Institute of Research and Publication Indonesia
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 1 Iss. 2 October 2021, pp: 144-154
P-ISSN: 2797-2313 ISSN(E): 2775-8575

Detection Distributed Denial of Service (DDoS) Using Sugeno's Fuzzy Logic

Deteksi Distributed Denial of Service (DDoS) Menggunakan Fuzzy Logic Sugeno

Hartanto Tantriawan[1]*, Rajif Agung Yunmar[2], Andhika Setiawan[3], Meiji Suryadi[4]

[1,2,3,4] Prodi Teknik Informatika, Jurusan Teknologi Produksi dan Industri
Institut Teknologi Sumatera

E-Mail: [1]hartanto.tantriawan@if.itera.ac.id , [2]rajif@if.itera.ac.id,
[3]andika.setiawan@if.itera.ac.id, [4]meijisuryadi1998@gmail.com

Received Jun 2nd 2021; Revised Jun 27th 2021; Accepted Aug 3rd 2021
Corresponding Author: Hartanto Tantriawan

Abstract

The Industrial Revolution 4.0 brings a new era of information technology. In this era, information becomes very easy to obtain on the internet. However, the development of internet technology also harms the development of internet crime. Distributed Denial of Service (DDOS) is one example of corruption in cyberspace. DDOS attackers is flooding the target website with so much data that the website cannot serve requests from real users. Therefore, we carried out this research on DDOS detection using fuzzy logic algorithms. This research was conducted by analyzing network traffic using Wireshark. Traffic data was processed using Sugeno's Fuzzy Logic to see whether the spell belongs to DDOS. The results of detection research using Sugeno fuzzy logic could detect DDoS attacks by 70%.

Keyword: Distributed Denial of Service (DDoS), Fuzzy Logic Sugeno, Matlab, Wireshark.

Abstrak

Revolusi Industri 4.0 membawa era baru teknologi informasi. Pada era ini, informasi menjadi sangat mudah didapatkan di internet. Namun demikian perkembangan teknologi internet juga membawa dampak buruk dengan berkembangnya kejahatan internet. Salah satu kejahatan internet adalah *Distributed Denial of Service*(DDOS). Penyerang DDOS membanjiri website target dengan data yang banyak sehingga website tersebut tidak mampu melayani permintaan dari pengguna asli. Oleh karena itu penelitian deteksi DDOS menggunakan algoritma *fuzzy logic* ini kami lakukan. Penelitian ini dilakukan dengan menganalisis lalu lintas jaringan menggunakan *Wireshark.* Data lalu lintas di olah menggunakan Fuzzy Logic Sugeno agar dapat di deteksi apakah serangan tersebut termasuk ke dalam DDOS. Hasil penelitian deteksi menggunakan fuzzy logic sugeno mampu mendeteksi serangan DDoS sebesar 70 %..

Kata Kunci: Distributed Denial of Service (DDoS), Logika Fuzzy Sugeno, Matlab, Wireshark.

1. PENDAHULUAN

Sampai saat ini, Internet adalah salah satu teknologi yang paling populer. Mampu mencari berbagai informasi dalam sebuah website merupakan salah satu keunggulan dari internet. Website adalah sebuah sistem di mana informasi berupa teks HTML, gambar, dan audio. File yang diminta dalam format HTML dibalas oleh server melalui browser [1]. Untuk mengakses ini, pengguna membuat permintaan ke situs web yang membutuhkan respons dari server, yang biasa disebut sebagai server web [2].

Di dunia teknologi, kejahatan internet meningkat pesat. Penjahat (penyerang) membuat lalu lintas jaringan menjadi anomali dengan membanjiri server web dengan data dalam jumlah besar. Ini dikenal sebagai serangan penolakan *Deteksi Distributed Denial of Service* (DDoS). Serangan ini menyebabkan kegagalan server karena ia menerima banyak permintaan dalam waktu singkat [2]. Dalam banyak kasus, serangan DDoS tidak diketahui oleh korban. Banjir SYN adalah salah satu metode melakukan serangan DDoS. Banjir SYN adalah salah satu paket yang paling sulit dideteksi dalam lalu lintas jaringan [3]. Karena SYN flood, host terus menunggu paket dengan menyimpannya di backlog [4].

User Diagram Protocol (UDP) flood bekerja dengan membanjiri host jarak jauh secara acak. Sumber daya pada host akan bermasalah (error) karena banjir UDP, membuat situs web menjadi tidak dapat diakses [4]. Logika fuzzy, sebuah teknologi komputasi lunak, dapat digunakan untuk mendeteksi serangan DDoS yang kompleks [5]. Soft computing sendiri disebut sebagai sistem yang memiliki keahlian seperti manusia dan dapat belajar serta beradaptasi dengan lingkungan [6].

Wireshark digunakan untuk merekam aktivitas dari jaringan. Software ini bekerja dengan cara menangkap semua paket yang melewati jaringan dan menampilkan datanya. *Low Orbit Ion Cannon* (LOIC) digunakan dalam proses simulasi serangan DDoS, dimana aplikasi ini digunakan dalam melakukan serangan DDoS berupa *Internet Control Message Protocol* (ICMP), *Transmission Control Protocol* (TCP), dan *User Data Protocol* (UDP) [7]. Serangan LOIC dengan port, *Internet Protocol* (IP), metode (methods) dan ancaman (threat) [8]. Kemudian MATLAB digunakan untuk proses logika fuzzy. MATLAB merupakan salah satu software untuk pembelajaran linier [9].

Penelitian Indra Wahyu Nugroho berjudul "Rancang Bangun Aplikasi Intrussion Detection System (IDS) dengan menggunakan Metode Fuzzy " menjelaskan bahwa metode fuzzy berperan dalam mendeteksi spesifisitas aktivitas jaringan [10]. Logika fuzzy merupakan salah satu bentuk soft computing, yaitu suatu sistem yang memiliki kemampuan seperti manusia dan belajar serta beradaptasi dengan perubahan lingkungan [11]. Pada tahun 2020, penelitian yang dilakukan oleh Nadila Sugianti berjudul Deteksi serangan DDoS berbasis *Hypertext Transfer Protocol* (HTTP) menggunakan logika fuzzy Sugeno berhasil mengembangkan sistem yang dapat mendeteksi serangan DDoS berbasis HTTP dengan akurasi 90% [2].

Maka dari itu untuk mengurangi permasalahan diatas, dilakukan lah penelitian ini yang mana nantinya mampu mendeteksi serangan – serangan yang akan dilakukan terhadap web dari user sehingga dapat melakukan pemcegahan sebelum menjadi sulit untuk ditangani.

2. BAHAN DAN METODE

Metode penelitian terdiri dari tahap perancangan hingga tahap pelaksanaan penelitian. Penelitian ini dibagi menjadi beberapa tahap berikut:

2.1 Tahapan Penelitian

Gambar 1. Tahapan Penelitian

Gambar 1 menggambarkan proses penelitian secara terurut. Tahap pertama adalah studi literatur terkait penelitian (DDoS dan Fuzzy Logic). Tahap selanjutnya adalah mendapatkan sampel data. Sampel data didapatkan melalui simulasi serangan DDoS. Hasil simulasi serangan DDoS terdapat log aktivitas jaringan yang dapat digunakan sebagai data penelitian. Kemudian data penelitian tersebut akan di kelompokan dan diolah menggunakan fuzzy logic sugeno. Langkah terakhir adalah analisis. Analisa dilakukan untuk mengetahui apakah aktivitas tersebut adalah aktivitas illegal yang berasal dari *botnet* ataupun *attacker* atau bukan merupakan aktivitas legal yang bukan bagian dari botnet (DDoS) [2].

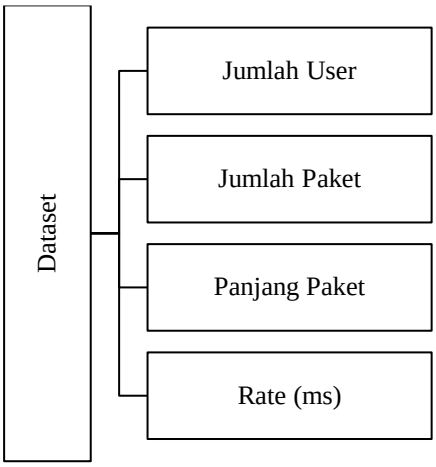
2.2 Pengambilan Sampel Data

Selama rentang sepuluh detik akan diambil sebanyak sepuluh data. Pengambilan data akan di iterasi sebanyak sepuluh kali. Simulasi akan dilakukan dengan tiga kali lalu lintas normal serta tujuh kali menggunakan serangan DDoS. Data yang di dapat akan dibedakan berdasarkan empat variabel input, yaitu jumlah paket, jumlah user, panjang paket, dan rate (ms). Pembagian variable dataset terdapat pada Gambar 2.

Semesta pembicara dari masing – masing variable yang sudah di dapatkan di sajikan pada Tabel 1.

Tabel 1. Semesta Pembicara

Fungsi	Variabel	Semesta Pembicara
Input	Jumlah User	[0 – 12]
	Pajang Paket	[0 – 5120]
	Rate (ms)	[0 – 4]
	Jumlah Paket	[0 – 32000]
Output	Status	[0 - 1]



Gambar 2. Sampel Data

Tabel 2. Data Uji

No	Jumlah User	Panjang Paket	Rate (ms)	Jumlah Paket	Status
1	3	1143	0.216	2015	Normal
2	3	318	0.012	127	Normal
3	10	307	0.011	103	Normal
4	10	799	0.888	7304	DDoS
5	9	830	1.032	8784	DDoS
6	6	745	1.672	13620	DDoS
7	6	722	0.830	8514	DDoS
8	6	754	1.634	15076	DDoS
9	4	743	3.056	31138	DDoS
10	11	735	2.636	27487	DDoS

Simulasi serangan dilakukan menggunakan tiga data normal dan tujuh data DDoS, sehingga diperoleh data uji seperti yang ditampilkan pada Tabel 2.

2.3 Pengolahan dan Pengelompokkan Data

Berdasarkan data yang sudah di ambil, data akan diolah dan dikelompokkan menggunakan fuzzy logic sugeno. Perhitungan fuzzy serta penentuan fungsi keanggotaan bimpunan fuzzy dan de-fuzzy-fikasi dihitung menggunakan software MATLAB.

Proses logika fuzzy digambarkan dengan flowchart seperti pada Gambar 3. Data sampel berupa jumlah paket, jumlah pengguna, panjang paket dan rate/ms yang diperoleh aplikasi Wireshark dimasukkan satu per satu. Tetapkan fungsi keanggotaan ke nilai antara batas atas dan bawah dari variabel input yang ada. Jenis fungsi keanggotaan fuzzy meliputi linier ke bawah, linier ke atas, trapesium, dan segitiga. Dalam penelitian ini, penulis menggunakan fungsi keanggotaan himpunan fuzzy segitiga.

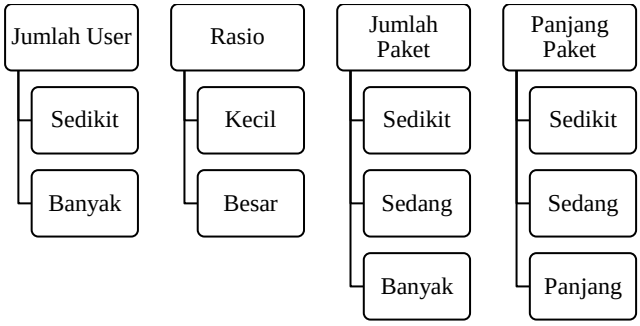
$$\mu(x) = \begin{cases} 0 & ; x \leq a \; atau \; x \geq c \\ \frac{(x-a)}{(b-a)} & ; a \leq x \leq b \\ \frac{(c-x)}{(c-b)} & ; b \leq x \leq c \end{cases} \quad (1)$$

Berdasarkan variabel input, tahap penentuan rule menggunakan aturan berbasis if-then. Proses de-fuzzy-fikasi didapatkan dari menghitung nilai rata-rata yang diperoleh dari rule. Output de-fuzzy-fikasi merupakan nilai 1 (sebagai data yang berupa serangan DDoS) atau 0 (sebagai data yang dianggap bukan serangan DDoS). Hasil data yang diperoleh ditampilkan sebagai nilai akhir dengan satuan persen (%).

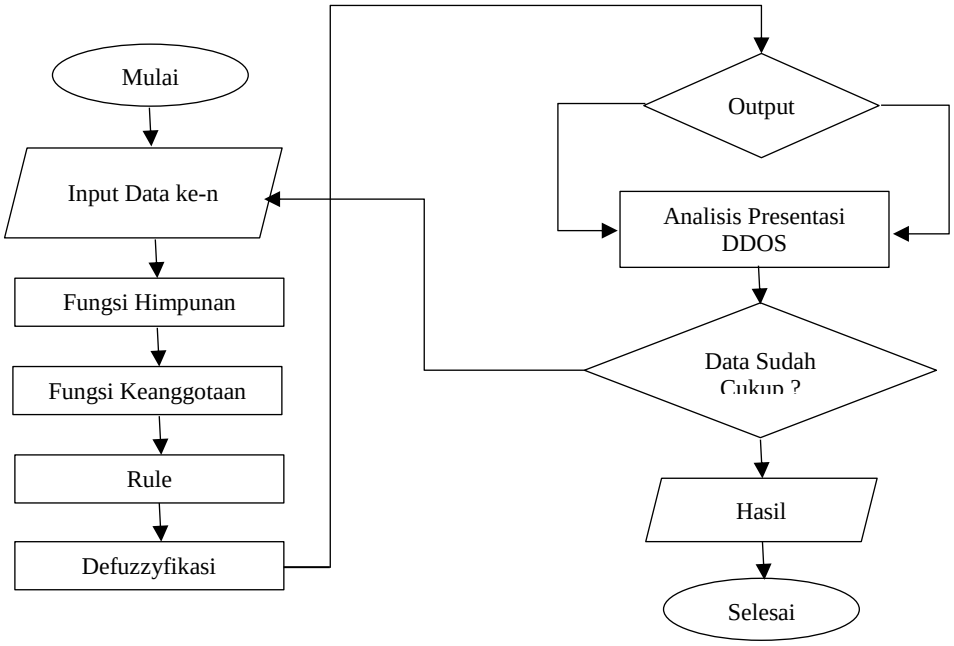
2.3.1 Tahap Fuzzy-fikasi

Tahap fuzzy-fikasi adalah tahap mengelompokkan nilai variable jumlah paket, jumlah user, panjang paket, dan rate (ms) menjadi beberapa kelompok. Pada Gambar 4 menjelaskan proses fuzzy-fikasi. Variable jumlah paket terbagi menjadi tiga kategori: sedikit, sedang, dan banyak. Variable jumlah user terbagi dalam dua kategori: sedikit dan banyak. Variable rate dapat dibagi menjadi dua kategori: kecil dan besar. Variable panjang paket dapat dibagi menjadi tiga jenis: sedikit, sedang, panjang. Kemudian setiap kategori

dikategorikan ke dalam nilai domain. Hal ini ditunjukkan pada Tabel 3. Pembentukan variable fuzzy memiliki nilai semesta pembicara dari nilai yang minimum hingga maksimum [6].



Gambar 4. Proses Fuzzy-fikasi



Gambar 3. Flowchart Fuzzy

Tabel 3. Himpunan Fuzzy

Fungsi	Variabel	Himpunan	Nilai Domain
Input	Jumlah User	Sedikit	[0 – 6]
		Banyak	[5 – 12]
	Pajang Paket	Sedikit	[0 – 1700]
		Sedang	[1500 – 3400]
		Panjang	[3200 – 5120]
	Rate (ms)	Kecil	[0 – 2.25]
		Besar	[1.75 – 4]
	Jumlah Paket	Sedikit	[0 – 1000]
		Sedang	[500 – 10000]
		Banyak	[5000 – 32000]
Output	Status	Normal	[0]
		DDOS Ringan	[0.1-0.99]
		DDoS	[1]

2.3.2. Tahap Inferensi

Pada tahap inferensi, proses pencarian nilai keanggotaan dari setiap variabel input ke variabel output dilakukan dengan menggunakan fungsi implikasi MIN. Hal ini bertujuan untuk mendapatkan nilai α – predikat dari setiap rule. Nilai α – predikat tersebut digunakan untuk menghitung output dari hasil inferensi.

2.3.3. Tahap De-fuzzy-fikasi

Pada metode fuzzy logic sugeno, tahap de-fuzzy-fikasi dihitung dengan fungsi rata-rata (Weight Average) seperti pada persamaan (2).

$$Z = \frac{\sum \alpha_i z_i}{\sum \alpha_i} \quad (2)$$

2.3.4. Rule Based

Fase ini membuat rule fuzzy yang digunakan untuk mendeteksi serangan DDoS. Rule Based dibuat berdasarkan jumlah data yang diperoleh dari proses simulasi yang dilakukan. Jumlah rule yang digunakan adalah 36, seperti yang disajikan pada Tabel 4.

Tabel 4. Rule Based

No Aturan	Variable Input	Variable Output
R1	Jika [[Jumlah_User = Sedikit] dan [Panjang_Paket = Sedikit] dan [Rate = Kecil] dan [Jumlah_Paket = Sedikit]]	Bukan DDoS
R9	Jika [[Jumlah_User = Sedikit] dan [Panjang_Paket = Sedang] dan [Rate = Besar] dan [Jumlah_Paket = Sedikit]]	Bukan DDoS
R21	Jika [[Jumlah_User = Sedikit] dan [Panjang _Paket = Panjang] dan [Rate = Besar] dan [Jumlah_Paket = Banyak]]	DDoS
.	.	.
.	.	.
.	.	.
R36	Jika [[Jumlah_User = Banyak] dan [Panjang_Paket = Panjang] dan [Rate = Besar] dan [Jumlah_Paket = Banyak]]	DDoS

3. IMPLEMENTASI DAN PENGUJIAN

3.1. Implementasi Data

Pada penelitian ini, nilai keanggotaan dihitung menggunakan metode fuzzy logic sugeno. Data yang digunakan dalam uraian ini berasal dari proses simulasi serangan DDoS yang diambil menggunakan aplikasi wireshark.

3.1.1. Fuzzy-fikasi

Pada subbagian ini, dilakukan proses fuzzy-fikasi terhadap variable input: jumlah user, jumlah paket, panjang paket, rate. Fungsi kurva segitiga digunakan untuk memperoleh fungsi keanggotaan setiap variable input, sebagai berikut:

a) Fungsi Keanggotaaan Jumlah *User*

Fungsi keanggotaan himpunan *fuzzy* pada *variable* Jumlah *User* adalah: sedikit dan banyak.

$$\mu\text{Sedikit} = \begin{cases} 0 & ; x \leq 0 \; atau \; x \geq 6 \\ \frac{(x-0)}{(3-0)} & ; 0 \leq x \leq 3 \\ \frac{(6-x)}{(6-3)} & ; 3 \leq x \leq 6 \end{cases} \quad (3)$$

$$\mu\text{Banyak} = \begin{cases} 0 & ; x \leq 5 \; atau \; \geq 12 \\ \frac{(x-5)}{(8-5)} & ; 5 \leq x \leq 8 \\ \frac{(12-x)}{(12-8)} & ; 8 \leq x \leq 12 \end{cases} \quad (4)$$

b) Fungsi Keanggotaaan Panjang Paket

Variabel panjang paket memiliki fungsi keanggotaan himpunan *fuzzy* sebagai berikut: Sedikit, Sedang, Panjang.

$$\mu\text{Sedikit} = \begin{cases} 0 & ; x \leq 0 \; atau \; \geq 1700 \\ \frac{(x-0)}{(850-0)} & ; 0 \leq x \leq 850 \\ \frac{(1700-x)}{(1700-850)} & ; 850 \leq x \leq 1700 \end{cases} \quad (5)$$

$$\mu\text{Sedang} = \begin{cases} 0 & ; x \leq 1500 \; atau \; x \geq 3400 \\ \frac{(x-1500)}{(2450-1500)} & ; 1500 \leq x \leq 2450 \\ \frac{(3400-x)}{(3400-2450)} & ; 2450 \leq x \leq 3400 \end{cases} \quad (6)$$

$$\mu\text{Panjang} = \begin{cases} 0 & ; x \leq 3200 \; atau \; x \geq 5120 \\ \frac{(x-3200)}{(4160-3200)} & ; 3200 \leq x \leq 4160 \\ \frac{(5120-x)}{(5120-4160)} & ; 4160 \leq x \leq 5120 \end{cases} \quad (7)$$

Berdasarkan fungsi keanggotaan dari empat variabel maka diperoleh derajat keanggotaan setiap variable seperti pada tabel berikut:

a. Jumlah *User*

Derajat keanggotaan yang didapatkan berdasarkan fungsi keanggotaan dari variable jumlah *user* disajikan pada Tabel 5.

Tabel 5. Derajat Keanggotaan Jumlah *User*

Data ke-	Jumlah User	
	Sedikit	Banyak
1	1	0
2	1	0
3	0	0.5
4	0	0.5
5	0	0.75
6	0	0.333333
7	0	0.333333
8	0	0.333333
9	0.6666667	0
10	0	0.25

b. Panjang Paket

Derajat keanggotaan yang didapatkan berdasarkan fungsi keanggotaan dari variable panjang paket dapat diperhatikan pada Tabel 6.

Tabel 6. Derajat Keanggotaan Panjang Paket

Data ke-	Panjang Paket		
	Sedikit	Sedang	Panjang
1	0.655294	0	0
2	0.374118	0	0
3	0.361176	0	0
4	0.94	0	0
5	0.976471	0	0
6	0.876471	0	0
7	0.849412	0	0
8	0.887059	0	0
9	0.874118	0	0
10	0.864706	0	0

Hal sama dilakukan pada variable rate dan jumlah paket.

3.1.2. Inferensi

Pada subbab ini dilakukan inferensi menggunakan metode Sugeno Orde-0, yang mana hasil akan berupa konstanta [0 1]. Berdasarkan dataset hasil simulasi serangan DDoS berikut adalah proses inferensi metode Sugeno Orde-0.

Data ke-1

α – predikat R = μSedikit_U ∩ μSedikit_P ∩ μKecil_R ∩ μSedikit_J
= MIN {μSedikit_U [3], μSedikit_P[1143], μKecil_R[0,216], μSedikit_J [2015]}
= MIN {1; 0,655294; 0,192; 0}
= 0

Berdasarkan perhitungan di atas, maka didapatkan nilai MIN (α-predikat) masing – masing Rule yang dapat dilihat pada Tabel 7.

Tabel 7. α-predikat Data ke-1

Data ke-	Jumlah User	Panjang Paket	Rate	Jumlah Paket	OUTPUT (z1)	MIN (α_1)
1	1	0.655294	0.192	0	0	0
2	1	0.655294	0.192	0.3367	0	0.192
3	1	0.655294	0.192	0	0	0
4	1	0.655294	0	0	0	0
5	1	0.655294	0	0.3367	0	0
6	1	0.655294	0	0	1	0
7	1	0	0.192	0	0	0
8	1	0	0.192	0.3367	0	0
9	1	0	0.192	0	0	0
10	1	0	0	0	0	0
11	1	0	0	0.3367	1	0
12	1	0	0	0	1	0
13	1	0	0.192	0	0	0
14	1	0	0.192	0.3367	0	0
15	1	0	0.192	0	1	0
16	1	0	0	0	1	0
17	1	0	0	0.3367	1	0
18	1	0	0	0	1	0
19	0	0.655294	0.192	0	0	0
20	0	0.655294	0.192	0.3367	0	0
21	0	0.655294	0.192	0	1	0
22	0	0.655294	0	0	1	0
23	0	0.655294	0	0.3367	1	0
24	0	0.655294	0	0	1	0
25	0	0	0.192	0	0	0
26	0	0	0.192	0.3367	1	0
27	0	0	0.192	0	1	0
28	0	0	0	0	1	0
29	0	0	0	0.3367	1	0
30	0	0	0	0	1	0
31	0	0	0.192	0	1	0
32	0	0	0.192	0.3367	1	0
33	0	0	0.192	0	1	0
34	0	0	0	0	1	0
35	0	0	0	0.3367	1	0
36	0	0	0	0	1	0
			Jumlah			0.192

Dari perhitungan fuzzy-fikasi yang dilakukan terhadap semua data, maka didapat hasil jumlah α-predikat pada tiap data dijasikan pada Tabel 8.

Tabel 8. α-predikat Seluruh Data

Data ke-	1	2	3	4	5	6	7	8	9	10
α-predikat	0.1920	0.1066	0.0097	0.6706	0.5234	0.3333	0.5574	0.3333	0.6385	0.2500

3.1.3. Defuzzy-fikasi

Metode yang dipakai dalam proses de-fuzzy-fikasi (sugeno) adalah *Weighted Average* yang mana aturan α-predikat yang dipakai adalah yang tidak sama dengan nol.

$$Z = \frac{\sum(z1*\alpha1)}{\sum\alpha1} \quad (8)$$

$$= \frac{0}{0.192} = 0$$

Berdasarkan perhitungan de-fuzzy-fikasi, maka di dapatkan nilai Z pada tiap – tiap data adalah yang disajikan pada Tabel 9:

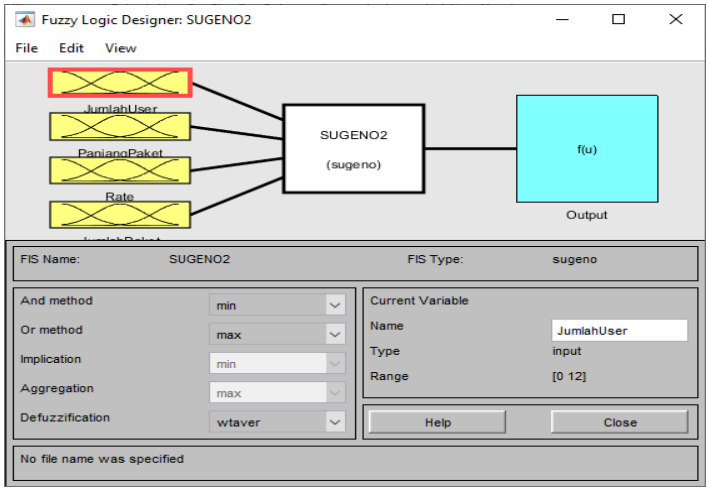
Tabel 9. De-fuzzy-fikasi (Z) Seluruh Data

Data	Data I	Data II	Data III	Data IV	Data V	Data VI	Data VII	Data VIII	Data IX	Data X
z	0	0	0	0.254	0.535	1	0.466	1	1	1

3.2 Implementasi pada Matlab

Proses perhitungan fuzzy sugeno dapat dilakukan menggunakan bantuan library yang telah disediakan oleh aplikasi MATLAB. Tahap ini akan dilakukan fuzzy-fikasi dan penentuan rule base berdasarkan apa yang telah penulis tentukan sebelumnya.

Proses dimulai dengan menambahkan variable input dan variable output serta merubah nama variable sesuai dengan yang telah penulis tentukan sebelumnya. Kemudian ubah "And Method" menjadi "MIN" untuk proses inferensi berikutnya. Hal ini dapat lebih jelas dilihat pada Gambar 5.



Gambar 5. Variable Input dan Output

3.2.1. Fuzzy-fikasi

Proses fuzzy-fikasi pada aplikasi matlab sama dengan proses fuzzy-fikasi yang telah dilakukan sebelumnya dengan mengelompokan variable – variable menjadi beberapa himpunan.

a. Jumlah User

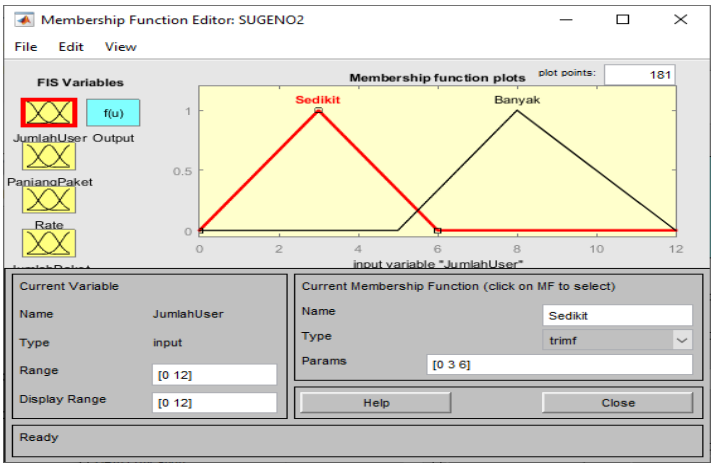
Gambar 6 menjelaskan bahwa variable jumlah user menggunakan dua himpunan: sedikit dan banyak. Maka ubah nama himpunan sesuai yang telah ditentukan kemudian masukan parameter masing-masing himpunan. Dengan parameter sedikit yaitu [0 3 6] dan banyak [5 8 12]. Ubah juga range dari variable menjadi [0 12].

b. Panjang Paket

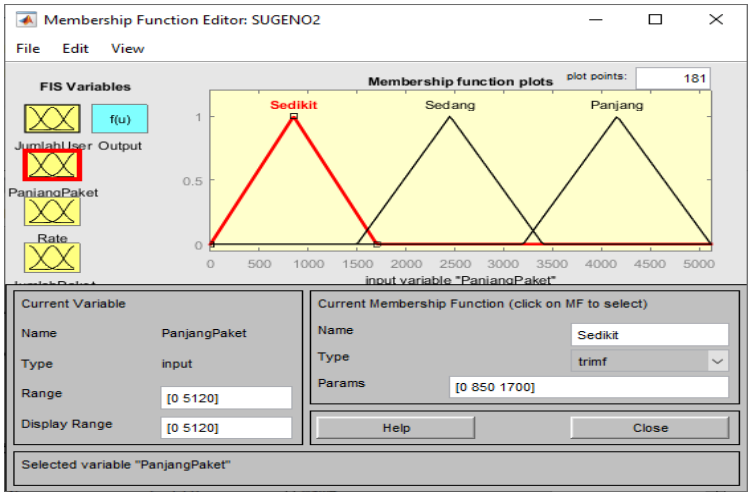
Gambar 7 menjelaskan bahwa variable panjang paket menggunakan 3 himpunan yaitu sedikit, sedang, dan banyak. Maka ubah nama himpunan sesuai yang telah ditentukan kemudian masukan parameter masing – masing himpunan. Dengan parameter sedikit yaitu [0 850 1700], sedang [1500 2450 3400] dan panjang [3200 4160 5120]. Ubah juga range dari variable menjadi [0 5120].

3.2.2. Rule Based

Pada tahapan ini penulis memasukan aturan – aturan yang sebelumnya telah dibuat pada Tabel 4 kedalam aplikasi MATLAB. Untuk lebih jelas rule base yang telah di buat pada aplikasi MATLAB dapat dilhat pada Gambar 8. Berdasarkan hasil yang didapatkan pada aplikasi MATLAB diatas, maka didapatkan hasil pada masing–masing data yang disajikan pada Tabel 10.



Gambar 6. Fuzzy-fikasi Jumlah User



Gambar 7. Fuzzy-fikasi Panjang Paket

Hal yang sama dilakukan pada variable Rate dan Jumlah Paket

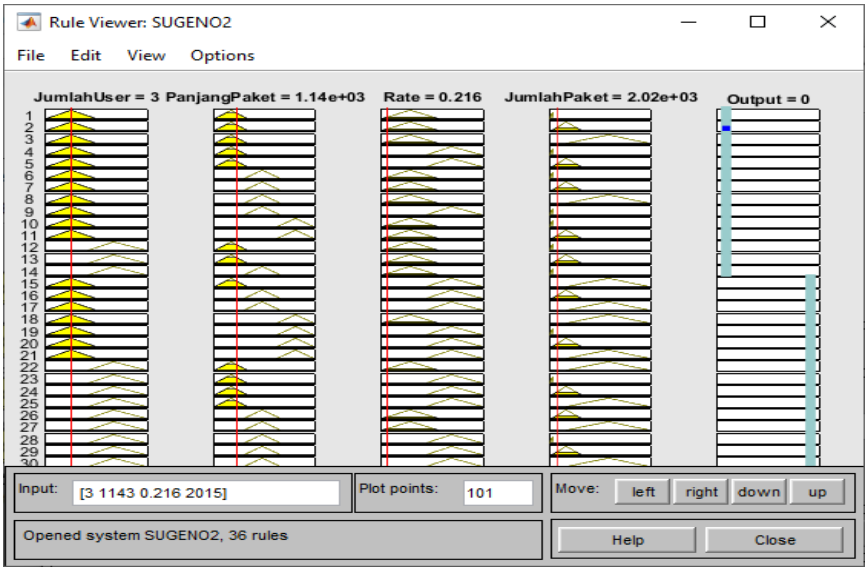
Tabel 10. Hasil Uji

Data	Data Uji	Matlab	Hasil
Data ke-1	Normal	Normal	Sesuai
Data ke-2	Normal	Normal	Sesuai
Data ke-3	Normal	Normal	Sesuai
Data ke-4	DDoS	DDOS Ringan	Tidak Sesuai
Data ke-5	DDoS	DDoS Ringan	Tidak Sesuai
Data ke-6	DDoS	DDoS	Sesuai
Data ke-7	DDoS	DDoS Ringan	Tidak Sesuai
Data ke-8	DDoS	DDoS	Sesuai
Data ke-9	DDoS	DDoS	Sesuai
Data ke-10	DDoS	DDoS	Sesuai

Berdasarkan Tabel 10, dari sepuluh data yang digunakan sebagai data uji didapatkan hasil tujuh data berhasil dideteksi dengan benar dan tiga tidak benar dengan konstanta yang telah ditentukan sebelumnya. Dengan menggunakan persamaan (9)

$$Tingkat\ Keakuratan\ = \frac{Jumlah\ Data\ Benar}{Jumlah\ Data\ Keseluruha\ n} \times 100\% \quad (9)$$

maka didapatkan tingkat keakuratan fuzzy logic sugeno dalam penelitian ini adalah 70 % dengan error sebesar 30%.



Gambar 8. Rule Base pada Aplikasi Matlab

4. KESIMPULAN

Penelitian ini dapat melakukan identifikasi terhadapat lalu lintas yang normal dan tidak normal berdasarkan variable jumlah user, panjang paket, rate, dan jumlah paket. Penelitian ini dapat mendeteksi serangan DDoS secara akurat menggunakan fuzzy logic sugeno dengan tingkat keakuratan 70% menggunakan aplikasi MATLAB dan 70% menggunakan perhitungan manual. Proses fuzzy-fikasi dan penetapan rule based akan menentukan hasil akhir dari keluaran nilai konstanta. Nilai de-fuzzy-fikasi yang di dapat diantara nilai 0 dan 1 akan masuk kedalam output DDoS Ringan. Saran yang bisa penulis berikan untuk penelitian berikutnya adalah penggunaan data uji yang lebih banyak agar mendapatkan hasil yang lebih rinci. Proses pengujian dapat menggunakan atau menambahkan parameter lain agar mendapat hasil yang lebih maksimal. Menambahkan proses mitigasi atau penyelesaian masalah terhadap data yang sudah terdeteksi sebagai DDoS. Menggunakan sumber dan pengkajian yang lebih mendalam untuk penentuan rule based nya.

5. PENGHARGAAN

Penulis mengucapkan terima kasih kepada Institut Teknologi Sumatera atas bantuan dana penelitian ini melalui Program Hibah Penelitian ITERA Smart 2019 dengan nomor kontrak B/321/IT9.C1/PT.01.03/ 2019.

REFERENSI

[1] P. A. Nugraha, M. A. Irwansyah, and H. Priyanto, “Rancang Bangun Web Server Berbasis Linux Dengan Metode Load Balancing (Studi Kasus : Laboratorium Teknik Informatika),” vol. 3, no. 1, pp. 1–5, 2016.

[2] N. Sugianti, Y. Galuh, S. Fatia, and K. F. H. Holle, “Deteksi Serangan Distributed Denial of Services (DDOS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno,” Jiska, vol. 4, no. 3, pp. 18–26, 2020, [Online]. Available: http://ejournal.uin-suka.ac.id/saintek/JISKA/article/view/1658.

[3] L. P. Ayuningtias, M. Irfan, and J. Jumadi, “Analisa Perbandingan Logic Fuzzy Metode Tsukamoto, Sugeno, Dan Mamdani (Studi Kasus : Prediksi Jumlah Pendaftar Mahasiswa Baru Fakultas Sains Dan Teknologi Universitas Islam Negeri Sunan Gunung Djati Bandung),” J. Tek. Inform., vol. 10, no. 1, 2017, doi: 10.15408/jti.v10i1.5610.

[4] I. P. D. A. N. Port, S. D. A. N. Wireshark, D. N. Apriliani, M. A. Sasmita, and T. Windari, “Kata Kunci :,” vol. 1, pp. 6–16, 2017.

[5] R. A. Purnomo, D. Syauqy, and M. H. Hanafi, “Implementasi Metode Fuzzy Sugeno Pada Embedded System Untuk Mendeteksi Kondisi Kebakaran Dalam Ruangan,” J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya, vol. 2, no. 4, pp. 1428–1435, 2018.

[6] J. Warmansyah and D. Hilpiah, “Penerapan metode fuzzy sugeno untuk prediksi persediaan bahan baku,” vol. 9, no. 2, pp. 12–20, 2019.

[7] M. Hilmi Hafid, “Investigasi Log Jaringan Untuk Deteksi Serangan Distributed Denial Of Service (Ddos) Dengan Menggunakan Metode General Regression Neural Network Skripsi Oleh : Muhammad Hilmi Hafid,” 2019.

[8] S. Dwiyatno, A. P. Sari, A. Irawan, and Safig, “Pendeteksi Serangan Ddos (Distributed Denial Of Service) Menggunakan Honeypot Di PT. Torini Jaya Abadi,” Simika, vol. 2, no. 2, pp. 64–80, 2019.

[9] B. Cahyono, "Penggunaan Software Matrix Laboratory (Matlab) Dalam Pembelajaran Aljabar Linier," Phenom. J. Pendidik. MIPA, vol. 3, no. 1, p. 45, 2016, doi: 10.21580/phen.2013.3.1.174.

[10] I. W. Nugroho, Harianto, and I. D. G. R. Mardiani, "Rancang Bangun Aplikasi Intrusion Detection System Dengan Menggunakan Metode Fuzzy," J. Control Netw. Syst., vol. 3, no. 1, pp. 37–45, 2014, [Online]. Available: http://jurnal.stikom.edu/index.php/jcone.

[11] A. W. Muhammad and I. Riadi, "Analisis Statistik Log Jaringan Untuk Deteksi," Ilk. J. Ilm., vol. 8, no. 3, pp. 220–225, 2016.