Available online to ejournal.pnc.ac.id

Journal of Innovation Information Technology and Application

Journal Page is available to https://ejournal.pnc.ac.id/index.php/jinita

A Classification Data Packets using the Threshold Method for Detection of DDoS

Sukma Aji [1],Davito Rasendriya [2] ,Imam Riadi [3],Abdul Fadlil [4] ,Muhammad Nur Faiz [5] ,Arif Wirawan Muhammad [6],Santi Purwaningrum [7],Laura Sari [8]

[1] *Lecturer of Informatic, Universitas Muhammadiyah Sidoarjo, Sidoarjo, East Java*
[2] *School of Informatic, Universitas Muhammadiyah Sidoarjo, Sidoarjo, East Java*
[3] *Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[4] *Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[5,7,8] *Department of Computer and Business, Politeknik Negeri Cilacap, Cilacap, Indonesia*
[6] *Department of Informatics, IT Telkom Purwokerto, Jawa Tengah, Indonesia*

:[1] sukmaaji@umsida.ac.id, [2] 201080200009@mhs.umsida.ac.id, [3] fadlil@mti.uad.ac.id, [4] imam.riadi@is.uad.ac.id, [5] faiz@pnc.ac.id, [6] arif@ittelkom-pwt.ac.id, [7] santi.purwaningrum@pnc.ac.id, , [8] laurasari@pnc.ac.id

ARTICLE INFO

Article history:
Received 26 January 2024
Revised 31 January 2024
Accepted 11 Juny 2024
Available 28 Juny 2024

Keywords:
Ddos
Data Packages
Classsification
Threshold
Numeric Attribute

IEEE style in citing this article:
S. Aji , D. Rasendriya, I. Riadi , A. Fadlil, and M. Nur Faiz, "Classification Data Packets Using the Threshold Method for Detection of DDoS," Journal of Innovation Information Technology and Application (JINITA), vol. 6, no. 1, pp. 30–39, Jun. 2024, doi: https://doi.org/doi.org/10.35970/jinita.v6i1.2224.

ABSTRACT

Computer communication is done by first synchronizing one computer with another computer. This synchronization contains Data Packages which can be detrimental if done continuously, it will be categorized as an attack. This type of attack, when performed against a target by many computers, is called a distributed denial of service (DDoS) attack. Technology and the Internet are growing rapidly, so many DDoS attack applications result in these attacks still being a serious threat. This research aims to apply the Threshold method in detecting DDoS attacks. The Threshold method is used to process numeric attributes so obtained from the logfile in a computer network so that data packages can be classified into 2, namely normal access and attack access. Classification results using the Threshold method after going through the fitting process, namely detecting 8 IP Addresses as computer network users and 6 IP addresses as perpetrators of DDoS attacks with optimal accuracy.

1. INTRODUCTION

The world of internet and network-based applications have now become an inseparable It's part of our daily life. Three important aspects of network security include integrity, confidentiality and availability [1]. Distributed Denial of Service (DDoS) attacks are the biggest threat to availability [2]. The attack also involves spoofing the source IP address to hide the attacker's identity, making it extremely difficult to track [3] . International service site Hackmageddon [4] reports cyber attack statistics in Quarter 2 (Q2) 2023 as follows: Malware 33%; Unknown 20.5%; Vulnerability 16.3%; Account Takeover 9.3%; Targeted Attack 7.5%; DDoS 4.6%; Coordinate Inauthentic Behavior 3.3%; and the rest is a Scam; Misconfiguration; Malicious Script Injection; Business Email Compromise; >1; SQLi; Defacement; Brute force; Malicious Chrome Extension; Credential stuffing; Flash Loans; N/A; Malvertising; Password-spray; Malverposting; Sextortion; Rug pull; Modified cold hardware; Mev bot attack which can be seen in Figure 1.

**) Corresponding Author : sukmaaji@umsida.ac.id*

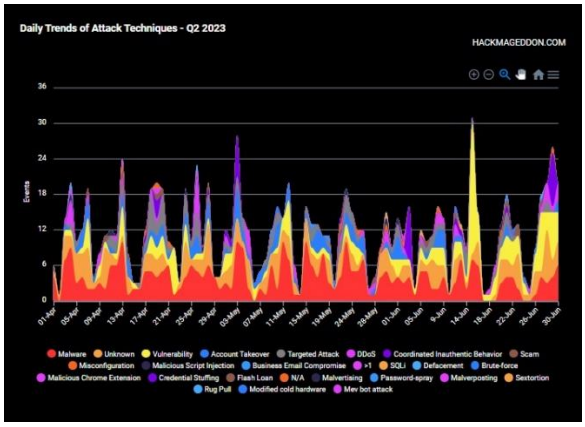

Figure 1. Q2 2023 Attack Techniques

DoS poses a major threat to network security because, as the name suggests, it aims to deny network resource service to legitimate users [5]. DDoS uses many machines to overload targeted network devices such as routers and servers, ensuring that legitimate hosts connected to the network are disrupted or taken down [6][7]. How do DoS or DDoS attacks occur? Computer communication occurs after protocols or connection rules are met. This rule is called "Three Way-handshake" which is where the user's computer sends a "SYN" (synchronize) packet to the server, then the server will reply with "SYN-ACK" (synchronize-acknowledgement), and the user will reply with "ACK" (acknowledgement).). DoS or DDoS attacks occur when the user does not reply to a "SYN-ACK" from the server with an "ACK" but the user sends a fake "SYN" packet to the server again [8]. A SYN flood attack is a well-known DoS technique that affects hosts running TCP server processes (the three-way handshake mechanism for TCP connections). Today, despite the original, many variations exist. Although there are many effective techniques against SYN flooding attacks, there is no effective defense [9]. The visualization of a DDoS attack on a server in this research is a router that sends "SYN" continuously by the attacker, which can be seen in Figure 2 so that users who should be served with the "ACK" protocol are ignored. Logfile Data packets in the form of network activity are then captured by investigators using port mirroring techniques.

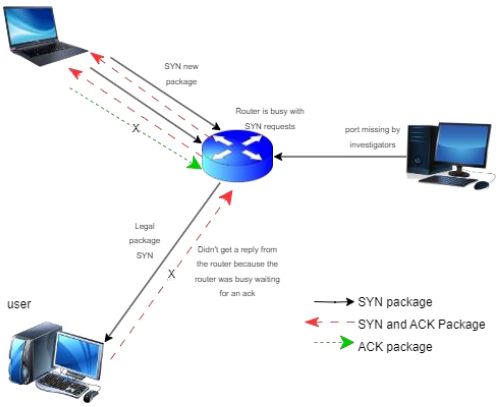

Figure 2. DoS Attack

Tabash and Bahroom's research on Denial of Service (DoS) attacks defines that DoS is a type of attack on a computer or internet network service by using up its resources until the computer or network service cannot carry out its function properly, so that it is not directly prevent legal users from accessing internet access services from the attacked computer network service. Several studies generally detect and prevent DoS attacks on large networks such as Wide Area Networks (WAN), but only a few studies investigate local networks such as Local Area Networks (LAN). This is because early prevention is carried out in a larger scope, so it is hoped that attacks cannot enter a smaller scope [10]. Bharti Nagpal believes that Distributed Denial of Service (DDoS) is a DoS attack that is executed across multiple computers. Therefore, the effects of DDoS attacks are more diverse and dangerous than his DoS attacks.

This research studies various applications to carry out various types of DDoS attacks so that it can help identify attacks and create defenses to anticipate DDoS attacks [11]. The attack data and ease of technology available above make it possible for anyone to carry out a DDoS attack, so research on DDoS will always be hot to study both technically and methodologically.

2. METHOD

Sentilkumaran explained that in his research uses the Threshold method to segment medical images [12] , according to him the threshold method is very easy to implement with good accuracy. The author will apply this method to classify DDoS attack data packets which will be visualized in 2-dimensional images to obtain the Threshold formula as follows:

$$T = T\,[\,x, P(x)] \tag{1}$$

T is Threshold value; x is the Threshold coordinate; P(x) is the probability of x; while the probability of x is obtained from:

$$P\,(x) = \begin{cases} \alpha\ , & x > \ (\mu + \ \delta) \\ \beta\ , & x\ other \end{cases} \tag{2}$$

Where P (x) is the probability of x; α is Class A; β is Class B; μ is the mean or average; and δ is the standard deviation.

The subject of this research is the Computer Network of Ahmad Dahlan University, Yogyakarta (CNADU) as the target of a DDoS attack. Computer Networks Computer Laboratory and Computer Networks Telecommunications Laboratory Electrical Engineering Ahmad Dahlan University as a DDoS Attacker. The CNADU topology shown in Figure 3 is distributed, a development of the star topology. CNADU becomes a network service center as well as sharing access for each user within its scope. The CNADU topology which acts as admin is a router with IP Address 192.168.10.254 for access from CNADU users to the wide internet network, while the IP Address 172.10.64.250 is for access from outside to the router as a CNADU service. Users in CNADU are IP addresses 192.168.10.64.2, 192.168.10.64.3, 192.168.10.64.4, 192.168.10.64.5, 192.168.10.64.6, 192.168.10.64.7, 192.168 .10.64.8, and 192.168 .10.64.9 in the scenario carries out normal activities by accessing the internet and carrying out functions on internet sites continuously for a duration of more than 1 hour. The attack was carried out from outside towards the target router of the CNADU network service with IP Address 172.10.64.250 by the attacker with IP Address 172.10.64.199, 172.10.85.151, 172.10.71.29, 172.10.71.49, 172.10.201.5, and 172.10.201 .19. Investigators used port mirroring access with IP Address 192.168.30.1 to retrieve network traffic log file data from within and to CNADU. Investigators captured the target IP address 192.168.10.254 to obtain a network activity logfile in the form of data packet traffic for approximately 1 hour. The results of this capturing are data which is then processed through extraction, filtering and pre-processing processes to obtain numeric attributes. This numeric attribute is classified so that normal access and attack access are known using the Threshold method. The capturing results obtained contain data which is then processed to be classified into 2 classes, namely the normal class and the attack class. The data is processed using the Threshold method so that each class can be identified.

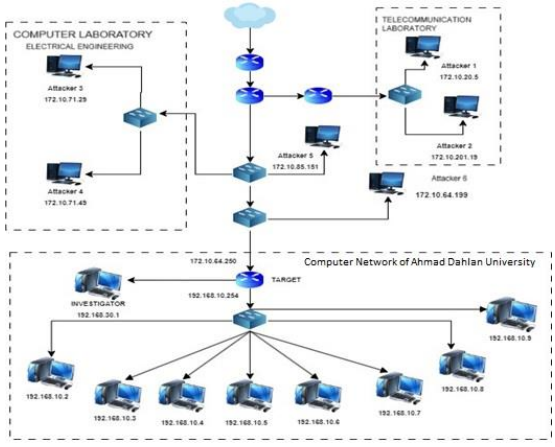

Figure 3. Topology

DOI: doi.org/10.35970/jinita.v6i1.2224

2.1. Threshold Method

Threshold is a method used to determine the threshold of an event [13]. The threshold method tasked with classifying normal and DDoS packet attacks, namely UDP Flood, Smurf, TCP SYN Flood and Ping of Death[14]. The Threshold symbol is used to create a normal class and an attack class based on Threshold for 2 input attributes, the IP Occurrence (x) and Packet Length (y) attributes [15] .

$$P(x) = \begin{cases} 1, & x > (\mu + \delta) \\ 0, & x \ other \end{cases} \quad (3)$$

$$P(y) = \begin{cases} 1, & y > (\mu + \delta) \\ 0, & y \ other \end{cases}$$

Where:
P (x) = Probability of attribute x
P (y) = Probability of attribute y
1 = attack
0 = normal
δ = standard deviation of the total data
μ = mean or average of the total data

Figure 4 shows a classification system using the Threshold method, where the output from the threshold will be 0 or 1 and then combined with or logic to produce class predictions.

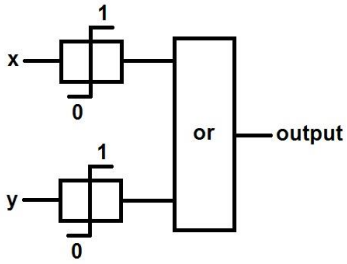

Figure 4. Classification Threshold Method [16]

Table 1. Class From Threshold Method

INPUT		CLASS (output) = x or y
x	*y*	
0	0	Normal
0	1	Attack
1	0	Attack
1	1	Attack

Table 1 shows the results of calculating 2 attributes x and y, then a decision is made using x or y logic.

3. RESULTS AND DISCUSSION

The results of the attack simulation in the form of a logfile are first processed into the desired parameters. The author has discussed data retrieval and pre-processing scenarios in depth in the publication DDoS Attack Classification using Numeric Attribute-based Gaussian Naïve Bayes [17] so we does not discuss it in detail in that section, but the author will discuss the Threshold method in detail for classifying DDoS attacks. The numeric attributes obtained from pre-processing get two parameters, namely the Occurrence IP Address and Packet Length.

DOI: doi.org/10.35970/jinita.v6i1.2224

Table 2. Input Data For Calculations Using Threshold Method

No	IP address	Access	IP Appearance x	Package Length y
1	192.168.10.2	Normal	81	16134
2	192.168.10.3	Normal	2939	405244
3	192.168.10.4	Normal	803	118889
4	192.168.10.5	Normal	1173	165510
5	192.168.10.6	Normal	1074	154472
6	192.168.10.7	Normal	1566	207772
7	192.168.10.8	Normal	1105	155560
8	192.168.10.9	Normal	1963	268497
9	172.10.64.199	Attack	3386	1088676
10	172.10.85.151	Attack	14323	2432059
11	172.10.201.5	Attack	10787	2282970
12	172.10.201.19	Attack	7658	1831513
13	172.10.71.29	Attack	8899	2525711
14	172.10.71.49	Attack	9437	1433478

3.1 Determining The Mean (μ) And Standard Deviation (δ)

The same network packet data, namely network packet data in the time range 0-3 minutes, is also used for network packet classification using the Threshold method. This data is shown in Table 2. From these data, find the mean (μ) and standard deviation (δ), and find the threshold that can cover the members of the set for each class. The mean and standard deviation in the Threshold method are calculated from all data for each attribute, so that the mean and standard deviation are obtained as follows:

Mean attribute x = 4657

Standard deviation of attribute x = 4605

Mean attribute y = 934749

Standard deviation of attribute y = 970224

Symbol (1) is then used to calculate the Threshold value based on the mean and standard deviation.

3.2 Determine Threshold

Determine the Threshold attribute x, $\mu + \delta = 4657 + 4605 = 9262$ so that the output has a value of 0 if it is smaller than the Threshold and a value of 1 if it is greater than the Threshold. The results of these calculations are shown in Table 3.

Table 3. Output Attribute x Using Threshold μ+ δ

No	IP address	IP Appearance x	><	Threshold	output
1	192.168.10.2	81	<	9262	0
2	192.168.10.3	2939	<	9262	0
3	192.168.10.4	803	<	9262	0
4	192.168.10.5	1173	<	9262	0
5	192.168.10.6	1074	<	9262	0
6	192.168.10.7	1566	<	9262	0
7	192.168.10.8	1105	<	9262	0
8	192.168.10.9	1963	<	9262	0
9	172.10.64.199	3386	<	9262	0
10	172.10.85.151	14323	>	9262	1
11	172.10.201.5	10787	>	9262	1
12	172.10.201.19	7658	<	9262	0
13	172.10.71.29	8899	<	9262	0
14	172.10.71.49	9437	>	9262	1

Determine the Threshold attribute y, $\mu + \delta = 934749 + 970224 = 1904973$ so that the output is 0 if it is smaller than the Threshold and 1 if it is greater than the Threshold. The calculation results are shown in Table 4.

DOI: doi.org/10.35970/jinita.v6i1.2224

Table 4. Output Attribute y Using Threshold μ+ δ

No	IP address	Package Length y	><	Threshold	Output
1	192.168.10.2	16134	<	1904973	0
2	192.168.10.3	405244	<	1904973	0
3	192.168.10.4	118889	<	1904973	0
4	192.168.10.5	165510	<	1904973	0
5	192.168.10.6	154472	<	1904973	0
6	192.168.10.7	207772	<	1904973	0
7	192.168.10.8	155560	<	1904973	0
8	192.168.10.9	268497	<	1904973	0
9	172.10.64.199	1088676	<	1904973	0
10	172.10.85.151	2432059	>	1904973	1
11	172.10.201.5	2282970	>	1904973	1
12	172.10.201.19	1831513	<	1904973	0
13	172.10.71.29	2525711	>	1904973	1
14	172.10.71.49	1433478	<	1904973	0

The calculation results are then classified using the or logic shown in Table 5.

Table 5. Output Attribute Y Using Threshold μ+ δ

IP Address	Access Type	Input		Output Class
		x	*y*	
192.168.10.2	normal	0	0	normal
192.168.10.3	normal	0	0	normal
192.168.10.4	normal	0	0	normal
192.168.10.5	normal	0	0	normal
192.168.10.6	normal	0	0	normal
192.168.10.7	normal	0	0	normal
192.168.10.8	normal	0	0	normal
192.168.10.9	normal	0	0	normal
172.10.64.199	Attack	0	0	normal
172.10.85.151	Attack	1	1	Attack
172.10.201.5	Attack	1	1	Attack
172.10.201.19	Attack	0	0	normal
172.10.71.29	Attack	0	1	Attack
172.10.71.49	Attack	1	0	Attack

Classification results in Table 5 with Threshold μ + δ produce an accuracy of 85.71%. This classification can be seen in Figure 5.

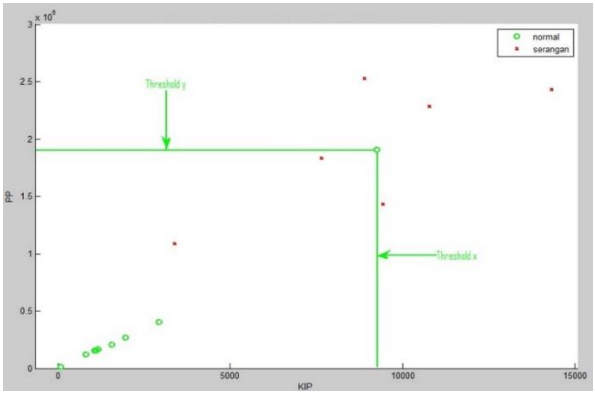

Figure 5. Classification Using Threshold μ + δ

The Set class does not properly contain its members, so the Threshold attribute x value is changed to, μ = 4657 so that the output has a value of 0 if it is smaller than the Threshold and a value of 1 if it is greater than the Threshold. The calculation results are shown in Table 6.

DOI: doi.org/10.35970/jinita.v6i1.2224

Table 6. Output attribute x using Threshold μ

No	IP address	IP Appearance x	><	Threshold	Output
1	192.168.10.2	81	<	4657	0
2	192.168.10.3	2939	<	4657	0
3	192.168.10.4	803	<	4657	0
4	192.168.10.5	1173	<	4657	0
5	192.168.10.6	1074	<	4657	0
6	192.168.10.7	1566	<	4657	0
7	192.168.10.8	1105	<	4657	0
8	192.168.10.9	1963	<	4657	0
9	172.10.64.199	3386	<	4657	0
10	172.10.85.151	14323	>	4657	1
11	172.10.201.5	10787	>	4657	1
12	172.10.201.19	7658	>	4657	1
13	172.10.71.29	8899	>	4657	1
14	172.10.71.49	9437	>	4657	1

The Set class does not properly contain its members, so the Threshold value of the y attribute is changed to, μ = 934749 so that the output has a value of 0 if it is smaller than the Threshold and a value of 1 if it is greater than the Threshold. The calculation results are shown in Table 7.

Table 7. Output attribute y Using Threshold μ

No	IP address	Package Length y	><	Threshold	output
1	192.168.10.2	16134	<	934749	0
2	192.168.10.3	405244	<	934749	0
3	192.168.10.4	118889	<	934749	0
4	192.168.10.5	165510	<	934749	0
5	192.168.10.6	154472	<	934749	0
6	192.168.10.7	207772	<	934749	0
7	192.168.10.8	155560	<	934749	0
8	192.168.10.9	268497	<	934749	0
9	172.10.64.199	1088676	>	934749	1
10	172.10.85.151	2432059	>	934749	1
11	172.10.201.5	2282970	>	934749	1
12	172.10.201.19	1831513	>	934749	1
13	172.10.71.29	2525711	>	934749	1
14	172.10.71.49	1433478	>	934749	1

The calculation results are then classified using the or logic shown in Table 8.

Table 8. Classification Results Using Threshold μ

No	IP Address	Access Type	Input		Class Output
			x	***y***	
1	192.168.10.2	normal	0	0	normal
2	192.168.10.3	normal	0	0	normal
3	192.168.10.4	normal	0	0	normal
4	192.168.10.5	normal	0	0	normal
5	192.168.10.6	normal	0	0	normal
6	192.168.10.7	normal	0	0	normal
7	192.168.10.8	normal	0	0	normal
8	192.168.10.9	normal	0	0	normal
9	172.10.64.199	Attack	0	1	Attack
10	172.10.85.151	Attack	1	1	Attack
11	172.10.201.5	Attack	1	1	Attack
12	172.10.201.19	Attack	1	1	Attack
13	172.10.71.29	Attack	1	1	Attack
14	172.10.71.49	Attack	1	1	Attack

Classification results in table 8 with Threshold μ produce 100% accuracy. This classification can be seen in Figure 6.

DOI: doi.org/10.35970/jinita.v6i1.2224

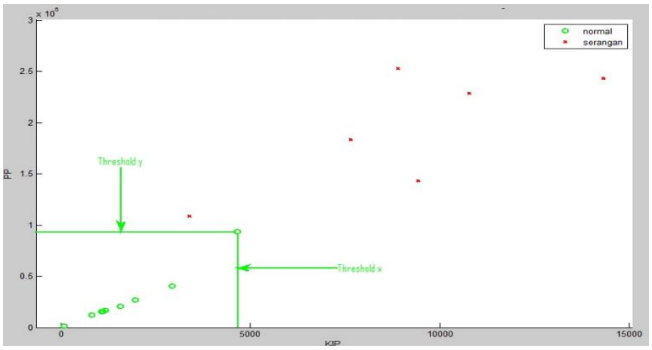

Figure 6. Classification with Threshold μ

3.3 Accuracy of The Tershold Method

By setting the Mean (μ) and Standard Deviation (δ) to get maximum accuracy, the results shown in Table 9 are obtained.

Table 9. Accuracy of Settings

Threshold	Normal IP Address Out of Class	IP Address Out-Of-Class Attack	Normal (True Positive)	Attack (True Negative)	Accuracy (%)
μ + δ	0	2	8	4	85,71
μ	0	0	8	6	100

The Threshold value is found by setting the Mean (μ) and Standard Deviation to get maximum accuracy (100%). The threshold value is Mean (μ).

3.4 Classification Results Using Threshold Methode

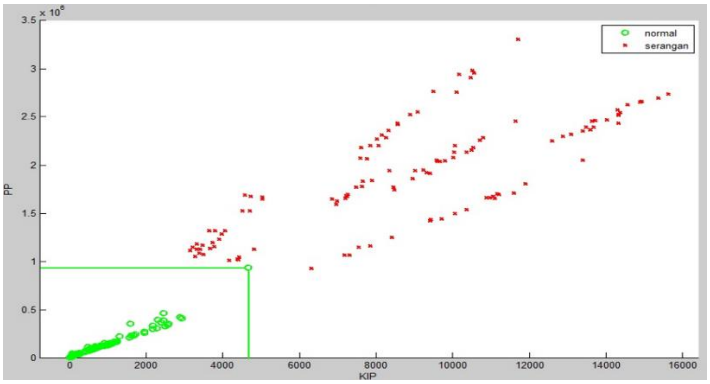

Figure 7. Classification all data with Threshold μ

Classification using the Threshold method then creates a class for all network packet data in CNADU. Mean (μ) is the limit of the set of each class. Classification results are obtained from all network packet data (attached) and report network access output in the form of IP address 192.168.10.2; 192.168.10.3; 192.168.10.4; 192.168.10.5; 192.168.10.6; 192.168.10.7; 192.168.10.8; and 192.168.10.9 is included in the normal class according to the access it performs, while the IP address is 172.10.64.199; 172.10.85.151; 172.10.201.5; 172.10.201.19; 172.10.71.29; and 172.10.71.46 is included in the attack class according to the access it performs. Visualization of the classification of all data for 60 minutes is shown in Figure 4.43. The set of normal classes and the set of attack classes are limited by the Threshold line.

4. CONCLUSION

Classification using the Threshold and Gaussian Naive Bayes methods can produce maximum accuracy of up to 100%. The set class using the Threshold method is limited by a straight line and the calculations are easier so it doesn't take a long time, while the Gaussian Naive Bayes method has 2 elliptical

DOI: doi.org/10.35970/jinita.v6i1.2224

set classes which are more specific in area with the mean (μ) as the center point of the set and the standard deviation (δ) as a matter of breadth, the calculations of the Gaussian Naive Bayes method are more complicated than those of the Threshold method.

ACKNOWLEDGEMENTS

All praise and honor goes to Allah SWT. I would like to express my sincere gratitude to my supervisor and everyone involved for their guidance and support until this research was completed as planned.

REFERENCES

[1] R. F. Fouladi, C. E. Kayatas, and E. Anarim, "Frequency Based DDoS Attack Detection Approach Using Naive Bayes Classification," no. June, 2016.

[2] Y. Bouzida *et al.*, "Detecting and reacting against distributed denial of service attacks To cite this version : HAL Id : hal-01923665 Detecting and Reacting against Distributed Denial of Service Attacks," 2018.

[3] K. Kato and V. Klyuev, "An Intelligent DDoS Attack Detection System Using Packet Analysis and Support Vector Machine," *Int. J. Intell. Comput. Res.*, vol. 5, no. 3, pp. 464–471, 2014, doi: 10.20533/ijicr.2042.4655.2014.0060.

[4] Paolo Passeri, "May 2023 Cyber Attacks Statistics," *Paolo Passeri*, 2023. https://www.hackmageddon.com/2023/07/06/may-2023-cyber-attacks-statistics/ (accessed Dec. 15, 2023).

[5] M. O. Schneider and J. Calmet, "Fibered Guard - A hybrid intelligent approach to denial of service prevention," *Proc. - Int. Conf. Comput. Intell. Model. Control Autom. CIMCA 2005 Int. Conf. Intell. Agents, Web Technol. Internet*, vol. 1, pp. 121–127, 2005, doi: 10.1109/cimca.2005.1631252.

[6] K. Elleithy and D. Blagovic, "Denial of Service Attack Techniques: Analysis, Implementation and Comparison," *J. Syst. …*, vol. 3, no. 1, pp. 66–71, 2006, [Online]. Available: http://www.iiisci.org/Journal/CV$/sci/pdfs/P129065.pdf

[7] M. Sazzadul Hoque, "An Implementation of Intrusion Detection System Using Genetic Algorithm," *Int. J. Netw. Secur. Its Appl.*, vol. 4, no. 2, pp. 109–120, 2012, doi: 10.5121/ijnsa.2012.4208.

[8] F. H. Hsu, Y. L. Hwang, C. Y. Tsai, W. T. Cai, C. H. Lee, and K. W. Chang, "TRAP: A Three-way handshake server for TCP connection establishment," *Appl. Sci.*, vol. 6, no. 11, 2016, doi: 10.3390/app6110358.

[9] M. Bogdanoski, T. Shuminoski, and A. Risteski, "Analysis of the SYN Flood DoS Attack," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 8, pp. 15–11, 2013, doi: 10.5815/ijcnis.2013.08.01.

[10] M. Merouane, "An approach for detecting and preventing DDoS attacks in campus," *Autom. Control Comput. Sci.*, vol. 51, no. 1, pp. 13–23, 2017, doi: 10.3103/S0146411616060043.

[11] B. Nagpal, P. Sharma, N. Chauhan, and A. Panesar, "DDoS tools: Classification, analysis and comparison," *2015 Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2015*, no. February, pp. 342–346, 2015.

[12] S. N and V. S, "Image Segmentation By Using Thresholding Techniques For Medical Images," *Comput. Sci. Eng. An Int. J.*, vol. 6, no. 1, pp. 1–13, 2016, doi: 10.5121/cseij.2016.6101.

[13] N. L. P. T. Ristanti and R. Pradana, "Penggunaan Metode Threshold Dalam Pembuatan Sistem Pendeteksi Asap Dan Api Dengan Berbasis Firebase Dan Android Menggunakan Nodemcu Pada BJ House 77," *J. TICOM Technol. Inf. Commun. Vol.*, vol. 11, no. 1, pp. 44–49, 2022.

[14] Z. binti mohd Safuan and M. azali bin zainal Abidin, "The Asian Journal of Professional and Business Studies," *Asian J. Prof. Bus. Stud.*, vol. 1, pp. 1–6, 2020.

[15] G. Loukas and E. Gelenbe, "Au th o r ' s ac c ep t ed m an u sc rip ep t m an u ac c Au th o r ' s sc".

[16] M. Sezgin, "Survey over image thresholding techniques and quantitative performance evaluation," *J. Electron. Imaging*, vol. 13, no. January, pp. 146–165, 2004, doi: 10.1117/1.1631316.

[17] A. Fadlil, I. Riadi, and S. Aji, "DDoS Attacks Classification using Numeric Attribute-based Gaussian Naive Bayes," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 8, pp. 42–50, 2017, doi: 10.14569/ijacsa.2017.080806.