BAB II
LANDASAN TEORI

2.1 Tinjauan Pustakan

Pada subbab ini akan menjelaskan teori dan penelitian terkait yang sudah dilakukan sebelum nya guna membantu dalam penelitian yang penulis kerjakan.

2.1.1 *DDOS (Distributed Denial of Service)*

DDoS *(Distributed Denial of Service)* merupakan salah satu serangan yang mengeksplorasi kelemahan pada suatu *web*. DDoS bekerja dengan membanjiri lalu lintas dengan banyak data sehingga *server* menjadi *down*. DDoS dilakukan menggunakan banyak komputer untuk dijadikan *botnet* yang terdistribusi untuk melakukan serangan secara bersamaan [1].

Beberapa jenis dari serangan DDoS yang paling sering terjadi, antara lain:

1. ***UDP Flood***

   User Diagram Protocol (UDP) adalah jaringan protocol tanpa session yang membanjiri *port* sebuah *remote host* secara acak. Proses ini menyebabkan *resource* milik *host* menjadi *error* sehingga *website* tidak dapat diakses. *UDP Flood* ini akan mengirimkan data yang akan mengetes jaringan korban [4].

2. ***ICMP Flood (TCP Flood)***

   TCP Flood dikernal juga dengan sebutan banjir *Ping*, yang mana serangan ini membanjiri target dengan *request* TCP secara cepat tanpa menunggu respon dari *server*. Dengan membanjiri target dengan banyak *request*, jaringan dipaksa untuk merespon dengan jumlah paket balasan yang sama. Ini menyebabkan target mejadi tidak dapat di akses oleh lalu lintas normal.

3. *SYN Flood*

Syn *flood* terjadi bila suatu host hanya mengirimkan paket SYN saja secara kontinyu tanpa mengirimkan paket ACK sebagai konfirmasinya. Hal ini akan menyebabkan host tujuan akan terus menunggu paket tersebut dengan menyimpan kedalam *backlog* [4].

Pada penelitian ini, penulis menggunakan *type* serangan *ICMP Flood* (*TCP Flood*) dengan membanjiri server menggunakan banyak *request* sehingga server akan mengalami lambar merespon dan akhirnya *down*.

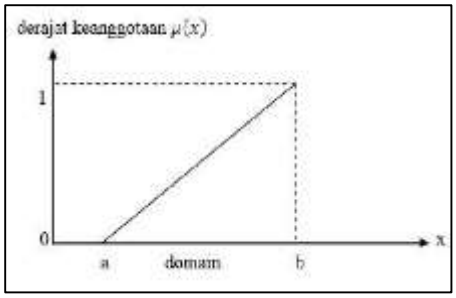
2.1.2 *Fuzzy Logic*

Fuzzy logic merupakan salah satu dari *soft computing*, yang mana *soft computing* adalah sistem yang memiliki keahlian seperti manusia, belajar dan beradaptasi dengan perubahan lingkungan [5]. *Fuzzy logic* diartikan untuk menjelaskan keambiguan, logika himpunan yang menyelesaikan keambiguan [2]. *Fuzzy logic* terdiri dari tiga pendekatan, yaitu *Tsukomoto*, *Sugeno*, dan *Mamdani*.

Tahapan-tahapan dalam metode *Fuzzy* yang digunakan yaitu sebagai berikut:

1. Pembentukan *variable fuzzy* ini terdiri dari *variable* yang akan dijadikan *variable input* dan *variable output*. *Variable* tersebut memiliki nilai dan semesta pembicaraan dengan jumlah dari yang terkecil dan terbesar [6].
2. Pembentukan himpunan *fuzzy*. Tahapan ini terdapat *variable input* dari sistem *fuzzy* yang dibuat kedalam himpunan *fuzzy* sehingga dapat digunakan dalam perhitungan. Tahap ini menentukan derajat keanggotaan dari setiap himpunan *fuzzy* [6].

a) Representasi Linear Naik

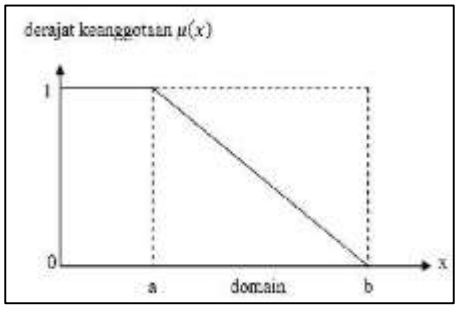


Gambar 2.1 Kurva Linier Naik

Rumus fungsi keanggotaan linear naik dinyatakan dengan:

$$\mu(x) = \begin{cases} 0 & ; x < a \\ \frac{(x-a)}{(b-a)} & ; a \le x \le b \\ 1 & ; x > b \end{cases} \qquad (2.1)$$

b) Representasi Linear Turun

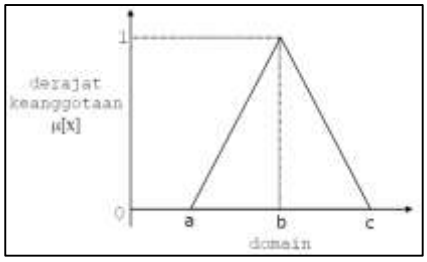


Gambar 2.2 Kurva Linear Turun

Rumus fungsi keanggotaan linear turun dinyatakan dengan:

$$\mu(x) = \begin{cases} 1 & ; x < a \\ \frac{(b-x)}{(b-a)} & ; a \le x \le b \\ 0 & ; x > b \end{cases} \qquad (2.2)$$

c) Representasi Kurva Segitiga



Gambar 2.3 Kurva Segitiga

Rumus fungsi keanggotaan kurva segitia dinyatakan dengan:

$$\mu(x) = \begin{cases} 0 & ; x \leq a \; atau \; x \geq c \\ \frac{(x-a)}{(b-a)} & ; a \leq x \leq b \\ \frac{(c-x)}{(c-b)} & ; b \leq x \leq c \end{cases} \quad (2.3)$$

Komposisi aturan adalah dengan membuat komposisi aturan berdasarkan himpunan *fuzzy* dan domain yang telah dihasilkan pada tahap sebelumnya. Rumusnya adalah sebagai berikut [6]:

[IF w is A and x is B and y is C THEN z is D] (2.4)

1. *Tsukomoto*

Metode *Tsukomoto* menggunakan fungsi implikasi MIN untuk mendapatkan nilai α tiap – tiap rule saat proses evaluasi. Proses de-*fuzzy*-fikasi pada metode *Tsukomoto* menggunakan perhitungan rata – rata (*Average*) [2].

Pada metode *Tsukamoto*, setiap konsekuen pada aturan yang berbentuk *IF-THEN* harus menggunakan himpunan *Fuzzy* dengan himpunan keanggotaan yang monoton, yaitu:

IF (x1 is A1) and (y is B1) THEN (z is C1) (2.5)

Dikarenakan pada metode *Tsukamoto* operasi himpunan yang digunakan adalah konjugasi (AND), Pada Metode ini de-*fuzzy*-fikasi dilakukan menggunakan rumus *Weight Average*, Berikut dapat dilihat rumus *Weight Average*:

$$Z = \frac{(\alpha - Predikat1 * z1) + (\alpha - Predikat2 * z2) + \cdots\ldots + (\alpha - Predikatn * zn)}{\alpha - Predikat1) + (\alpha - Predikat2) + \cdots\ldots + (\alpha - Predikatn)} \quad (2.6)$$

2. *Sugeno*

Secara umum metode *Sugeno* mempunyai 2 model, yaitu *Sugeno* Orde-Nol dan *Sugeno* Orde-Satu. Proses de-*fuzzy*-fikasi yang dilakukan pada metode *Sugeno* dilakukan dengan mencari nilai rata – ranya [2].

Secara umum bentuk *Fuzzy Sugeno* Orde-0 adalah:
IF(x1 is Ai)o(x2 is A2)o(x3 is A3)o ….o(xn is An) THEN z = K
Dengan Ai adalah himpunan *fuzzy* ke-I sebagai anteseden, dan k suatu konstanta (tegas) sebagai konsekuen, sehingga untuk mencari nilai keanggotaan pada model Sugeno.

3. *Mamdani*

Saat melakukan evaluasi, *Mamdani* menggunakan fungsi MIN dan komposisi antar *rule* sedangkan fungsi MAX digunakan untuk menghasilkan himpunan *fuzzy* baru. Rumus *Centroid* digunakan dalam proses de-*fuzzy*-fikasi pada metode *Mamdani* [2].

Fuzzy Mamdani sering disebut juga sebagai Metode MAX-MIN. Untuk mendapatkan *output* menggunakan metode mamdani, terdapat beberapa tahapan, diantaranya adalah:

a. Pembentukan Himpunan Fuzzy
b. Aplikasi fungsi Implikasi
   Menggunakan fungsi AND untuk proses implikasi, dicari nilai keanggotaan pada *variable input*.
c. Komposisi aturan
   Melakukan komposisi aturan menggunakan fungsi OR dengan mencari luas daerah *variable - variable input fuzzy* terhadap *variable output* nya.
d. De-*fuzzy*-fikasi, *defuzz*y-fikasi Pada metode mamdani diperoleh menggunakan metode *centroid* berikut:

$$Z = \frac{\int \mu(z).z\, dz}{\int \mu(z).dz} \qquad (2.7)$$

Keterangan:
Z = Hasil de-*fuzzy*-fikasi
z = *Variabel Input*
μ =Nilai keanggotaan z

Keluaran de-*fuzzy*-fikasi didapat dengan membagi nilai *moment* dengan luas daerah hasil komposisi aturan, mencari moment dan luas daerah pada metode *centroid* dapat dilakukan dengan menggunakan rumus berikut:

$$M = \int_b^a (\propto - predikat) z.dz \quad (2.8)$$

$$A = (\propto - predikat) * (a - b) \quad (2.9)$$

Keterangan:

$\propto - predikat$ = Nilai Keanggotaan

M = Moment

A = Luas Daerah

a = Batas Atas

b = Batas Bawah

2.1.3 *Web Server*

Web server adalah sebuah bentuk *server* yang digunakan untuk menyimpan halaman *website*. Untuk dapat mengakses halaman pada situs *web*, *browser* memerlukan koneksi ke *server* menggunakan protokol HTTP. *Server* akan melakukan respon terhadapat *request* yang di lakukan *user* melalui *browser* dengan mengirimkan *file* yang diinginkan dalam bentuk HTML [7]. Kemudian *browser* akan mengolah informasi yang di terima dari *server* untuk ditampilkan kepada *user*. Adapun beberapa fungsi *web server* sebagai berikut:

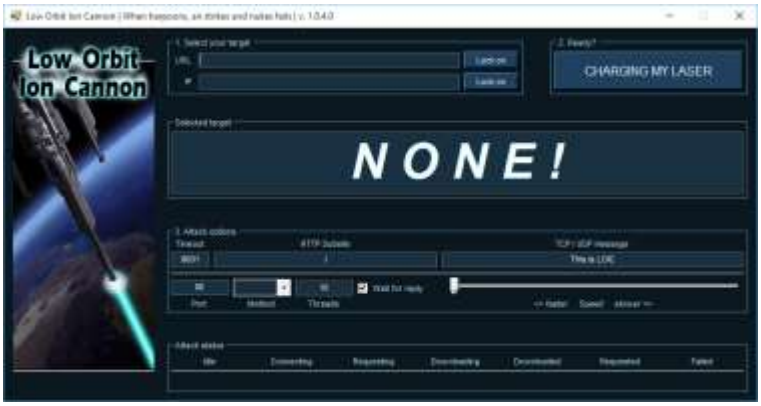
1. Memastikan semua modul yang dibutuhkan tersedia dan siap digunakan.
2. Membersihkan penyimpanan, *cache*, dan modul yang tidak terpakai.
3. Melakukan pemeriksaan keamanan terhadap HTTP *request* yang dikirimkan *browser*.

2.2 *Software* Pendukung

Penulis menggunakan beberapa *software* yang digunakan untuk melakukan penelitian ini, antara lain:

2.2.1 *Low Orbit Ion Cannon (LOIC)*

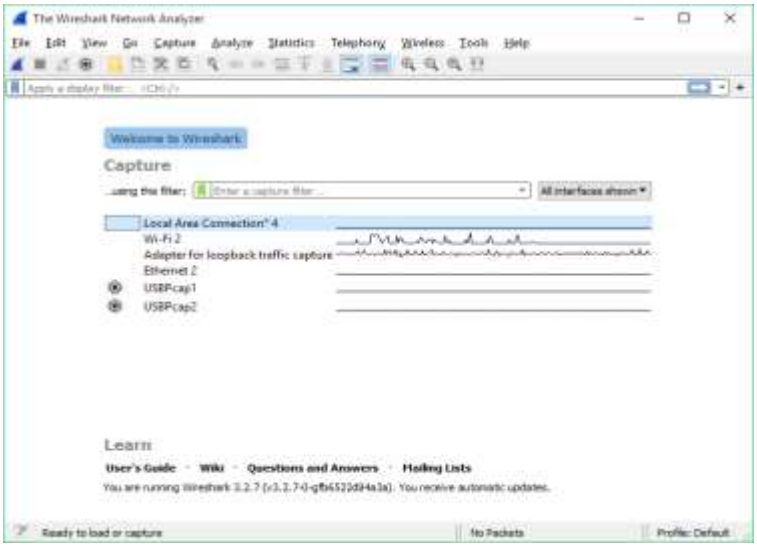
LOIC adalah salah satu *software* yang banyak digunakan untuk melakukan serangan DDoS. Aplikasi berbasis *Windows* ini sangat efektif dalam mengirimkan banyak jumlah paket ICMP, TCP, ataupun UDP [8]. LOIC akan menyerang meggunakan perintah IP, *port*, *method*, dan *threads* serta pengaturan kecepatan penyerangan dengan merubah slinder [9]. Tampilan dari aplikasi LOIC dapat dilihat pada Gambar 2.4.



Gambar 2.4 Tampilan LOIC

2.2.2 *Wireshark*

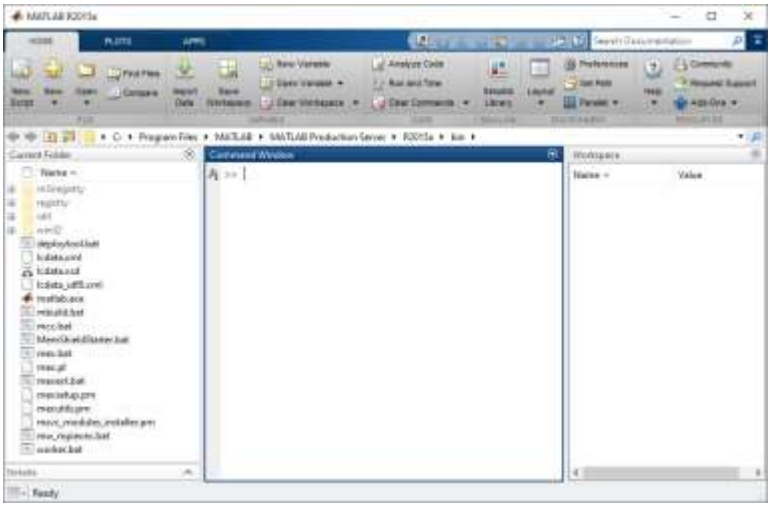
Wireshark digunakan untuk merekam log aktivitas jaringan. *Software* ini berkerja dengan menangkap semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin [8]. *Wireshartk* memungkinkan melihat apa yang terjadi pada jaringan pada tingkat mikroskopis dan merupakan standar *de facto* dibanyak perusahaan komersial dan nirlaba, lembaga pemerintah, dan lembaga pendidikan. Tampilan dari apliaksi *Wireshark* dapat dilihat pada Gambar 2.5.



Gambar 2.5 Tampilan *Wireshark*

2.2.3 *MATLAB*

Matrix Laboratory (MATLAB) adalah salah satu perangkat lunak yang banyak digunakan dalam pembelajaran *Aljabar Linier* [10]. Program ini dapat digunakan untuk memanipulasi *matrix*, implementasi algoritma, dan lain – lain. MATLAB menggunakan GUI sebagai *interface* nya dan di desain dengan bahasa pemrograman yang mengekspresikan matriks dan matematika *array* secara langsung dan menggabungkan *code*, *output* dan teks dalam satu kesatuan. Tampilan MATLAB dapat dilihat pada Gambar 2.6



Gambar 2.6 Tampilan *MATLAB*

2.3 Penelitian Terkait

Penelitian ini bukanlah penelitian pertama yang melakukan deteksi serangan DDoS menggunakan *fuzzy logic*. Ada beberapa penelitian sebelumnya yang melakukan penelitian yang sama, diantaranya:

1. Pada tahun 2020, penelitian Deteksi Serangan *Distributed Denial of Service* (DDoS) berbasis HTTP menggunakan metode *Fuzzy Sugeno* yang ditulis oleh Nadila Sugianti dkk, menjelaskan bahwa telah dilakukan identifikasi terhadap serangan DDoS menggunakan *variable input* jumlah user, jumlah paket, jumlah panjang/user dan panjang paket. Pengolahan data dilakukan menggunakan *software* MATLAB. Penelitian menghasilkan sistem yang dapat mendeteksi serangan DDoS berbasis HTTP menggunakan metode *Fuzzy Sugeno* dengan tingkat keakuratan 90% [1].
2. Indra Wahyu Nugroho ddk, dalam penelitian mereka yang berjudul Rancang Bangun Aplikasi *Intrussion Detection System* dengan menggunakan Metode *Fuzzy* menjelaskan bagaimana metode *fuzzy* berperan dalam pengambilan keputusan *Intrussion Detection System* (IDS) yaitu melihat keanehan atau ketidak normalan aktivitas yang terjadi dalam jaringan. *Varible input* yang digunakan dalm penelitian ini berupa panjang paket (*length*) dan besar paket (*frekuensi*). Penerapan *fuzzy logic* dapat menidentifikasi paket *ping* normal dengan frekuensi 3 detik dengan *length* paket 180 *Byte* per detik, serangan ICMP *flooding* dengan frekuesi serangan 5 per detik dengan *length* paket 325.000 *Byte* per detik, serangan UDP *flooding* dengan frekuensi 1 per detik dengan *length* paket sebanyak 1.500 *Byte* per detik, dan serangan TCP *flooding* dengan frekuensi serangan 1 per detik dengan *length* paket 1.500 *Byte* per detik. Namun penerapan *fuzzy logic* belum mampu mengkasifikasi paket serangan *syn-ack* dan mengidentifikasi data HTTP dengan benar [11].
3. Penelitian yang berjudul Analisis Statistik Log Jaringan untuk Deteksi Serangan DDoS Berbasis *Neural Network* yang ditulis oleh Arif Wirawan Muhammad, dkk pada tahun 2016 menjelaskan bahwa

pendekatan baru dalam mendeteksi serangan DDoS dengan memanfaatkan analisis log aktivitas jaringan menggunakan metode *neural network* mampu mengenali sernagan DDoS dengan baik. *Variable input* yang digunakan dalam penelitian ini antara lain ukuran/panjang paket, jumlah paket, variasi waktu kedatangan paket, variasi ukuran/panjang paket, kecepatan paket/detik, dan jumlah bit. Penelitian berhasil mendeteksi serangan DDoS menggunakan metode *Neural Network* dengan fungsi *Fixed Moving Average* (FMAW) dengan hasil persentase rata – rata 90,52 % terhadap tiga kondisi (normal, *slow* DDoS, dan DDoS) [5].

4. Muhammad Hilmi Hafid pada tahun 2019, melakukan penelitian yang berjudul Investigasi Log Jaringan untuk Deteksi Serangan *Distributed Denial of Servic*e (DDoS) dengan menggunakan Metode *General Regression Neural Network* menjelaskan bahwa *Genral Regression* mampun mendeteksi serangan DDoS dengan baik. Analisis menggunakan data latih dari set data terbaru untuk intrusi yaitu CICIDS2017 dan data uji diperoleh dari hasil simulasi serangan DDoS ke *web server*. Penulis melakukan dua percobaan pada penelitian nya yang mana percobaan pertama menggunakan 69 fitur dengan hasil *accuracy* 66,41%; *precision* 73,85; *recall* 64,52%; *fl-score* 61,89%. Percobaan kedua menggunakan 20 fitur dengan hasil *accuracy* 97,21%; *precision* 97,21%; *recall* 97,19%; *fl-score* 97,2% [8].
5. Julio Wermansyah dan Dida Hilpiah melakukan penelituian yang berjudul Penerapan Metode *Fuzzy Sugeno* untuk Prediksi Persediaan Bahan Baku pada tahun 2019 yang mana menghasilkan nilai prediksi sebesar 38% (*Reasonable*) [6].

Tabel 2.1 Penelitian Terkait

No	Nama Peneliti	Judul Penelitian	Metode Penelitian	Hasil	
				Kelebihan	Kekurangan
1	Nadila Sugianti, dkk	Deteksi Serangan	Penelitian ini menggunakan	Berhasil melakukan	Dari 10 data sampel yang

		Distributed Denial of Service (DDoS) Berbasis HTTP Menggunakan Metode *Fuzzy Sugeno*	fuzzy logic sugeno sebagai pendekatan dengan variable input jumlah user, jumlah paket, jumlah panjang/user dan panjang paket.	deteksi serangan DDoS dengan akurasi 90 %	digunakan, terdapat 10 % dari sampel yang tidak dapat terdeteksi
2	Indra Wahyu Nugroho, dkk	Rancang Bangun Aplikasi *Intrussion Detection System* dengan Menggunakan Metode *Fuzzy*	Penelitian ini menggunakan metode *fuzzy sugeno* dalam prosesnya, serta menggunakan *variable input* berupa panjang paket (*length*) dan besar paket (*frekuensi*).	Mampu mengklarifikasi paket serangan DDoS *ICMP Flooding*, *UDP Flooding,* dan *TCP Flooding*	Belum mampu mengklarifikasi paket serangan *syn attack* dan mengidentifikasi data HTTP dengan benar
3	Arif Wirawan Muhammad, dkk	Analisis Statistik Log Jaringan untuk Deteksi Serangan DDoS berbasis *Neural Network*	Penelitian ini menggunakan metode *neural network* dalam proses pendekatan dan menggunakan *variable input* ukuran/panjang paket, jumlah paket, variasi waktu kedatangan paket, variasi ukuran/panjang paket, kecepatan paket/detik, dan jumlah *bit*	Berhasil melakukan deteksi serangan DDoS dengan persentasi 90,52%	Penelitian tidak menjelaskan apakah metode yang disampaikan mampu melakukan deteksi serangan DDoS yang berjenis *ICMP Flooding*, *UDP Flooding*, ataupun *TCP Flooding.*

4	Muhammad Hilmi Hafid	Investigasi Log Jaringan untuk Deteksi Serangan *Distributed Denial of Service* (DDoS) dengan menggunakan Metode *General Regression Neural Network*	Penelitian ini menggunakan *Regression Neural Network* dalam proses pendekatan nya. Penulis melakukan dua percobaan dengan 69 fitur dan 20 fitur.	Penelitian ini berhasil mendapatkan hasil *accuracy 66,41%; precision 73,85; recall 64,52%; fl-score 61,89%* pada percobaan pertama dengan 69 fitur dan *accuracy 97,21%; precision 97,21%; recall 97,19%; fl-score 97,2%* pada percobaan kedua dengan 20 fitur..	Penelitian ini belum dapat menghasilkan output yang baik dengan jumolah fitur yang lebih banyak.
5	Julio Warmansyah dan Dida Hilpiah	Penerapan Metode *Fuzzy Sugeno* untuk Prediksi Persediaan Bahan Baku	Penelitian ini menggunakan fuzzy logic sugeno dalam proses prediksi persediaan bahan baku.	Berhasil memprediksi persediaan bahan baku dengan nilai MAPE sebesar 38% *Reasonable*	Penelitian ini belum mampu digunakan dalam data set yang lebih besar.

Penelitian – penelitian tersebut memperoleh hasil yang cukup baik dalam melakukan deteksi atau identifikasi terhadap serangan DDoS. Penelitian yang penulis lakukan akan menggunakan metode *fuzzy logic sugeno* namun dengan *variable input* yang berbeda, yang mana diharapkan mampu memperoleh hasil yang lebih baik lagi dari penelitian sebelumnya.