

ISSN 2548-8368 (media online)

Jurnal
Media Informatika Budidarma

MIIB
STMIK Budi Darma Journal

Diterbitkan Oleh :



STMIK Budi Darma Medan

Jl. Sisingamangaraja No.338 Simpang Limun Medan

Telp. 061-7875998

<http://www.stmik-budidarma.ac.id>

Jurnal Media Informatika Budidarma	Volume : No.	Halaman:	Medan	ISSN 2548-8368 (media online)
---------------------------------------	-----------------	----------	-------	-------------------------------------

Editorial Team

Editor in Chief

Surya Darma Nasution, M.Kom, (SCOPUS ID: 57202607800, Universitas Budi Darma, Medan), Indonesia

Editorial Board

Prof. Dr. Dahlan Abdullah, ST, M.Kom, IP, (SCOPUS: 57205132023, Universitas Malikussaleh)

Tengku Mohd Diansyah, M.Kom, (SCOPUS ID: 57200092375, Universitas Harapan Medan, Medan), Indonesia

Fadlina Fadlina, M.Kom, (SCOPUS ID: 57202939718, Universitas Budi Darma, Medan), Indonesia

Khasanah Khasanah, M.Kom, (SCOPUS ID: 57205060611, Universitas Siber Asia, Jakarta Selatan), Indonesia

Akbar Iskandar, M.T, (SCOPUS ID:57203122768 , STMIK AKBA Makasar), Indonesia

Section Editor

Dr. Suginam Suginam, (SCOPUS ID:57202060942, Universitas Budi Darma, Medan), Indonesia

Dwika Assrani, M.Kom, (STMIK Mulia Darma, Rantoprapat), Indonesia

Alwin Fau, M.Kom, (Universitas Budi Darma, Medan), Indonesia

Vol 7, No1 (2023)

anuari 2023


DOI: <http://dx.doi.org/10.30865/mib.v7i1>


Table of Contents


Articles

Analisis Metode Ensemble Pada Klasifikasi Penyakit Jantung Berbasis Decision Tree

1-12 

 **Mochammad Ilham Aziz** (Universitas Dian Nuswantoro, Semarang, Indonesia)

 **Ahmad Zainul Fanani** (Universitas Dian Nuswantoro, Semarang, Indonesia)


 **Affandy Affandy** (Universitas Dian Nuswantoro, Semarang, Indonesia)


DOI: [10.30865/mib.v7i1.5169](https://doi.org/10.30865/mib.v7i1.5169) Abstract View 831 times


Efek Transformasi Wavelet Diskrit Pada Klasifikasi Aritmia Dari Data Elektrokardiogram Menggunakan Machine Learning


13-21 


 **Dodon Turianto Nugrahadi** (Universitas Lambung Mangkurat, Banjarbaru, Indonesia)


 **Tri Mulyani** (Universitas Lambung Mangkurat, Banjarbaru, Indonesia)

 **Dwi Kartini** (Universitas Lambung Mangkurat, Banjarbaru, Indonesia)

 **Rudy Herteno** (Universitas Lambung Mangkurat, Banjarbaru, Indonesia)

 **Mohammad Reza Faisal** (Universitas Lambung Mangkurat, Banjarbaru, Indonesia)

 **Irwan Budiman** (Universitas Lambung Mangkurat, Banjarbaru, Indonesia)


 **Friska Abadi** (Universitas Lambung Mangkurat, Banjarbaru, Indonesia)


DOI: [10.30865/mib.v7i1.4859](https://doi.org/10.30865/mib.v7i1.4859) Abstract View 347 times


Penerapan Data Mining Dalam Analisis Penilaian Kinerja Pegawai Menerapkan Metode K-Means

22-29 

 **Supriadi Sahibu** (Universitas Handayani Makassar, Makassar, Indonesia)

 **Rismawati Bambang** (Universitas Handayani Makassar, Makassar, Indonesia)


 **Imran Taufik** (Universitas Handayani Makassar, Makassar, Indonesia)


 **Agusriandi Agusriandi** (Universitas Sulawesi Barat, Majene, Indonesia)


DOI: [10.30865/mib.v7i1.5100](https://doi.org/10.30865/mib.v7i1.5100) Abstract View 488 times

Penerapan Algoritma C4.5 Untuk Klasifikasi Tren Pelanggaran Kendaraan Angkutan Barang dengan Metode CRISP-DM

30-40 

 **Novie Hari Purnomo** (STMIK LIKMI, Bandung, Indonesia)

 **Bayu Pamungkas** (STMIK LIKMI, Bandung, Indonesia)

 **Christina Juliane** (STMIK LIKMI, Bandung, Indonesia)

DOI: [10.30865/mib.v7i1.5247](https://doi.org/10.30865/mib.v7i1.5247) Abstract View 415 times

Implementasi Metode Convolutional Neural Network untuk Klasifikasi Breast Cancer pada Citra Histopatologi



41-49 

 **Muhammad Afrizal Amrustian** (Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia)
 **Merlinda Wibowo** (Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia)

DOI: [10.30865/mib.v7i1.5194](https://doi.org/10.30865/mib.v7i1.5194) Abstract View 251 times

Simulasi Pengukuran Mutu Perguruan Tinggi: Principal Component Analysis (PCA) pada Model Integrasi BANPT - COBIT



50-57 

 **Faradillah Faradillah** (Universitas Indo Global Mandiri, Palembang, Indonesia)
 **Muhammad Fadhiel Alie** (Universitas Sriwijaya, Palembang, Indonesia)

DOI: [10.30865/mib.v7i1.5190](https://doi.org/10.30865/mib.v7i1.5190) Abstract View 233 times

Optimasi Biaya Distribusi Kusen Pintu Menggunakan Model Transportasi Northwest Corner Method, Russel Approximation Method, dan Stepping Stone




58-65 

 **Poppy Andriani** (Universitas Islam Negeri Sumatera Utara, Medan, Indonesia)
 **Hendra Cipta** (Universitas Islam Negeri Sumatera Utara, Medan, Indonesia)

DOI: [10.30865/mib.v7i1.5224](https://doi.org/10.30865/mib.v7i1.5224) Abstract View 354 times

Analysis of Distributed Denial of Service Attacks Using Support Vector Machine and Fuzzy Tsukamoto






66-73 

 **Paradise Paradise** (Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia)
 **Wahyu Adi Prabowo** (Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia)
 **Teguh Rijanandi** (Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia)

DOI: [10.30865/mib.v7i1.5199](https://doi.org/10.30865/mib.v7i1.5199) Abstract View 211 times

Analisis Penerapan Metode WASPAS dan MOORA dalam Kelayakan Pengangkatan Karyawan Tetap



74-81 

 **Kraugusteeliana Kraugusteeliana** (Universitas Pembangunan Nasional Veteran Jakarta, Jakarta, Indonesia)
 **Sitti Nur Alam** (Universitas Yapis Papua, Jayapura, Indonesia)
 **Bambang Triwahyono** (Universitas Pembangunan Nasional Veteran Jakarta, Jakarta, Indonesia)
 **Muhammad Bayu Wibisono** (Universitas Pembangunan Nasional Veteran Jakarta, Jakarta, Indonesia)
 **Fryda Fatmayati** (Sekolah Tinggi Teknologi Kedirgantaraan, Bantul, Indonesia)

DOI: [10.30865/mib.v7i1.5343](https://doi.org/10.30865/mib.v7i1.5343) Abstract View 260 times

Sistem Pakar Untuk Mendiagnosa Penyakit Paru-Paru dengan Menggunakan Metode Teorema Bayes

82-88 

 **Alex Wenda** (Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia)
 **Kraugusteeliana Kraugusteeliana** (Universitas Pembangunan Nasional Veteran Jakarta, Jakarta, Indonesia)
 **Andik Adi Suryanto** (Universitas PGRI Ronggolawe, Tuban, Indonesia)
 **Sitti Nur Alam** (Universitas Yapis Papua, Jayapura, Indonesia)
 **Karya Suhada** (STMIK Rosma Karawang, Karawang, Indonesia)

DOI: [10.30865/mib.v7i1.5394](https://doi.org/10.30865/mib.v7i1.5394) Abstract View 765 times

Aspect-Based Sentiment Analysis on iPhone Users on Twitter Using the SVM Method and Optimization of Hyperparameter Tuning

89-98 

 **I Gusti Ayu Putu Sintha Deviya Yuliani** (Telkom University, Bandung, Indonesia)
 **Yuliant Sibaroni** (Telkom University, Bandung, Indonesia)
 **Erwin Budi Setiawan** (Telkom University, Bandung, Indonesia)

DOI: [10.30865/mib.v7i1.5430](https://doi.org/10.30865/mib.v7i1.5430) Abstract View 244 times



Analysis of Distributed Denial of Service Attacks Using Support Vector Machine and Fuzzy Tsukamoto

Paradise¹, Wahyu Adi Prabowo^{1,*}, Teguh Rijanandi²

¹Faculty of Informatics, Departement of Informatics Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia

²Faculty of Informatics, Departement of Software Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia

Email: ¹paradise@ittelkom-pwt.co.id, ^{2,*}wahyuadi@ittelkom-pwt.ac.id, ³19104008@ittelkom-pwt.ac.id

Correspondence Author Email: wahyuadi@ittelkom-pwt.ac.id

Abstract—Advances in technology in the field of information technology services allow hackers to attack internet systems, one of which is the DDOS attack, more specifically, the smurf attack, which involves multiple computers attacking database server systems and File Transfer Protocol (FTP). The DDOS smurf attack significantly affects computer network traffic. This research will analyze the classification of machine learning Support Vector Machine (SVM) and Fuzzy Tsukamoto in detecting DDOS attacks using intensive simulations in analyzing computer networks. Classification techniques in machine learning, such as SVM and fuzzy Tsukamoto, can make it easier to distinguish computer network traffic when detecting DDOS attacks on servers. Three variables are used in this classification: the length of the packet, the number of packets, and the number of packet senders. By testing 51 times, 50 times is the DDOS attack trial dataset performed in a computer laboratory, and one dataset derived from DDOS attack data is CAIDA 2007 data. From this study, we obtained an analysis of the accuracy level of the classification of machine learning SVM and fuzzy Tsukamoto, each at 100%.

Keywords: DDOS; Support Vector Machine; Fuzzy Tsukamoto

1. INTRODUCTION

With the development of technology used by various groups of people, the number of Internet users worldwide has also increased yearly. Many industries have used web-based information service systems [1] to provide services to their customers as a form of convenience in serving the public. Various industries use this online information service, such as education, government, and other sectors [2]–[6]. The availability of information services can also lure hackers [7] into attacking the internet system with a specific purpose. DoS and DDoS attacks can damage the availability of information services [8], [9]. These DoS and DDOS attacks also aim to prevent access to the server and network resources from clients that use those resources. This attack can be carried out by one person or several people or, more commonly, bots controlled by one person or system. Bots can act as malware when they are injected into a computer system [8], [10], [11]. So these bots can be considered a type of DDOS attack. A DDOS attack using bots can be executed via TCP, UDP, ICMP, and DNS packets to annoy clients by consuming server resources such as server sockets, ports, memory, databases, and incoming bandwidth. Usually, this DDOS attack is carried out by flooding website traffic through the HTTP web page system, and DDOS is a famous and dangerous attack.[12], [13]. There are three main categories of DDOS attacks based on target and behavior: bandwidth attacks, network traffic attacks, and application attacks. In an attack on bandwidth, the attacker sends anonymous pieces of data into a system and can cause congestion in the system, requiring more bandwidth in the computer network. In a traffic-based attack, the attacker sends a large number of TCP or UDP packets to the victim server, and these large packets will reduce the overall performance of the victim server. In application attacks, the attacker uses specific attacks to attack the system and shut down the system; this attack is difficult to mitigate. [14]

An efficient way to detect DDOS attacks on computer network channels is to monitor network traffic based on packet data and warn network administrators about suspicious behavior [4]. According to several reports on computer attacks, DDOS attacks are the most frequent attacks from year to year [16], [17] a significant attack on large system infrastructure. From paper [7], There are several ways to detect DDOS attacks: traffic analysis, entropy methods, connection analysis, and machine learning methods. Among these methods, the main concern in detecting DDOS attacks is using machine learning. [19], [20].

Several studies have found that machine learning capabilities can classify computer network traffic paths [21]–[24]. Research on the K-means method can detect DDOS attacks [13] Research on the K-means method can detect DDOS attacks [13]. This study can detect large-scale DDOS attacks in internet networks and worm attacks on the internet. Research on DDOS was also conducted by Niyaz et al [25], This study evaluates DDOS attacks based on normal traffic datasets and DDOS attack datasets. Deep learning has proven that DDOS attacks can be detected properly, but this research is limited to networks with a small coverage. Another study using the convolutional neural network [26], found that this method can detect phishing and DDOS attacks in the Internet of Things (IoT) environment. This study also makes use of traffic datasets, as well as phishing and DDOS datasets.

The research mentioned above highlights the use of machine learning in DDOS detection in internet traffic. According to several literature sources, data analysis and system design differ according to the networking environment. Given that using machine learning in internet security will be able to bring about major changes in



the organizational environment, this paper will focus on SVM and fuzzy Tsukamoto machine learning analysis to detect DDOS attacks on internet networks.

2. RESEARCH METHODOLOGY

The research method in this study is systematic and sequential which consists of several stages, namely the stages of observation, data collection, design of SVM and Fuzzy Tsukamoto machine learning parameters and stages of data analysis which can be seen in Figure 1.

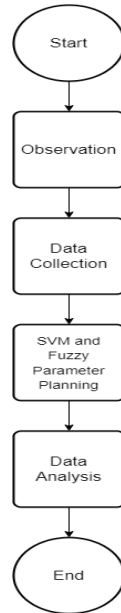


Figure 1. Research Methodology

Monitoring attacks on the network carry out during this observation stage. Researchers have found that DDOS attacks are still a common type of attack against services on the Internet. Based on these findings, researchers decided to classify DDOS attacks using the SVM and fuzzy Tsukamoto methods. The next step is data collection. In addition to the data used as research subjects, researchers gathered information through literature searches. Literature research is needed as a basis for decision-making and determining fuzzy parameters. At this point, the researcher also took a data set of Internet traffic that experienced DDOS attacks as a parameter for the SVM and Tsukamoto fuzzy machine learning classification. After gathering sufficient information and knowledge, the researcher designed the SVM and Tsukamoto fuzzy parameters. Parameter determination is based on network traffic observations and related literacy. After the program is designed, the next step is to test the program using network traffic capture data. The results of each test were analyzed using the confusion matrix method. The accuracy of the DDOS detection of the program that has been created is the result of this step.

3. RESULT AND DISCUSSION

3.1 Observation & Data Collection

The initial stage carried out in this study was data collection. Data were obtained from the CAIDA DDoS 2007 Attack Dataset, which contains network traffic for about one hour from the DDoS attack on August 4, 2007 (20:50:08 UTC to 21:56:16 UTC), was first converted to CSV format. In addition, additional data were obtained from the results of the DDOS trial via a live computer by capturing computer network traffic packets using the Wireshark application from the simulation scenarios. In table 1. The simulation is carried out with one attacker computer, three client computers, and one server computer connected to the same wireless network, each with an Internet Protocol address as follows:

Table 1. Internet Protocol DDOS Trial

PC Name	IP Address
PC O (Attacker)	192.168.111.7
PC A (Client)	192.168.111.1
PC B (Client)	192.168.111.3
PC C (Client)	192.168.111.5
SERVER	192.168.111.10



Then the three client computers send ICMP packets to the server computer simultaneously, according to the predetermined simulation scenario. The following are two simulation scenarios:

1. Normal simulation scenario

The first simulation scenario is a normal traffic simulation between the client and the server, shown in Figure 2. In this scenario, the three clients send ICMP packets controlled by the attacker's computer according to the ICMP packet standard in browsing mode. Meanwhile, the server computer opens the Wireshark application installed to start packet capture. The capture process is stopped when approximately 1000 packets are received. Then the capture results are stored in CSV format. This process was repeated 50 times.

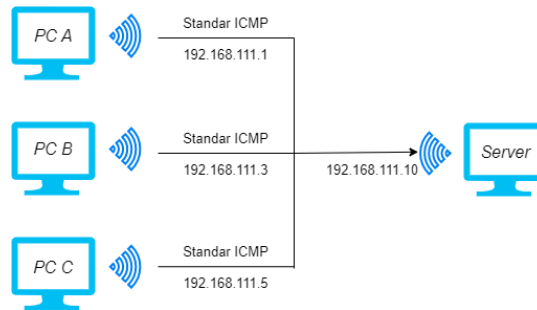


Figure 2. Normal Simulation Scenario

2. DDOS simulation scenario

The second simulation scenario is a traffic simulation where the client carries out a DDoS Smurf Attack attack on the server, which can be seen in Figure 3. In this scenario, the three clients send ICMP packets larger than the standard ICMP packet size. The packet size used is 65,500 bytes. The packet size is the standard size sent for DDoS smurf attacks. Next, similar to the first simulation scenario, the server computer opens the Wireshark application to start packet capture. The capture process is stopped when the number of packets reaches around 1000. Then save the capture results in CSV format, and this trial is repeated up to 50 times, the same as the first simulation scenario, so the data is validated correctly.

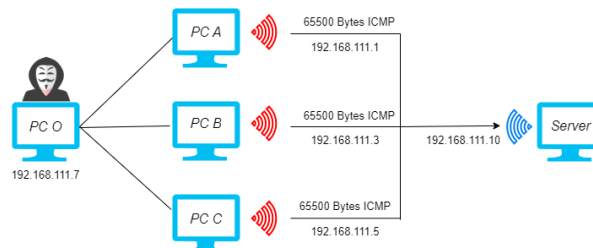


Figure 3. DDOS Simulation Scenario

Determining Variables and Fuzzy Sets The next step is determining the variables and fuzzy sets. The following are the variables and fuzzy sets that the author uses:

1. Number of variable packages

The number of packets is used to measure the number of packets that enter one server's IP address. There are two fuzzy sets for the variable number of packets, namely the small number of packets and the large number of packets. If the number of incoming packets in one interval is still less than 50, then the number of packets is still relatively small. However, if the number of incoming packets in one interval is more than 50, the number of packets is quite large.

2. Number of sources (origin of packages)

The variable number of sources, or the number of packet origins, is used to measure the number of IP addresses that send packets to one server's IP address. There are two fuzzy sets on the variable number of sources, namely, 43 (the number of single sources) and 51 (the number of multi-source sources). If only one IP address sends data to the server IP address in a given time interval, the number of sources is considered single. However, if more than three different IP addresses send packets to the same server IP address, it is classified as a multi-source number.

3. Package Length

The packet length variable measures the packet size received by one server IP address. If there is more than one package sender, then the average package size from each sender is calculated. Normally, ICMP packets have the smallest packet size of 56 bytes, and the largest is 84 bytes if the IPV4 header is included. However, generally, ICMP packets have a packet size of 74 bytes. The writer uses this quantity as a reference to determine the fuzzy set on the packet length variable. There are three classifications for the determined packet length variable: short packet length, normal packet length, and long packet length. If the total length of packets received in one interval is less than 74 bytes, then the packet length is classified as short. If the packet length is between 56 bytes and 84



bytes, the packet length is normal. However, if the packet length is more than 84 bytes, the packet length is relatively long.

3.2 SVM and Fuzzy Parameter Planning

SVM machine learning design To classify network traffic, machine learning requires training data that serves as the foundation for a learning model. Train data is generated by collecting traffic on the network that has been received. At this stage, a network traffic design is used to determine the type of traffic sent to the server. In this research, there are two categories of traffic: normal traffic and DDoS attack traffic. As explained in the previous section, this research was conducted by collecting data to obtain training data from normal traffic and DDoS attack traffic. After that, a dataset will be generated that contains data from network traffic that has been extracted. Figure 4 is a machine learning design that is carried out to create a support vector machine model.

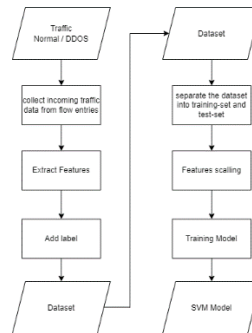


Figure 4. SVM flowcharts

Determining fuzzy parameters is carried out to meet the needs of calculations using the fuzzy method. Based on the Tsukamoto fuzzy flowchart in Figure 5, several parameters are input for the primary process of fuzzy calculations. In the fuzzification process, the input of fuzzy variables, fuzzy domains, and the x value of the variable to be searched is required to produce output in the form of the degree of membership of the x value. Variables and fuzzy domains are static, while the value of x is dynamic. The inference process requires input from fuzzy rules and membership degree values resulting from the fuzzification process to produce output in alpha predicate values and x values for each rule. Fuzzy rules are static, while membership degree values are dynamic. The final process, namely defuzzification, requires alpha predicate input and the x value of each rule from the results of the inference process to produce output in the form of classification results. Alphapredicate input is dynamic. Three parameters must be determined from static input: fuzzy variables, fuzzy domains, and fuzzy rules. Researchers determine three fuzzy variables based on network traffic capture results: packet length, number of packets received, and number of packet senders. Apart from fuzzy variables, other parameters that must be determined are domains and fuzzy rules. The method used to determine the domain in each variable is through discussions with network security experts and literature studies.

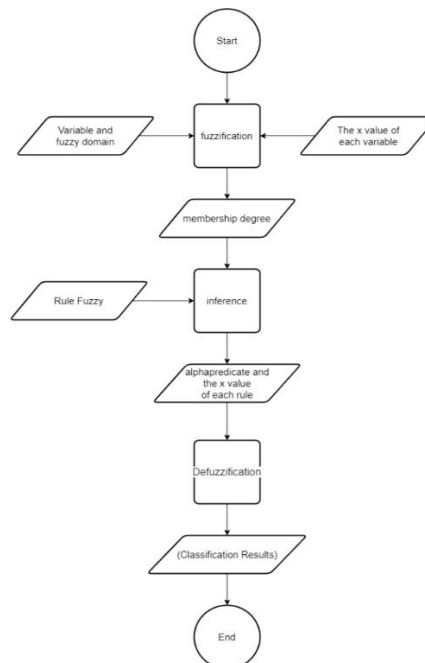


Figure 5. Fuzzy Tsukamoto Flow Chart



In contrast, IPV4 is included because, in some cases, the packet will be segmented if the data size of the ICMP packet sent is large. Segmented packets will be recognized as IPv4 protocols. The second step is to change the time for each packet in seconds. Packages captured using Wireshark will have a time in milliseconds. The reason for converting to seconds is that packets will be counted every one-second interval during the fuzzy algorithm's calculation process. The third stage is eliminating the destination IP address other than the server IP address. The goal is that the packets analyzed only go to the server's IP address. On the other hand, a packet containing the server IP address is cleaned for the source IP address, so the packet does not come from the server IP address. Figure 6 is the line of code in the preprocessing step:

```
path = " normaldata.csv"
df = pd.read_csv (path)
server_ip = "192.168.111.10"
df = df[df['protocol'].isin (['ICMP', 'IPv4'])]
df.Time = df.Time.astype(int)
df = df[df['Source'] != server_ip]
df = df[df['Destination'] == server_ip]
```

Figure 6. Data Preprocessing

3.3 Data Analysis

After the program has been created, the next step is to test it. Testing is done by scanning the data that has been obtained. The test was carried out 51 times, and 50 times the normal simulation data was scanned. Fifty times against DDoS simulation data and once against CAIDA data. This test uses a network topology consisting of one controller, two switches, and 30 hosts. The following are the detection results from all tests:

Table 2. DDOS Dataset Test Results

No	Data Type	Result
1	Normal Simulation 1	Normal Traffic
2	Normal Simulation 2	Normal Traffic
3	Normal Simulation 3	Normal Traffic
4	Normal Simulation 4	Normal Traffic
5	Normal Simulation 5	Normal Traffic
6	Normal Simulation 6	Normal Traffic
7	Normal Simulation 7	Normal Traffic
8	Normal Simulation 8	Normal Traffic
9	Normal Simulation 9	Normal Traffic
10	Normal Simulation 10	Normal Traffic
11	Normal Simulation 11	Normal Traffic
12	Normal Simulation 12	Normal Traffic
13	Normal Simulation 13	Normal Traffic
14	Normal Simulation 14	Normal Traffic
15	Normal Simulation 15	Normal Traffic
16	Normal Simulation 16	Normal Traffic
17	Normal Simulation 17	Normal Traffic
18	Normal Simulation 18	Normal Traffic
19	Normal Simulation 19	Normal Traffic
20	Normal Simulation 20	Normal Traffic
21	Normal Simulation 21	Normal Traffic
22	Normal Simulation 22	Normal Traffic
23	Normal Simulation 23	Normal Traffic
24	Normal Simulation 24	Normal Traffic
25	Normal Simulation 25	Normal Traffic
26	DDOS Simulation 1	DDOS Attack
27	DDOS Simulation 2	DDOS Attack
28	DDOS Simulation 3	DDOS Attack
29	DDOS Simulation 4	DDOS Attack
30	DDOS Simulation 5	DDOS Attack
31	DDOS Simulation 6	DDOS Attack
32	DDOS Simulation 7	DDOS Attack
33	DDOS Simulation 8	DDOS Attack
34	DDOS Simulation 9	DDOS Attack
35	DDOS Simulation 10	DDOS Attack



No	Data Type	Result
36	DDOS Simulation 11	DDOS Attack
37	DDOS Simulation 12	DDOS Attack
38	DDOS Simulation 13	DDOS Attack
39	DDOS Simulation 14	DDOS Attack
40	DDOS Simulation 15	DDOS Attack
41	DDOS Simulation 16	DDOS Attack
42	DDOS Simulation 17	DDOS Attack
43	DDOS Simulation 18	DDOS Attack
44	DDOS Simulation 19	DDOS Attack
45	DDOS Simulation 20	DDOS Attack
46	DDOS Simulation 21	DDOS Attack
47	DDOS Simulation 22	DDOS Attack
48	DDOS Simulation 23	DDOS Attack
49	DDOS Simulation 24	DDOS Attack
50	DDOS Simulation 25	DDOS Attack
51	Data Set CAIDA	DDOS Attack

From the test results above, it can be mapped into the confusion matrix mapping table as follows:

Table 3. Confussion Matrix

Prediction Actual	Normal Traffic	DDOS Attack
Normal Traffic	25	0
DDOS Attack	0	26

The normal simulation data detection results that are detected by normal traffic yield true positive values, while the DDOS and CAIDA simulation data that are detected by DDOS attack yield true negative values. The false positive value is obtained from the DDOS and CAIDA simulation data detection results detected by normal traffic. The false negative value is obtained from the normal simulation data detection results detected by a DDOS attack. So, the True Positive (TP) value is 20, the True Negative (TN) value is 21, the False Positive (FP) value is 0, and the False Negative (FN) value is 0. Then, from these results, the detection accuracy level can be calculated as follows:

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$accuracy = \frac{25 + 26}{25 + 26 + 0 + 0}$$

$$accuracy = \frac{51}{51}$$

$$accuracy = 1$$

From the calculation above, the detection accuracy level of the program that has been made is 100%. Testing the accuracy of DDoS attack detection aims to measure the system's accuracy in detecting DDoS attacks. A DDoS attack is carried out at this stage, namely a smurf attack. The experiment was carried out by sending the attack, and then the data from the attack was tested for accuracy using SVM and fuzzy machine learning. Table 3 is the result of testing the accuracy of DDoS attack detection.

Table 4. Machine Learning Test Results

Types of DDOS Attacks	Machine Learning	Level of accuracy
Smurf Attack	SVM	100%
Smurf Attack	Fuzzy Tsukamoto	100%

4. CONCLUSION

The DDOS smurf attack is tested by entering the DDOS attack dataset based on the conditions that exist in the running network. Then the dataset is assessed and processed using machine learning techniques such as SVM (support vector machines) and fuzzy Tsukamoto to obtain DDOS detection values. Based on the 51 test results, the detection results obtained were 25 normal data points without DDOS attacks and 25 DDOS attacks. This data was obtained through a real-time test attack against the networking system. One dataset was obtained through CAIDA 2007 data, and the result is that the data was detected as a DDOS attack. The level of accuracy resulting



from the program created to detect the type of DDOS Ping of Death attack using the Tsukamoto fuzzy method and SVM is 100%. This can be seen from the confusion matrix mapping table, where the program can detect the actual class of the input data. The detection model relies on a reference dataset, which a learning process will then form a system that labels each packet that enters the networking system. Tsukamoto's fuzzy machine learning and SVM can classify network traffic data subjected to a DDOS attack by analyzing packet length, the number of packets, and a number of packet senders. The results of this study still need to be studied further because they are limited to three analyses: the packet length, the number of packets, and the number of packet senders: the fewer variables, the greater the level of accuracy. In future research, adding other variables that can be used to detect DDOS attacks and use other DDOS attack simulation scenarios would be better.

ACKNOWLEDGMENT

We would like to thank the Ministry of Research, Technology and Higher Education of the Republic of Indonesia (RISTEKDIKTI) for funding this research through the "skim Penelitian Dasar Pemula 2022" program.

REFERENCES

- [1] I. Lizarralde, C. Mateos, J. M. Rodriguez, and A. Zunino, "Exploiting named entity recognition for improving syntactic-based web service discovery," *J Inf Sci*, vol. 45, no. 3, 2019, doi: 10.1177/0165551518793321.
- [2] L. Jiang, Q. Xie, and L. Chen, "Application and Feasibility Study of Integrated Nursing Information Construction in Nephrology Nursing," *J Healthc Eng*, vol. 2022, 2022, doi: 10.1155/2022/7033840.
- [3] D. N. Aryani *et al.*, "Factors Influencing Consumer Behavioral Intention to Use Food Delivery Services: A Study of Foodpanda," *Journal of The Community Development in Asia*, vol. 5, no. 1, 2022.
- [4] F. Liang, L. Mu, D. Wang, and B. S. Kim, "A new model path for the development of smart leisure sports tourism industry based on 5G technology," *IET Communications*, vol. 16, no. 5, 2022, doi: 10.1049/cmu2.12271.
- [5] P. Tambare, C. Meshram, C. C. Lee, R. J. Ramteke, and A. L. Imoize, "Performance measurement system and quality management in data-driven industry 4.0: A review," *Sensors*, vol. 22, no. 1, 2022. doi: 10.3390/s22010224.
- [6] Z. Bezhovski, "The Future of the Mobile Payment as Electronic Payment System," *European Journal of Business and Management*, 2016.
- [7] M. C. Cohen, "Big Data and Service Operations," *Prod Oper Manag*, vol. 27, no. 9, 2018, doi: 10.1111/poms.12832.
- [8] M. Zolotukhin, T. Hamalainen, T. Kokkonen, and J. Siltanen, "Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic," in *2016 23rd International Conference on Telecommunications, ICT 2016*, 2016. doi: 10.1109/ICT.2016.7500408.
- [9] D. J. Prathyusha and G. Kannayaram, "A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment," *Evol Intell*, vol. 14, no. 2, 2021, doi: 10.1007/s12065-019-00340-4.
- [10] X. Zhang, O. Upton, N. L. Beebe, and K. K. R. Choo, "IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers," *Forensic Science International: Digital Investigation*, vol. 32, 2020, doi: 10.1016/j.fsidi.2020.300926.
- [11] P. K. Manadhata, S. Yadav, P. Rao, and W. Home, "Detecting malicious domains via graph inference," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2014, vol. 2014-November, no. November. doi: 10.1145/2666652.2666659.
- [12] Y. M. Alginahi and M. N. Kabir, *Authentication technologies for cloud computing, iot and big data*. 2019. doi: 10.1049/pbse009e.
- [13] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, and A. Patel, "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique," *Engineering Applications of Artificial Intelligence*, vol. 26, no. 9, 2013. doi: 10.1016/j.engappai.2013.04.010.
- [14] S. Sambangi and L. Gondi, "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression," 2020. doi: 10.3390/proceedings2020063051.
- [15] A. A. Sallam, M. N. Kabir, Y. M. Alginahi, A. Jamal, and T. K. Esmeel, "IDS for Improving DDoS Attack Recognition Based on Attack Profiles and Network Traffic Features," in *Proceedings - 2020 16th IEEE International Colloquium on Signal Processing and its Applications, CSPA 2020*, 2020. doi: 10.1109/CSPA48992.2020.9068679.
- [16] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali, "Towards a Universal Features Set for IoT Botnet Attacks Detection," in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, 2020. doi: 10.1109/INMIC50486.2020.9318106.
- [17] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, 2020. doi: 10.1109/INMIC50486.2020.9318216.
- [18] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, 2017. doi: 10.1007/s13369-017-2414-5.
- [19] H. Wang *et al.*, "DDoS Attack in Software Defined Networks: A Survey," *Neural Regen Res*, vol. 7, no. 14, 2017.
- [20] L. F. Eliyan and R. di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, 2021, doi: 10.1016/j.future.2021.03.011.
- [21] V. Deepa, K. Muthamil Sudar, and P. Deepalakshmi, "Detection of DDoS attack on SDN control plane using hybrid machine learning techniques," in *Proceedings of the International Conference on Smart Systems and Inventive Technology, ICSSIT 2018*, 2018. doi: 10.1109/ICSSIT.2018.8748836.
- [22] L. Yang and H. Zhao, "DDoS attack identification and defense using SDN based on machine learning method," in *Proceedings - 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018*, 2019. doi: 10.1109/I-SPAN.2018.00036.



- [23] M. Revathi, V. v. Ramalingam, and B. Amutha, "A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework," *Wirel Pers Commun*, 2021, doi: 10.1007/s11277-021-09071-1.
- [24] R. T. Kokila, S. Thamarai 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*, 2015. doi: 10.1109/ICoAC.2014.7229711.
- [25] Q. Niyaz, W. Sun, and A. Y. Javaid, "A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)," *ICST Transactions on Security and Safety*, vol. 4, no. 12, 2017, doi: 10.4108/eai.28-12-2017.153515.
- [26] G. de La Torre Parra, P. Rad, K. K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *Journal of Network and Computer Applications*, vol. 163, Aug. 2020, doi: 10.1016/j.jnca.2020.102662.

Paper Analysis of Distributed Denial of Service Attacks Using Support Vector Machine and Fuzzy Tsukamoto

by Paradise Paradise

Submission date: 31-Jul-2023 07:28PM (UTC+0700)

Submission ID: 2139499068

File name: ice_Attacks_Using_Support_Vector_Machine_and_Fuzzy_Tsukamoto.pdf (477.8K)

Word count: 4758

Character count: 25274



Analysis of Distributed Denial of Service Attacks Using Support Vector Machine and Fuzzy Tsukamoto

Paradise¹, Wahyu Adi Prabowo^{1,*}, Teguh Rijanandi²

¹Faculty of Informatics, Departement of Informatics Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia

²Faculty of Informatics, Departement of Software Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia

Email: ¹paradise@ittelkom-pwt.co.id, ^{2,*}wahyuadi@ittelkom-pwt.ac.id, ³19104008@ittelkom-pwt.ac.id

Correspondence Author Email: wahyuadi@ittelkom-pwt.ac.id

Abstract—Advances in technology in the field of information technology services allow hackers to attack internet systems, one of which is the DDOS attack, more specifically, the smurf attack, which involves multiple computers attacking database server systems and File Transfer Protocol (FTP). The DDOS smurf attack significantly affects computer network traffic. This research will analyze the classification of machine learning Support Vector Machine (SVM) and Fuzzy Tsukamoto in detecting DDOS attacks using intensive simulations in analyzing computer networks. Classification techniques in machine learning, such as SVM and fuzzy Tsukamoto, can make it easier to distinguish computer network traffic when detecting DDOS attacks on servers. Three variables are used in this classification: the length of the packet, the number of packets, and the number of packet senders. By testing 51 times, 50 times is the DDOS attack trial dataset performed in a computer laboratory, and one dataset derived from DDOS attack data is CAIDA 2007 data. From this study, we obtained an analysis of the accuracy level of the classification of machine learning SVM and fuzzy Tsukamoto, each at 100%.

Keywords: DDOS; Support Vector Machine; Fuzzy Tsukamoto

1. INTRODUCTION

With the development of technology used by various groups of people, the number of Internet users worldwide has also increased yearly. Many industries have used web-based information service systems [1] to provide services to their customers as a form of convenience in serving the public. Various industries use this online information service, such as education, government, and other sectors [2]–[6]. The availability of information services can also lure hackers [7] into attacking the internet system with a specific purpose. DoS and DDOS attacks can damage the availability of information services [8], [9]. These DoS and DDOS attacks also aim to prevent access to the server and network resources from clients that use those resources. This attack can be carried out by one person or several people or, more commonly, bots controlled by one person or system. Bots can act as malware when they are injected into a computer system [8], [10], [11]. So these bots can be considered a type of DDOS attack. A DDOS attack using bots can be executed via TCP, UDP, ICMP, and DNS packets to annoy clients by consuming server resources such as server sockets, ports, memory, databases, and incoming bandwidth. Usually, this DDOS attack is carried out by flooding website traffic through the HTTP web page system, and DDOS is a famous and dangerous attack [12], [13]. There are three main categories of DDOS attacks based on target and behavior: bandwidth attacks, network traffic attacks, and application attacks. In an attack on bandwidth, the attacker sends anonymous pieces of data into a system and can cause congestion in the system, requiring more bandwidth in the computer network. In a traffic-based attack, the attacker sends a large number of TCP or UDP packets to the victim server, and these large packets will reduce the overall performance of the victim server. In application attacks, the attacker uses specific attacks to attack the system and shut down the system; this attack is difficult to mitigate. [14]

An efficient way to detect DDOS attacks on computer network channels is to monitor network traffic based on packet data and warn network administrators about suspicious behavior [4]. According to several reports on computer attacks, DDOS attacks are the most frequent attacks from year to year [16], [17] a significant attack on large system infrastructure. From paper [7], There are several ways to detect DDOS attacks: traffic analysis, entropy methods, connection analysis, and machine learning methods. Among these methods, the main concern in detecting DDOS attacks is using machine learning. [19], [20].

Several studies have found that machine learning capabilities can classify computer network traffic paths [21]–[24]. Research on the K-means method can detect DDOS attacks [13] Research on the K-means method can detect DDOS attacks [13]. This study can detect large-scale DDOS attacks in internet networks and worm attacks on the internet. Research on DDOS was also conducted by Niyaz et al [25], This study evaluates DDOS attacks based on normal traffic datasets and DDOS attack datasets. Deep learning has proven that DDOS attacks can be detected properly, but this research is limited to networks with a small coverage. Another study using the convolutional neural network [26], found that this method can detect phishing and DDOS attacks in the Internet of Things (IoT) environment. This study also makes use of traffic datasets, as well as phishing and DDOS datasets.

The research mentioned above highlights the use of machine learning in DDOS detection in internet traffic. According to several literature sources, data analysis and system design differ according to the networking environment. Given that using machine learning in internet security will be able to bring about major changes in



the organizational environment, this paper will focus on SVM and fuzzy Tsukamoto machine learning analysis to detect DDOS attacks on internet networks.

2. RESEARCH METHODOLOGY

The research method in this study is systematic and sequential which consists of several stages, namely the stages of observation, data collection, design of SVM and Fuzzy Tsukamoto machine learning parameters and stages of data analysis which can be seen in Figure 1.

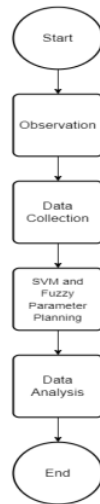


Figure 1. Research Methodology

Monitoring attacks on the network carry out during this observation stage. Researchers have found that DDOS attacks are still a common type of attack against services on the Internet. Based on these findings, researchers decided to classify DDOS attacks using the SVM and fuzzy Tsukamoto methods. The next step is data collection. In addition to the data used as research subjects, researchers gathered information through literature searches. Literature research is needed as a basis for decision-making and determining fuzzy parameters. At this point, the researcher also took a data set of Internet traffic that experienced DDOS attacks as a parameter for the SVM and Tsukamoto fuzzy machine learning classification. After gathering sufficient information and knowledge, the researcher designed the SVM and Tsukamoto fuzzy parameters. Parameter determination is based on network traffic observations and related literacy. After the program is designed, the next step is to test the program using network traffic capture data. The results of each test were analyzed using the confusion matrix method. The accuracy of the DDOS detection of the program that has been created is the result of this step.

18

3. RESULT AND DISCUSSION

3.1 Observation & Data Collection

The initial stage carried out in this study was data collection. Data were obtained from the CAIDA DDoS 2007 Attack Dataset, which contains network traffic for about one hour from the DDoS attack on August 4, 2007 (20:50:08 UTC to 21:56:16 UTC), was first converted to CSV format. In addition, additional data were obtained from the results of the DDOS trial via a live computer by capturing computer network traffic packets using the Wireshark application from the simulation scenarios. In table 1. The simulation is carried out with one attacker computer, three client computers, and one server computer connected to the same wireless network, each with an Internet Protocol address as follows:

Table 1. Internet Protocol DDOS Trial

PC Name	IP Address
P21 (Attacker)	192.168.111.7
PC A (Client)	192.168.111.1
PC B (Client)	192.168.111.3
PC C (Client)	192.168.111.5
SERVER	192.168.111.10



Then the three client computers send ICMP packets to the server computer simultaneously, according to the predetermined simulation scenario. The following are two simulation scenarios:

1. Normal simulation scenario

The first simulation scenario is a normal traffic simulation between the client and the server, shown in Figure 2. In this scenario, the three clients send ICMP packets controlled by the attacker's computer according to the ICMP packet standard in browsing mode. Meanwhile, the server computer opens the Wireshark application installed to start packet capture. The capture process is stopped when approximately 1000 packets are received. Then the capture results are stored in CSV format. This process was repeated 50 times.

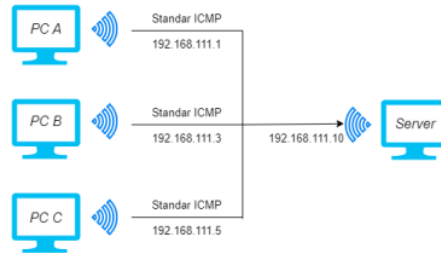


Figure 2. Normal Simulation Scenario

2. DDOS simulation scenario

The second simulation scenario is a traffic simulation where the client carries out a DDos Smurf Attack attack on the server, which can be seen in Figure 3. In this scenario, the three clients send ICMP packets larger than the standard ICMP packet size. The packet size used is 65,500 bytes. The packet size is the standard size sent for DDOS smurf attacks. Next, similar to the first simulation scenario, the server computer opens the Wireshark application to start packet capture. The capture process is stopped when the number of packets reaches around 1000. Then save the capture results in CSV format, and this trial is repeated up to 50 times, the same as the first simulation scenario, so the data is validated correctly.

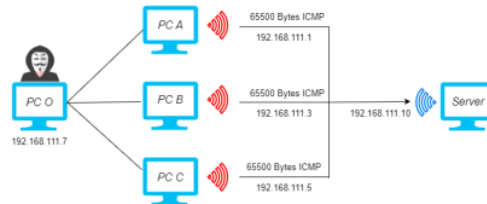


Figure 3. DDOS Simulation Scenario

Determining Variables and Fuzzy Sets The next step is determining the variables and fuzzy sets. The following are the variables and fuzzy sets that the author uses:

1. Number of variable packages

The number of packets is used to measure the number of packets that enter one server's IP address. There are two fuzzy sets for the variable number of packets, namely the small number of packets and the large number of packets. If the number of incoming packets in one interval is still less than 50, then the number of packets is still relatively small. However, if the number of incoming packets in one interval is more than 50, the number of packets is quite large.

2. Number of sources (origin of packages)

The variable number of sources, or the number of packet origins, is used to measure the number of IP addresses that send packets to one server's IP address. There are two fuzzy sets on the variable number of sources, namely, 43 (the number of single sources) and 51 (the number of multi-source sources). If only one IP address sends data to the server IP address in a given time interval, the number of sources is considered single. However, if more than three different IP addresses send packets to the same server IP address, it is classified as a multi-source number.

3. Package Length

The packet length variable measures the packet size received by one server IP address. If there is more than one package sender, then the average package size from each sender is calculated. Normally, ICMP packets have the smallest packet size of 56 bytes, and the largest is 84 bytes if the IPV4 header is included. However, generally, ICMP packets have a packet size of 74 bytes. The writer uses this quantity as a reference to determine the fuzzy set on the packet length variable. There are three classifications for the determined packet length variable: short packet length, normal packet length, and long packet length. If the total length of packets received in one interval is less than 74 bytes, then the packet length is classified as short. If the packet length is between 56 bytes and 84



bytes, the packet length is normal. However, if the packet length is more than 84 bytes, the packet length is relatively long.

3.2 SVM and Fuzzy Parameter Planning

SVM machine learning design To classify network traffic, machine learning requires training data that serves as the foundation for a learning model. Train data is generated by collecting traffic on the network that has been received. At this stage, a network traffic description is used to determine the type of traffic sent to the server. In this research, there are two categories of traffic: normal traffic and DDoS attack traffic as explained in the previous section, this research was conducted by collecting data to obtain training data from normal traffic and DDoS attack traffic. After that, a dataset will be generated that contains data from network traffic that has been extracted. Figure 4 is a machine learning design that is carried out to create a support vector machine model.



Figure 4. SVM flowcharts

Determining fuzzy parameters is carried out to meet the needs of calculations using the fuzzy method. Based on the Tsukamoto fuzzy flowchart in Figure 5, several parameters are input for the primary process of fuzzy calculations. In the fuzzification process, the input of fuzzy variable, fuzzy domains, and the x value of the variable to be searched is required to produce output in the form of the degree of membership of the x value. Variables and fuzzy domains are static, while the value of x is dynamic. The inference process requires input from fuzzy rules and membership degree values resulting from the fuzzification process to produce output in alpha predicate values and x values for each rule. Fuzzy rules are static, while membership degree values are dynamic. The final process, namely defuzzification, requires alpha predicate input and the x value of each rule from the results of the inference process to produce output in the form of classification results. Alphapredicate input is dynamic. Three parameters must be determined from static input: fuzzy variables, fuzzy domains, and fuzzy rules. Researchers determine three fuzzy variables based on network traffic capture results: packet length, number of packets received, and number of packet senders. Apart from fuzzy variables, other parameters that must be determined are domains and fuzzy rules. The method used to determine the domain in each variable is through discussions with network security experts and literature studies.



Figure 5. Fuzzy Tsukamoto Flow Chart



In contrast, IPV4 is included because, in some cases, the packet will be segmented if the data size of the ICMP packet sent is large. Segmented packets will be recognized as IPv4 protocols. The second step is to change the time for each packet in seconds. Packages captured using Wireshark will have a time in milliseconds. The reason for converting to seconds is that packets will be counted every one-second interval during the fuzzy algorithm's calculation process. The third stage is eliminating the destination IP address other than the server IP address. The goal is that the packets analyzed only go to the server's IP address. On the other hand, a packet containing the server IP address is cleaned for the source IP address, so the packet does not come from the server IP address. Figure 6 is the line of code in the preprocessing step:

```
path = "normaldata.csv"
df = pd.read_csv(path)
server_ip = "192.168.111.10"
df = df[df['protocol'].isin(['ICMP', 'IPV4'])]
df.Time = df.Time.astype(int)
df = df[df['Source'] != server_ip]
df = df[df['Destination'] == server_ip]
```

Figure 6. Data Preprocessing

3.3 Data Analysis

After the program has been created, the next step is to test it. Testing is done by scanning the data that has been obtained. The test was carried out 51 times, and 50 times the normal simulation data was scanned. Fifty times against DDoS simulation data and once against CAIDA data. This test uses a network topology consisting of one controller, two switches, and 30 hosts. The following are the detection results from all tests:

Table 2. DDOS Dataset Test Results

No	Data Type	Result
1	Normal Simulation 1	Normal Traffic
2	Normal Simulation 2	Normal Traffic
3	Normal Simulation 3	Normal Traffic
4	Normal Simulation 4	Normal Traffic
5	Normal Simulation 5	Normal Traffic
6	Normal Simulation 6	Normal Traffic
7	Normal Simulation 7	Normal Traffic
8	Normal Simulation 8	Normal Traffic
9	Normal Simulation 9	Normal Traffic
10	Normal Simulation 10	Normal Traffic
11	Normal Simulation 11	Normal Traffic
12	Normal Simulation 12	Normal Traffic
13	Normal Simulation 13	Normal Traffic
14	Normal Simulation 14	Normal Traffic
15	Normal Simulation 15	Normal Traffic
16	Normal Simulation 16	Normal Traffic
17	Normal Simulation 17	Normal Traffic
18	Normal Simulation 18	Normal Traffic
19	Normal Simulation 19	Normal Traffic
20	Normal Simulation 20	Normal Traffic
21	Normal Simulation 21	Normal Traffic
22	Normal Simulation 22	Normal Traffic
23	Normal Simulation 23	Normal Traffic
24	Normal Simulation 24	Normal Traffic
25	Normal Simulation 25	Normal Traffic
26	DDOS Simulation 1	DDOS Attack
27	DDOS Simulation 2	DDOS Attack
28	DDOS Simulation 3	DDOS Attack
29	DDOS Simulation 4	DDOS Attack
30	DDOS Simulation 5	DDOS Attack
31	DDOS Simulation 6	DDOS Attack
32	DDOS Simulation 7	DDOS Attack
33	DDOS Simulation 8	DDOS Attack
34	DDOS Simulation 9	DDOS Attack
35	DDOS Simulation 10	DDOS Attack



No	Data Type	Result
36	DDOS Simulation 11	DDOS Attack
37	DDOS Simulation 12	DDOS Attack
38	DDOS Simulation 13	DDOS Attack
39	DDOS Simulation 14	DDOS Attack
40	DDOS Simulation 15	DDOS Attack
41	DDOS Simulation 16	DDOS Attack
42	DDOS Simulation 17	DDOS Attack
43	DDOS Simulation 18	DDOS Attack
44	DDOS Simulation 19	DDOS Attack
45	DDOS Simulation 20	DDOS Attack
46	DDOS Simulation 21	DDOS Attack
47	DDOS Simulation 22	DDOS Attack
48	DDOS Simulation 23	DDOS Attack
49	DDOS Simulation 24	DDOS Attack
50	DDOS Simulation 25	DDOS Attack
51	Data Set CAIDA	DDOS Attack

From the test results above, it can be mapped into the confusion matrix mapping table as follows:

Tabel 3. Confusion Matrix

Prediction Actual	Normal Traffic	DDOS Attack
Normal Traffic	25	0
DDOS Attack	0	26

The normal simulation data detection results that are detected by normal traffic yield true positive values, while the DDOS and CAIDA simulation data that are detected by DDOS attack yield true negative values. The false positive value is obtained from the DDOS and CAIDA simulation data detection results detected by normal traffic. The false negative value is obtained from the normal simulation data detection results detected by a DDOS attack. So, the True Positive (TP) value is 20, the True Negative (TN) value is 21, the False Positive (FP) value is 0, and the False Negative (FN) value is 0. Then, from these results, the detection accuracy level can be calculated as follows:

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$accuracy = \frac{25 + 26}{25 + 26 + 0 + 0}$$

$$accuracy = \frac{51}{51}$$

$$accuracy = 1$$

From the calculation above, the detection accuracy level of the program that has been made is 100%. Testing the accuracy of DDoS attack detection aims to measure the system's accuracy in detecting DDoS attacks. A DDoS attack is carried out at this stage, namely a smurf attack. The experiment was carried out by sending the attack, and then the data from the attack was tested for accuracy using SVM and fuzzy machine learning. Table 3 is the result of testing the accuracy of DDoS attack detection.

Table 4. Machine Learning Test Results

Types of DDOS Attacks	Machine Learning	Level of accuracy
Smurf Attack	SVM	100%
Smurf Attack	Fuzzy Tsukamoto	100%

4. CONCLUSION

The DDOS smurf attack is tested by entering the DDOS attack data based on the conditions that exist in the running network. Then the dataset is assessed and processed using machine learning techniques such as SVM (support vector machines) and fuzzy Tsukamoto to obtain DDOS detection values. Based on the 51 test results, the detection results obtained were 25 normal data points without DDOS attacks and 25 DDOS attacks. This data was obtained through a real-time test attack against the networking system. One dataset was obtained through CAIDA 2007 data, and the result is that the data was detected as a DDOS attack. The level of accuracy resulting



from the program could detect the type of DDOS Ping of Death attack using the Tsukamoto fuzzy method and SVM is 100%. This can be seen from the confusion matrix mapping table, where the program can detect the actual class of the input data. The detection model relies on a reference dataset, which a learning process will then form a system that labels each packet that enters the networking system. Tsukamoto's fuzzy machine learning and SVM can classify network traffic data subjected to a DDOS attack by analyzing packet length, the number of packets, and a number of packet senders. The results of this study still need to be studied further because they are limited to three analyses: the packet length, the number of packets, and the number of packet senders: the fewer variables, the greater the level of accuracy. In future research, adding other variables that can be used to detect DDOS attacks and use other DDOS attack simulation scenarios would be better.

ACKNOWLEDGMENT

We would like to thank the Ministry of Research, Technology and Higher Education of the Republic of Indonesia (RISTEKDIKTI) for funding this research through the "skim Penelitian Dasar Pemula 2022" program.

REFERENCES

- [1] I. Lizarralde, C. Mateos, J. M. Rodriguez, and A. Zunino, "Exploiting named entity recognition for improving syntactic-based web service discovery," *J Inf Sci*, vol. 45, no. 3, 2019, doi: 10.1177/0165551518793321.
- [2] L. Jiang, Q. Xie, and L. Chen, "Application and Feasibility Study of Integrated Nursing Information Construction in Nephrology Nursing," *J Healthc Eng*, vol. 2022, 2022, doi: 10.1155/2022/7033840.
- [3] D. N. Aryani *et al.*, "Factors Influencing Consumer Behavioral Intention to Use Food Delivery Services: A Study of Foodpanda," *Journal of The Community Development in Asia*, vol. 5, no. 1, 2022.
- [4] F. Liang, L. Mu, D. Wang, and B. S. Kim, "A new model path for the development of smart leisure sports tourism industry based on 5G technology," *IET Communications*, vol. 16, no. 5, 2022, doi: 10.1049/cmu2.12271.
- [5] P. Tambare, C. Meshram, C. C. Lee, R. J. Ramteke, and A. L. Imoize, "Performance measurement system and quality management in data-driven industry 4.0: A review," *Sensors*, vol. 22, no. 1, 2022, doi: 10.3390/s22010224.
- [6] Z. Bezhovski, "The Future of the Mobile Payment as Electronic Payment System," *European Journal of Business and Management*, 2016.
- [7] M. C. Cohen, "Big Data and Service Operations," *Prod Oper Manag*, vol. 27, no. 9, 2018, doi: 10.1111/poms.12832.
- [8] M. Zolotukhin, T. Hamalainen, T. Kokkonen, and J. Siltanen, "Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic," in *2016 23rd International Conference on Telecommunications, ICT 2016*, 2016, doi: 10.1109/ICT.2016.7500408.
- [9] D. J. Prathyusha and G. Kannayaram, "A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment," *Evol Intell*, vol. 14, no. 2, 2021, doi: 10.1007/s12065-019-00340-4.
- [10] X. Zhang, O. Upton, N. L. Beebe, and K. K. R. Choo, "IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers," *Forensic Science International: Digital Investigation*, vol. 32, 2020, doi: 10.1016/j.fsidi.2020.300926.
- [11] P. K. Manadhata, S. Yadav, P. Rao, and W. Horne, "Detecting malicious domains via graph inference," in *Proceedings of the ACM Conference on Computer and Communications Security*, 2014, vol. 2014–November, no. November, doi: 10.1145/2666652.2666659.
- [12] Y. M. Alginahi and M. N. Kabir, *Authentication technologies for cloud computing, iot and big data*. 2019. doi: 10.1049/pbse009e.
- [13] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, and A. Patel, "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique," *Engineering Applications of Artificial Intelligence*, vol. 26, no. 9, 2013, doi: 10.1016/j.engappai.2013.04.010.
- [14] S. Sambangi and L. Gondii, "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression," 2020, doi: 10.3390/proceedings2020063051.
- [15] A. A. Sallam, M. N. Kabir, Y. M. Alginahi, A. Jamal, and T. K. Esmeel, "IDS for Improving DDoS Attack Recognition Based on Attack Profiles and Network Traffic Features," in *Proceedings - 2020 16th IEEE International Colloquium on Signal Processing and its Applications, CSPA 2020*, 2020, doi: 10.1109/CSPA48992.2020.9068679.
- [16] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali, "Towards a Universal Features Set for IoT Botnet Attacks Detection," in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, 2020, doi: 10.1109/INMIC50486.2020.9318106.
- [17] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, 2020, doi: 10.1109/INMIC50486.2020.9318216.
- [18] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, 2017, doi: 10.1007/s13369-017-2414-5.
- [19] H. Wang *et al.*, "DDoS Attack in Software Defined Networks: A Survey," *Neural Regen Res*, vol. 7, no. 14, 2017.
- [20] L. F. Eliyan and R. di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, 2021, doi: 10.1016/j.future.2021.03.011.
- [21] V. Deepa, K. Muthamil Sudar, and P. Deepalakshmi, "Detection of DDoS attack on SDN control plane using hybrid machine learning techniques," in *Proceedings of the International Conference on Smart Systems and Inventive Technology, ICSSIT 2018*, 2018, doi: 10.1109/ICSSIT.2018.8748836.
- [22] L. Yang and H. Zhao, "DDoS attack identification and defense using SDN based on machine learning method," in *Proceedings - 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018*, 2019, doi: 10.1109/I-SPAN.2018.00036.

JURNAL MEDIA INFORMATIKA BUDIDARMA

Volume 7, Nomor 1, Januari 2023, Page 66-73

ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)

Available Online at <https://ejournal.stmik-budidarma.ac.id/index.php/mib>

DOI: 10.30865/mib.v7i1.5199



- [23] M. Revathi, V. v. Ramalingam, and B. Amutha, "A Machine Learning Based Detection and Mitigation of the DDOS Attack by Using SDN Controller Framework," *Wirel Pers Commun*, 2021, doi: 10.1007/s11277-021-09071-1.
- [24] R. T. Kokila, S. Thamarai 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*, 2015, doi: 10.1109/ICoAC.2014.7229711.
- [25] Q. Niyaz, W. Sun, and A. Y. Javaid, "A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)," *ICST Transactions on Security and Safety*, vol. 4, no. 12, 2017, doi: 10.4108/eai.28-12-2017.153515.
- [26] G. de La Torre Parra, P. Rad, K. K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *Journal of Network and Computer Applications*, vol. 163, Aug. 2020, doi: 10.1016/j.jnca.2020.102662.

Paper Analysis of Distributed Denial of Service Attacks Using Support Vector Machine and Fuzzy Tsukamoto

ORIGINALITY REPORT

13%

SIMILARITY INDEX

8%

INTERNET SOURCES

10%

PUBLICATIONS

2%

STUDENT PAPERS

PRIMARY SOURCES

1	docshare.tips Internet Source	1%
2	www.diva-portal.org Internet Source	1%
3	Mona Alduailij, Qazi Waqas Khan, Muhammad Tahir, Muhammad Sardaraz, Mai Alduailij, Fazila Malik. "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method", Symmetry, 2022 Publication	1%
4	jurnal.iaii.or.id Internet Source	1%
5	Heru Nurwarsito, Muhammad Fahmy Nadhif. "DDoS Attack Early Detection and Mitigation System on SDN using Random Forest Algorithm and Ryu Framework", 2021 8th International Conference on Computer and Communication Engineering (ICCCE), 2021 Publication	1%

6	www.mdpi.com Internet Source	1 %
7	A Junaidi, C Kartiko. "Design of Pond Water Quality Monitoring System Based on Internet of Things and Pond Fish Market in Real-Time to Support the Industrial Revolution 4.0", IOP Conference Series: Materials Science and Engineering, 2020 Publication	1 %
8	Radosław Olgierd Schoeneich, Piotr Sadło. "Delay Tolerant Networks over Near Field Communications: The Automatic Multi-packet Communication", International Journal of Computers Communications & Control, 2017 Publication	<1 %
9	Lecture Notes in Computer Science, 2002. Publication	<1 %
10	ojs3.unpatti.ac.id Internet Source	<1 %
11	www.hindawi.com Internet Source	<1 %
12	apps.dtic.mil Internet Source	<1 %
13	"Computational Science and Technology", Springer Science and Business Media LLC, 2018 Publication	<1 %

14

Hassan A. Alamri, Vijey Thayananthan.
"Bandwidth Control Mechanism and Extreme
Gradient Boosting Algorithm for Protecting
Software-Defined Networks Against DDoS
Attacks", IEEE Access, 2020

Publication

<1 %

15

www.techscience.com

Internet Source

<1 %

16

Zahiriddin Rustamov, Jaloliddin Rustamov,
Nazar Zaki, Sherzod Turaev, Most Sarmin
Sultana, Jeanne Ywei Tan, Vimala
Balakrishnan. "Enhancing Cardiovascular
Disease Prediction: A Domain Knowledge-
Based Feature Selection and Stacked
Ensemble Machine Learning Approach",
Research Square Platform LLC, 2023

Publication

<1 %

17

R. B. Harithaa, M. Vijayalakshmi. "Chapter 57
DDoS Attack Using Machine Learning: A Brief
Survey", Springer Science and Business Media
LLC, 2023

Publication

<1 %

18

link.springer.com

Internet Source

<1 %

19

mau.diva-portal.org

Internet Source

<1 %

20	porto.polito.it Internet Source	<1 %
21	www.datasheet.hk Internet Source	<1 %
22	"A Hybrid Defense Technique for ISP Against the Distributed Denial of Service Attacks", 'Deanship of Scientific Research' Internet Source	<1 %
23	"Authentication Technologies for Cloud Computing, IoT and Big Data", Institution of Engineering and Technology (IET), 2019 Publication	<1 %
24	"Intelligent Computing Theories and Application", Springer Science and Business Media LLC, 2020 Publication	<1 %
25	Ahamed Aljuhani. "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments", IEEE Access, 2021 Publication	<1 %
26	Encyclopedia of Complexity and Systems Science, 2009. Publication	<1 %
27	assets.researchsquare.com Internet Source	<1 %

28

J Hendry, W Pamungkas, A F Isnawati. "V2V Channel Performance on VANET Technology with OFDM and Moving Scatterer's Influence", Journal of Physics: Conference Series, 2019

Publication

<1 %

29

Sajal Bhatia, Desmond Schmidt, George Mohay. "Ensemble-based DDoS detection and mitigation model", Proceedings of the Fifth International Conference on Security of Information and Networks - SIN '12, 2012

Publication

<1 %

30

Hossein Ahmadvand, Chhagan Lal, Hadi Hemmati, Mehdi Sookhak, Mauro Conti. "Privacy-Preserving and Security in SDN-Based IoT: A Survey", IEEE Access, 2023

Publication

<1 %

Exclude quotes

Off

Exclude matches

Off

Exclude bibliography

Off