, the data from the testing set is the data used to avoid bias towards the implementation of the algorithm.
We apply the train_test_split function to build the data splitting. Data splitting into the training set and testing set is based on train_size = 0.8 and test_size = 0.2 functions, where the percentage of training sets is 80% and 20% for the testing set. Based on most researchers, data splitting between the training set and testing set with a percentage of 80% and 20% respectively is a suitable method as the dataset we used in this study contain a lot of data.

4.4 Classification of DDoS Attack

The final phase of our study is the classification of DDoS attack. This phase is completed using PTA, which has been designed and combined with several machine learning algorithms such as K-Nearest Neighbor, Naïve Bayes, Support Vector Machine and Logistic Regression as shown in Figure 2.
This algorithm checks the presence of incoming traffic to the server. If the packet size detected less than 60 packets per second and the packet type is TCP, UDP or ICMP, this algorithm will classify incoming packets as a normal packet. If the packet size detected is 60 or more SYN packets per second and the packet type is TCP, this algorithm will classify the incoming packet as a TCP SYN flood. If the packet size detected is 60 or more UDP packets per second and packet type is UDP, this algorithm will classify the incoming packet as a UDP flood. If the packet size detected is 65,535 or more ICMP packets per second and the packet type is ICMP, this algorithm will classify incoming packets as a Ping of Death. If the packet size detected is 60 and less than 65,535 ICMP packets per second and the packet type is ICMP, this algorithm will classify incoming packets as a Smurf.

Start

Check incoming packets

if (Pkt_Size < 60) and (Pkt_Type = TCP) or (Pkt_Type = UDP) or (Pkt_Type = ICMP) then
Pkt_Class = Normal
Action: Pass packet

Else
if (Pkt_Size ≥ 60) and (Pkt_Type = TCP) then
Pkt_Class = TCP SYN flood
Action: Drop packet

Else
if (Pkt_Size ≥ 60) and (Pkt_Type = UDP) then
Pkt_Class = UDP flood
Action: Drop packet

Else
if (Pkt_Size ≥ 65,535) and (Pkt_Type = ICMP) then
Pkt_Class = Ping of Death
Action: Drop packet

Else
if (Pkt_Size ≥ 60 and Pkt_Size < 65,535) and (Pkt_Type = ICMP) then
Pkt_Class = Smurf
Action: Drop packet

End

Packet Threshold Algorithm (PTA)

Our algorithm is assessed based on the performance metric as presented in Table 3.

Table - 3 Description of Performance Metric

Performance Metric	Description	Equation
TP Rate	DDoS packet correctly detected as DDoS packet.	$TPR = \frac{TP}{TP + FN} \times 100$
FP Rate	Normal packet incorrectly detected as DDoS packet or DDoS packet incorrectly detected as DDoS	$FPR = \frac{FP}{FP + TN} \times 100$

	packet itself.	
FN Rate	DDoS packet incorrectly detected as normal packet.	$FNR = \frac{FN}{FN + FP} \times 100$
TN Rate	Normal packet correctly detected as normal packet.	$TNR = \frac{TN}{TN + FP} \times 100$
Detection Accuracy	The percentage of packets detected is correct.	$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \times 100$
Precision	The proportion of the predicted positive cases that were correct.	$Precision = \frac{TP}{TP + FP} \times 100$
Recall	The number of correct positive predictions divided by the total number of positives.	$Recall = \frac{TP}{TP + FN} \times 100$
F1-Score	A harmonic mean of precision and recall.	$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$

V. RESULTS AND DISCUSSION

This section presents the results obtained after we conducted the evaluation to evaluate the techniques involved in this study. Based on Table 4, it shows the number of correctly detected packets for PTA-KNN is 47,829 packets and 171 misclassified packets. Meanwhile, PTA-NB has acquired 47,664 correctly detected packets with 336 misclassified packets, 47,818 correctly detected packets with 182 misclassified packets for PTA-SVM and 47,568 correctly detected packets with 432 misclassified packets for PTA-LR. Two types of accuracy can be used to assess the performance of a technique or model. They are training accuracy and testing accuracy [25]. In our study, it only displays data from test results based on testing accuracy, where it involves a 20% testing set as described in the methodology and evaluation section.

Table - 4 Performance Comparison Between the Techniques Involved

Technique	Packet Class	Correctly Detected Packets	Misclassified Packets
PTA-KNN	Normal	42,876	40
	Ping of Death	133	4
	Smurf	338	74
	TCP SYN flood	88	38
	UDP flood	4,394	15
PTA-NB	Normal	42,916	0
	Ping of Death	133	4
	Smurf	298	114
	TCP SYN flood	87	39
	UDP flood	4,230	179
PTA-SVM	Normal	42,880	36
	Ping of Death	133	4
	Smurf	329	83
	TCP SYN flood	86	40
	UDP flood	4,390	19
PTA-LR	Normal	42,893	23
	Ping of Death	132	5
	Smurf	112	300
	TCP SYN flood	87	39
	UDP flood	4,344	65

When looking at detection accuracy, it shows that PTA-KNN has gained 99.64% followed by 0.10% FP rate, 97.50% TP rate, 99.90% TN rate, 2.50% FN rate, 99.63% precision and 99.64% recall and f1-score. Detection accuracy for PTA-NB is 99.30% with 0.39% FP rate, 96.60% TP rate, 99.61% TN rate, 3.40% FN rate, 99.34% precision, 99.30% recall and 99.32% f1-score. PTA-SVM has reached 99.62% detection accuracy with 0.13% FP rate, 97.47% TP rate, 99.87% TN rate, 2.53% FN rate, 99.62% recall and 99.61% precision and f1-score. Meanwhile, PTA-LR has achieved 99.10% detection accuracy with 0.57% FP rate, 96.17% TP rate, 99.43% TN rate, 3.83% FN rate, 98.98% precision, 99.10% recall and 99.04% f1-score. Based on the performance comparison presented in Table 4, PTA-KNN can be considered as a highly relevant technique for classifying incoming traffic either normal traffic or DDoS attacks.

VI. CONCLUSION

An algorithm named PTA has been introduced where we have combined the algorithm with four machine learning algorithms. This merging algorithm aims to detect incoming traffic based on normal traffic or DDoS attacks. DDoS attacks that were given focus this study are TCP SYN flood, UDP flood, Ping of Death and Smurf. Based on the analysis made on the testing of all the techniques involved in our study, it is found that PTA-KNN is the most appropriate technique for detecting traffic entering the network environment.

VII. ACKNOWLEDGEMENT

This research is supported by the Research Management Institute, Universiti Teknologi MARA and the Ministry of Higher Education and registered under the #600-IRMI/FRGS 5/3 (017/2017).

VIII. REFERENCE

[1] Y. Sun and I. Davidson, “Influential Factors of Online Fraud Occurrence in Retailing Banking Sectors from a Global Prospective: An Empirical Study of Individual Customers in the UK and China,” Information & Computer Security, vol. 23, no. 1, pp. 3–19, 2015.
[2] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, “Anatomy of Threats to The Internet of Things,” IEEE Communications Surveys & Tutorials, pp. 1–50, 2018.
[3] A. Serrano Mamolar, Z. Pervez, J. M. Alcaraz Calero, and A. M. Khattak, “Towards the Transversal Detection of DDoS Network Attacks in 5G Multi-tenant Overlay Networks,” Computers & Security, vol. 79, pp. 132–147, 2018.
[4] M. S. Gadelrab, M. Elsheikh, M. A. Ghoneim, and M. Rashwan, “BotCap: Machine Learning Approach for Botnet Detection Based on Statistical Features,” International Journal of Communication Networks and Information Security (IJCNIS), vol. 10, no. 3, pp. 563–579, 2018.
[5] Imperva, “The Top 10 DDoS Attack Trends,” White Paper, p. 14, 2015.
[6] A. Bonguet and M. Bellaiche, “A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing,” Future Internet, vol. 9, no. 43, pp. 1–19, 2017.
[7] Neustar, “Neustar Annual DDoS Attacks and Impact,” 2014.
[8] S. Sivabalan and P. J. Radcliffe, “A Novel Framework to Detect and Block DDoS Attack at the Application Layer,” in IEEE Tencon - Spring, 2013, pp. 578–582.
[9] S. H. Lim and J. H. Kim, “Dynamic Security Level Changing Strategy using Attack Predictions: Case Study of TCP SYN Attacks,” in International Conference on IT Convergence and Security (ICITCS), 2014, pp. 1–4.
[10] R. C. Baishya, N. Hoque, and D. K. Bhattacharyya, “DDoS Attack Detection Using Unique Source IP Deviation,” International Journal of Network Security, vol. 19, no. 6, pp. 929–939, 2017.
[11] S. S. Kolahi, K. Treseangrat, and B. Sarrafpour, “Analysis of UDP DDoS Flood Cyber Attack and Defense Mechanisms on Web Server with Linux Ubuntu 13,” in International Conference on Communications, Signal Processing, and Their Applications (ICCSPA), 2015, pp. 1–5.
[12] H. S. Salunkhe, P. S. Jadhav, and P. V. Bhosale, “Analysis and Review of TCP SYN Flood Attack on Network with Its Detection and Performance Metrics,” International Journal of Engineering Research & Technology (IJERT), vol. 6, no. 1, pp. 250–256, 2017.
[13] Harshita and R. Nayyar, “Detection of ICMP Flood DDoS Attack,” International Journal of Computer Science Trends and Technology (IJCST), vol. 5, no. 2, pp. 199–205, 2017.
[14] N. Priyanka and V. Vetriselvi, “Detection of Smurf Attack in SDN with Multiple Controllers,” in International Conference on Electrical, Information and Communication Technology, 2016, pp. 91–94.
[15] F. Yihunie, E. Abdelfattah, and A. Odeh, “Analysis of Ping of Death DoS and DDoS Attacks,” in IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2018, pp. 3–6.
[16] F. Nkemneme and R. Wei, “A Multi-Queue Algorithm for DDoS Attacks,” in IEEE 18th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2014, pp. 118–123.
[17] E. Ahmed, G. Mohay, A. Tickle, and S. Bhatia, “Use of IP Addresses for High Rate Flooding Attack Detection,” in IFIP Advances in Information and Communication Technology, 2014, pp. 1–13.
[18] K. RT, S. T. Selvi, and K. Govindarajan, “DDoS Detection and Analysis in SDN-Based Environment Using Support Vector Machine Classifier,” in 6th International Conference on Advanced Computing (ICoAC), 2014, pp. 205–210.
[19] L. Miao, W. Ding, and J. Gong, “A Real-Time Method for Detecting Internet-Wide SYN Flooding Attacks,” in IEEE International Workshop on Local and Metropolitan Area Networks, 2015, pp. 1–6.
[20] M. I. W. Pramana, Y. Purwanto, and F. Y. Suratman, “DDoS Detection Using Modified K-Means Clustering with Chain Initialization Over Landmark Window,” in International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), 2015, pp. 7–11.

[21] C. Li, J. Yang, Z. Wang, F. Li, and Y. Yang, "A Lightweight DDoS Flooding Attack Detection Algorithm Based on Synchronous Long Flows," in IEEE Global Communications Conference (GLOBECOM), 2015, pp. 1–6.
[22] S. O. Al-Mamory and Z. M. Algelal, "A Modified DBSCAN Clustering Algorithm for Proactive Detection of DDoS Attacks," in Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), 2017, pp. 304–309.
[23] M. Alkasassbeh, G. Al-Naymat, A. B.A, and M. Almseidin, "Detecting Distributed Denial of Service Attacks Using Data Mining Techniques," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 7, no. 1, pp. 436–445, 2016.
[24] R. K. Deka, D. K. Bhattacharyya, and J. K. Kalita, "Granger Causality in TCP Flooding Attack," International Journal of Network Security, vol. 21, no. 1, pp. 30–39, 2019.
[25] Q. Wei and R. L. Dunbrack, "The Role of Balanced Training and Testing Data Sets for Binary Classifiers in Bioinformatics," Plos One, vol. 8, no. 7, pp. 1–12, 2013.