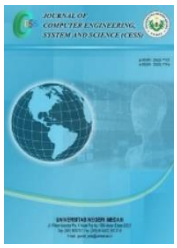
CESS
(Journal of Computing Engineering, System and Science) 7(1) January 2022 129-144

e-ISSN: 2502-714x
p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess



Analisa Pendeteksian Serangan DDoS Menggunakan Teori Pendekatan Neural Network Backpropagation

Analysis of DDoS Attack Detection Using Neural Network Backpropagation Approach

Ahmad Fajri Khumara[1], Agung Sediyono[2*], Gatot Budi Santoso[3]

[1,2,3] Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Trisakti
Jl. Kyai Tapa No.1, Jakarta Barat, DKI Jakarta, Indonesia, Indonesia.
email: [1]1ahmadfajri200697@gmail.com, [2]trisakti_agung06@trisakti.ac.id, [3]bulish@gmail.com

Diterima: 28 Juli 2021 | Diterima setelah perbaikan: 04 Nopember 2021 | Disetujui: 30 Desember 2021

A B S T R A K

Distributed Denial of Service (DDoS) adalah suatu serangan yang dimana memiliki volume, intensitas, serta biaya mitigasi yang akan terus meningkat sejalan dengan pertumbuhannya skala dari suatu instansi. Pada penelitian ini, peneliti mempunyai tujuan untuk menerapkan suatu konfigurasi terbaik dalam sebuah arsitektur jaringan syaraf tiruan guna meningkatkan tingkat akurasi yang sangat tinggi pada pendeteksian serangan DDoS menggunakan algoritma Backpropagation. Data yang digunakan dalam penelitian ini adalah data trafic jaringan dimana sudah ditandai keterangan DDoS tidaknya dari masing – masing data. Penelitian ini dilaksanakan menggunakan aplikasi Matlab berserta fiturnya yaitu NNToolBox. Dengan menguji 12 jenis Training Function berserta arsitektur Hidden Layer. Berdasarkan dari uji coba tersebut, nilai Error (MSE) paling minimal didapatkan sebesar 0,0585 dengan menggunakan Training Function trainbr serta arsitektur Hidden Layer berbentuk 3 lapisan dengan tiap lapisan terdapat masing – masing 4 neuron.

Kata Kunci: *Serangan Distributed Denial of Service, Arsitektur Jaringan Syaraf Tiruan, NNToolBox, MATLAB, Mean Square Error.*

A B S T R A C T

Distributed Denial of Service (DDoS) is an attack which has volume, intensity, and mitigation costs that will continue to increase in line with the growth of the scale of an agency. In this study, the researcher aims to implement the best configuration in an artificial neural network architecture in order to increase the very high level of accuracy in the detection of DDoS attacks using the Backpropagation algorithm. The data used in this study is network traffic data where the DDoS information has been marked as DDoS or not for each data. This research

**Penulis Korespondensi:*
email: trisakti_agung06@trisakti.ac.id

was carried out using the Matlab application and its features, namely NNToolBox. By testing 12 types of Training Function along with Hidden Layer architecture. Based on these trials, the minimum Error (MSE) value was obtained at 0.0585 using the Training Function trainbr and the Hidden Layer architecture in the form of 3 layers with each layer containing 4 neurons.

Keywords: *Distributed Denial of Service Attack, Artificial Neural Network Architecture, NNToolBox, MATLAB, Mean Square Error.*

1. PENDAHULUAN

Perkembangan teknologi informasi beberapa tahun terakhir khususnya dibidang jaringan komputer sudah berkembang sangat pesat. Adapun manfaat dari teknologi tersebut diharapkan dapat membantu mempermudah perkerjaan manusia dan perusahaan dibidang apapun. Dengan berkembangnya teknologi tersebut, pengelolaan data dan informasi diharapkan dapat lebih efisien dan efektif karena sudah semakin banyak perkerjaan yang membutuhkan kemampuan sharing resources, intergrasi data, dan keamanan data pada komputer serta dukungan jaringan internet.

Pada umumnya banyak instansi memiliki tingkat transaksi data yang tinggi disetiap harinya sehingga memerlukan sebuah konsep keamanan data dan jaringan yang terhubung pada server aplikasi. Untuk membuat konsep yang sesuai kebutuhan maka diperlukan sebuah analisa untuk Pendeteksian Serangan Distributed Denial of Service (DDoS) dengan menggunakan pendekatan Neural Network Back Propagation.[2]

Adapun tujuan dari penelitian ini adalah membangun sebuah sistem yang dapat mendeteksi serangan DDoS berdasarkan pola perilaku dan karakteristik trafik jaringan secara akurat dengan bantuan Aplikasi Matlab. Berdasarkan data trafic yang diperoleh dari Website penyedia dataset yang bernama Kaggle tentang trafic data dengan berbagai karakteristik serta label jenis trafic yang menyatakan DDoS atau bukan. Dari data tersebut dapat dipelajari pola karakteristik trafic data yang merupakan serangan DDoS.[5,7,9,14]

Research gap yang dihasilkan dari penelitian yang dilakukan oleh Siregar, Junita Juwita (2013) ini adalah memerlukan sebuah cara pengamanan pada jaringan komputer dilembaga tersebut dengan pengawasan yang lebih rutin terhada serangan DoS (Denial-of-Service Attacks). Hal ini bertujuan agar para peretas tidak dapat memenuhi dengan IP (Index Protocol) address pada jaringan komputer dan dapat mengganggu transaksi data antara server dan pengguna. Sehingga permintaan akses dari pengguna kepada sistem atau layanan jaringan yang disediakan oleh sebuah host agar tidak ditolak.

Adapun Research gap yang dihasilkan dari penelitian yang dilakukan oleh Muhammad, Arif Wirawan, dkk (2016) menunjukkan bahwa menggunakan pendekatan baru dalam pendeteksian serangan DDoS dengan menggunakan data analisis statistik terhadap log aktivitas pada jaringan komputer dengan metode neural network sebagai fungsi pendeteksi yang dapat mengenali jenis serangan DDoS dengan baik. Persentase yang didapatkan dari penelitian tersebut mendapatkan hasil rata-rata terhadap 3 kondisi jaringan (normal, slow DDoS, dan DDoS) sebesar 90,52%.

Dari 2 penilitian tersebut dapat diambil kesimpulan bahwa penyerangan terhadap DDoS melalui jaringan yang tersedia pada lembaga atau instansi masih rentan terjadi. Maka dapat diusulkan analisa untuk pendeteksian serangan DDoS agar sistem keamanan jaringan pada suatu instansi dapat lebih ditingkatkan dikemudian hari. Neural Network merupakan sebuah

solusi yang cukup handal dalam penyelesaian masalah, salah satunya adalah pendeteksian serangan DDoS dengan menggunakan metode Back Propagation.[11,14,17,18]

Back Propagation adalah salah satu metode Artificial Intelligence (AI) yang mampu melakukan pembelajaran peristiwa berdasarkan data training. Proses analisa metode Back Propagation adalah melakukan melakukan perhitungan secara runut maju yang dimulai dari data Input, Bias hingga ke Ouput.[10,15,16] Dengan adanya sistem pendeteksi ini, maka dapat segera diketahui terjadinya pola acaman serangan DDoS, sehingga dapat segera dilakukan tindakan-tindakan pencegahan.

2. LANDASAN TEORI

2.1. Denial of Service

Denial of Service atau DoS merupakan sebuah aktifitas yang dapat mengurangi laju kerja sebuah layanan ataupun mematikan layanan tersebut sehingga dapat menyebabkan pengguna asli tidak dapat menggunakan layanan. Denial of Service (DoS) juga dapat melakukan eksploitasi dari aspek suite Internet Protocol untuk menghalangi akses pihak yang berhak atas informasi atau sistem yang diserang. Serangan ini biasanya memanfaatkan sebuah celah keamanan atau hole yang ada pada sebuah sistem operasi yang sedang dipergunakan. Sebagai contoh serangan seperti ini adalah TCP SYN, seperti permohonan untuk terhubung ke sebuah jaringan yang dikirimkan kepada server dalam jumlah yang besar. Hal ini mengakibatkan server dibanjiri dengan membludaknya permintaan koneksi dan membuat sebuah sistem menjadi terhambat atau sistem tidak dapat dicapai sama sekali. Kasus Hole ini biasanya hampir terdapat di semua sistem operasi yang mengoperasikan TCP/IP untuk terhubung dengan jaringan internet. Serangan DoS cukup ditakutkan di sistem jaringan di karena efek dari serangan ini yang dapat mengakibatkan server mati atau down sehingga membuat server tidak dapat beroperasi lagi dan dengan otomatis dapat menghentikan laju pelayanan dari server tersebut. [8,9]

Menurut Douligeris & Serpanos, Serangan Denial of Service (DoS) dideskripsikan sebagai suatu ancaman yang dapat menghabiskan resource dari sebuah komputer maupun dari sebuah jaringan sehingga tidak dapat menyediakan layanan secara normal. Dampak dari serangan DoS dapat disadari ketika pengguna legal jaringan mengakses komputer atau ke sumber daya jaringan, akan tetapi akses yang ingin dijalankan terblokir atau sulit diakses oleh pengguna legal hal ini dikarenakan adanya tindakan illegal yang dilakukan oleh pengguna lain.

Serangan DoS biasanya menyerang komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang miliki komputer tersebut sehingga komputer tersebut tidak dapat menjalankan fungsinya secara maksimal sehingga membuat pengguna lain tidak dapat mengakses layanan dari komputer yang telah diserang tersebut. [8,9]

2.2. Distributed Denial of Service

Distributed denial-of-service (DDoS) adalah sebuah jenis serangan yang muncul pada tahun 1990an. Volume serta intensitas DDoS dari tahun ke tahun sangat meningkat. Pada bulan November tahun 2014, terlapor bahwa sebuah serangan DDoS merupakan teknik seranggan paling populer (ArborNetworks, 2014). Hal ini menjadikan DDoS sebuah ancaman utama didalam dunia maya serta menjadi masalah utama pada keamanan cyber. DDoS disebut sebagai senjata pilihan terbaik para hacker karena sudah terbukti bahwa DDos adalah ancaman permanen terhadap pengguna, organisasi serta infrastruktur didalam dunia maya

(BussinessWeek, 2014). Disebuah serangan lainnya pada jaringan merupakan resiko untuk integritas, ketersediaan serta kerahasiaan merupakan sumber daya (resource) yang difasilitaskan oleh organisasi (Zhao et.al, 2015).

Intrusion Detection System (IDS) Bertujuan melakukan Deteksi dini pada serangan DDoS secara otomatis. IDS pada masa ini melakukan teknik deteksi yang tidak terlalu sempurna jika dibedakan dengan teknik serangan cyber yang lebih semakin canggih. Bagi beberapa hacker, serangan DDoS salah satu yang sangat mudah untuk dilakukan, sementara untuk korban sendiri biasanya sangat sulit untuk menyadarinya. Semakin bertambahnya perkembangan teknologi membuat serangan DDoS mengalami pengembangan Teknik juga, salah satu contohnya adalah SYN-Flood. Secara umum pada sebuah paket tunggal SYN, dimana paket ini bersifat legal pada aktivitas jaringan. Sehingga sangat sulit untuk mendeteksi SYN sebagai artefak yang abnormal oleh IDS. Hal ini membuat IDS cukup sulit untuk menyadarkan alert atau peringatan apakah jaringan sedang dalam penyerangan atau tidak oleh SYN-Flood (Eray et al.,2014). Adanya permasalahan alert yang bersifat false-positive dan sering terjadi pada IDS yang berbasis signature. Pengenalan pola serangan DDoS pada IDS ini sendiri terjadi dikarenakan defisit TCP/IP itu sendiri. Sistem IDS pada umumnya hanya bertugas memantau dan memberikan penanda terhadap aktivitas jaringan yang mencurigakan dan langsung ditindang dengan dilaporkannya sebagai alert. Sistem ini akan memberikan dampak adanya volume alert yang terlalu besar dengan tingkat rata-rata false-positive yang tinggi. Hal ini disebabkan karena lalu lintas data jaringan merupakan sistem bersifat non-stasioner.[8,12,18]

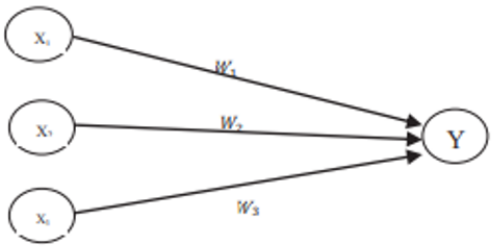
Sistem IDS pada umumnya hanya dapat memantau serta sebagai sistem peringatan (alert), sehingga memberikan dampak adanya volume alert yang terlalu besar dengan tingkat rata - rata false - positive yang tinggi. Hal itu disebabkan karena lalu lintas data jaringan merupakan sesuatu yang bersifat non-stasioner (Lee et al.,2011). Riset mengenai deteksi serangan DDoS dengan menganalisis nilai entropi artefak jaringan dalam keadaan jaringan normal serta abnormal yang dipengaruhi oleh DoS , worm serta port scanning yang sudah dilaksanakan oleh Nychis et al.(2008) serta menciptakan kesimpulan kalau nilai entropi dari artefak jaringan mempunyai korelasi . Nychis, Sekar, & Anderson(2008) menggunakan fungsi entropi optimal buat membangun angka distribusi jaringan yang wajar , setelah itu memakai entropi relatif buat mengetahui anomali atau serangan DDoS. Riset yang dilakukan oleh Gautama et al.(2016) memakai model distribusi jaringan yang didasarkan pada atribut TCP / IP yang menciptakan campuran atribut yang lumayan besar. Paket data artefak jaringan wajib diberi label serta diurutkan sehingga langkah preprocessing bisa jadi kompleks serta dengan cepat merendahkan kemampuan buat pendeteksian serangan DDoS.

2.3. Artificial Neural Network

Suatu Jaringan Syaraf Tiruan (Artificial Neural Network) merupakan suatu paradigma pengolahan data yang termotivasi dari sistem kerja syaraf biologis, semacam kinerja otak, yang memproses sesuatu data. Jaringan Syaraf Tiruan pula semacam manusia yang bisa belajar dari contoh ataupun pola. Suatu jaringan syaraf tiruan merupakan hasil konfigurasi buat aplikasi tertentu semacam pengenalan pola ataupun klasifikasi informasi lewat sesuatu proses pembelajaran. Jaringan syaraf tiruan mempunyai keahlian buat mengekstrak hubungan antara input serta output dari suatu proses, tanpa terdapatnya keberadaan fisik.[1, 9] Elemen kunci dari dari paradigma ini merupakan sesuatu struktur baru dari sistem pengolahan data. Perihal ini terdiri dari beberapa besar elemen. elemen pemrosesan yang saling berhubungan (neuron) serta saling berkolaborasi buat pemecahan masalah- masalah tertentu(Balaji dan Baskaran, 2013).

Menurut Siang, 2005, Konsep awal dari Neural Network merupakan sebuah sistem untuk mengelolah informasi yang sudah memiliki ciri-ciri serupa dengan jaringan syaraf pada manusia. Implementasi dari Neural Network sudah banyak dilakukan diberbagai bidang diantaranya adalah Diagnosa Bidang Medis, Pengenalan Pola, Proses Pengelolahan Signal, dan forecasting. Meskipuns sudah banyak yang memakainya, tetapi neural network memiliki beberapa kekurangan, ialah ketidakakuratan dari output yang diberikan. Neural network dibangun berdasarkan pola yang terdapat pada input nya.

Menurut Fausset, 1994 Neural network dibangun atas beberapa elemen yang akan digunakan untuk memproses informasi yang disebut sebagai neuron. Setiap neuron akan disambungkan dengan neuron lainnya melalui connection link yang direpresentasikan terhadap suatu bobot. Metode yang digunakan dalam menentukan besar nya dari weight disebut sebagai proses training dengan berbagai algoritma. Neuron pada neural network tersusun atas beberapa kelompok, kelompok yang dimaksud itu adalah layer. Susunan berbagai neurons dalam layer serta pola koneksi di dalam antar lapisan disebut dengan arsitektur jaringan. Arsitektur ini merupakan sebuah karakteristik penting yang membedakan dengan neural network.[22]



Keterangan gambar:

Xi : Nilai *input* ke-i

Y : Nilai *output* hasil pembangkitan nilai *input* oleh suatu fungsi aktifasi

Wi : Bobot atau nilai

Gambar 1. Contoh grafik ANN

2.4. Backpropagation

Backpropagation merupakan tata cara universal pembelajaran dalam sebuah Jaringan Syaraf Tiruan tentang bagaimana cara menuntaskan sebuah tugas yang akan diberikan. Ini adalah suatu proses pembelajaran yang terawasi serta merupakan uji coba (implementasi) dari delta rule (Vamsidhar et al, 2010). Backporopagation menyuguhkan beberapa metode komputasi yang sangat efisien untuk merubah suatu bobot dalam jaringan umpan maju (feed forward) dengan unit - unit guna aktivasi ter-diferensial untuk sebuah pembelajaran suatu set pola input output (Rebello et al, 2011). Backpropagation adalah algoritma yang menggunakan metode pembelajaran yang terawasi serta termasuk jaringan dengan beberapa lapisan. Pada jaringan arsitektur backpropagation terdapat tiga lapisan, yakni lapisan input, (hidden layer) lapisan tersembunyi, serta lapisan output. Setiap lapisan yang terdapat di jaringan tersebut memiliki satu bahkan lebih neuron (Hermawan, 2006).

Istilah ini digunakan sebab jaringan syaraf diaplikasi dengan menggunakan komputer sanggup menuntaskan beberapa proses perhitungan sepanjang proses training (pembelajaran). JST ataupun Jaringan syaraf tiruan ialah sesuatu model komputasi yang

menirukan metode kerja sistem otak manusia. Semacam halnya jaringan saraf biologis, JST juga mempunyai keahlian buat belajar serta menyesuaikan diri terhadap masukan - masukan. Jaringan Syaraf Tiruan menyerupai seperti otak manusia dalam dua hal, yakni [6]:

1. Pengetahuan didapatkan pada jaringan melalui proses training (Pembelajaran);
2. Kekuatan hubungan antara sel syaraf (neuron) yang dikenal sebagai bobot-bobot sinaptik digunakan untuk menyimpan pengetahuan.

Backpropagation merupakan salah satu bentul model Neural Network yang dapat mengatur keseimbangan terhadap jaringan agar dapat mempelajari pola yang akan digunakan selama training dan juga dapat memberikan respon yang benar atau mendekati dari pola yang dimasukkan dengan pola yang dipakai selama pelatihan. Di dalam Backpropagation terdapat banyak hidden layer yang dimana setiap hidden layer itu terdapat banyak juga neuron. Arsitektur Backpropagation dengan n(buah) masukan (ditambah satu bias), dan sebuah layar tersembunyiyang terdiri dari p(unit) (ditambah satu bias), dan juga m(buah) unit keluaran.

2.5. Matlab

MATLAB yakni singkatan dari Matrix Laboratory, sebuah perangkat lunak yang sanggup mengatasi permasalah perhitungan dalam bentuk matriks. MATLAB pada versi pertama dikenalkan oleh Cleve Moler pada tahun 1970. Pada permulaan terciptanya, MATLAB ini sendiri didesain untuk memecahkan masalah - masalah pada persamaan aljabar linear. Seiring berjalannya waktu, program ini terus mengalami perkembangan yang signifikan dari segi fungsi serta kinerja komputasi. Bahasa pemrograman yang sekarang dikembangkan serta dioptimalkan oleh MathWorks Inc. menggabungkan proses pemrograman, komputasi, serta visualisasi melewati lingkungan kerja yang gampang untuk diaplikasikan. MATLAB digunanakan sebagai program untuk menjalankan analisa dan komputasi numerik. MATLAB sendiri ialah suatu bahasa pemrograman matematika lanjutan yang terbentuk dengan dasar pemikiran memakai sifat serta bentuk matriks itu sendiri. Pada mulanya, program ini ialah interface untuk koleksi rutin - rutin numeric dari proyek LINPACK beserta EISPACK, yang dikembangkan dan dioptimalkan menggunkan bahasa FORTRAN tetapi pada masa sekarang ini merupakan produk komersial merk software yang dikembangkan dan dioptimalkan oleh Mathworks.Inc. (http://www.mathworks.com) yang paling efisien dalam melaksanakan perhitungan numeric berbasis matriks yang akan dikembangkan serta dimaksimalkan berikutnya. Mengaplikasikan bahasa C++ dan assembler (utamanya pada fungsi dasar MATLAB).[1,20]

MATLAB mempunyai keunggulan umum seperti analisa dan eksplorasi data, pengembangan algoritma, pemodelan serta simulasi, visualisasi plot dalam format 2D dan 3D, hingga sampai pengembangan aplikasi antar muka grafis. MATLAB juga dapat dikaitkan dengan aplikasi atau bahasa pemrograman eksternal lainnya, seperti C, Java, .NET, dan Microsoft Excel. Dalam MATLAB tersedia pula kotak kakas (toolbox) yang bisa diaplikasikan untuk aplikasi - aplikasi khusus, seperti pengolahan sinyal, sistem kontrol, logika fuzzy, jaringan syaraf tiruan, optimalisasi, pengolahan citra digital, bioinformatika, simulasi, serta bermacan - macam teknologi lainnya. Dalam ruang lingkup perguruan tinggi, MATLAB diaplikasikan sebagai alat pembelajaran pemrograman matematika, teknik, dan sains pada tahapan pengenalan dan lanjutan, meskipun dalam dunia industri, MATLAB dipilih sebagai alat penelitian, pengembangan, dan analisa produk industri. MATLAB dapat dioperasikan pada sistem operasi Windows, Linux, serta macOS.[13]

3. METODE PENELITIAN

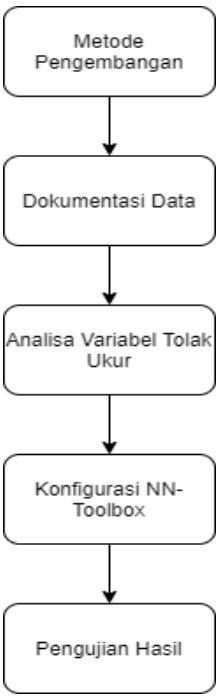
3.1. Tahapan Penelitian

Pada tahap ini penulis mengumpulkan dan mempelajari berbagai literatur baik dari jurnal, buku, maupun artikel penunjang lainnya yang berhubungan dengan DoS, DDoS, Neural Network, Backpropagation, MATLAB, dan lain-lain untuk mendapatkan pemahaman tentang apa yang akan dilakukan berdasarkan studi literatur terdahulu yang dapat menunjang dalam melakukan penelitian ini.

Setelah melakukan studi literatur, peneliti mencari dataset yang dapat digunakan pada penelitian ini dengan terdapat variable yang menunjukkan apakah transaksi yang masuk merupakan DDoS atau transaksi yang benar. Peneliti mendapatkan data tersebut dari website yang menyediakan berbagai dataset yaitu, www.kaggle.com. Kemudian untuk mengubah bentuk data csv menjadi format sql, peneliti meminta bantuan Pembimbing Utama dikarenakan data yang terlalu besar. Hal ini dilakukan untuk mempermudah penarikan data yang digunakan dalam proses prediksi di aplikasi MATLAB.

Setelah tahap pencarian dan pengolahan data, peneliti melakukan analisa akan faktor-faktor apa saya yang menjadi ciri-ciri DDoS berdasarkan variable yang tersedia di dalam dataset. Pada penelitian, peneliti mengambil variabel sesuai dengan jurnal utama yang didapatkan dari tahap studi literatur sebelumnya.

Setelah merampungkan semua keperluan data, peneliti mulai membuat script pada MATLAB untuk menciptakan rangkaian neural network dengan bantuan fitur Neural Network Toolbox. Pada tahap ini, peneliti juga melakukan konfigurasi serta melakukan uji coba untuk function – function yang cocok bagi dataset. Lalu peneliti menetapkan konfigurasi yang akan digunakan berdasarkan jumlah error yang paling kecil. Untuk memperjelas alur penelitian yang dilakukan peneliti, dapat dilihat pada Gambar 2.



Gambar 2. Alur Penelitian

3.2. Metode Penelitian

Penelitian Tugas Akhir ini menggunakan Metode Eksperimen sebagai metode penelitian yang meliputi langkah-langkah berikut:

1. Analisa Masalah

Pada langkah ini, peneliti menganalisa dan menentukan apa saja masalah pada kasus pendeteksian DDOS serta mempelajari solusi yang dapat diberikan berdasarkan berbagai jurnal serta sumber - sumber yang terpercaya. Dalam tahap ini, peneliti menentukan rencana perjalanan dari penelitian, metode yang akan digunakan serta bentuk dataset yang diperlukan. Berdasarkan dari jurnal "Analisis Statistik Log Jaringan Untuk Deteksi Serangan DDOS Berbasis Neural Network" yang diterbitkan pada Tahun 2016 oleh Arif Wirawan Muhammad, Imam Riadi dan Sunardi, untuk mendeteksi serangan DDOS variabel yang menjadi tolak ukur adalah rata-rata ukuran Panjang paket yang didapatkan dalam satuan frame waktu tertentu, jumlah total paket dalam frame waktu tertentu, nilai akar dari deviasi waktu kedatangan paket, nilai akar dari deviasi panjang paket, besar kecepatan paket per detik dalam satuan frame waktu tertentu, dan durasi aliran paket pada satuan frame waktu tertentu.

2. Pengumpulan Data

Pada langkah ini, peneliti mencari data yang dapat digunakan dalam penelitian ini. Data yang diperlukan dalam penelitian ini adalah Dataset yang berisikan detail komunikasi yang masuk ke dalam server serta label yang menunjukkan komunikasi tersebut berupa komunikasi normal atau berupa serangan DDOS. Kemudian dari dataset tersebut, ditentukan variabel - variabel yang menjadi input dan yang menjadi output.

3. Penyiapan Model

Pada langkah ini, peneliti menyiapkan model dari metode yang telah dipilih. Dikarenakan pada penelitian ini menggunakan Metode ANN, maka persiapan model yang dilakukan adalah membuat arsitektur dari ANN tersebut dan menentukan fungsi training yang akan digunakan, serta skenario uji coba untuk menentukan arsitektur ANN, fungsi training yang terbaik, dan konfigurasi yang diperlukan sesuai dengan jurnal yang dijadikan panduan dalam penelitian ini.

4. Implementasi Program

Pada tahap ini, peneliti mengimplementasikan arsitektur ANN yang telah dimodel kan beserta konfigurasi yang telah ditentukan. Dimulai dari pembuatan script ANN pada MATLAB serta men setting konfigurasi yang diperlukan. Selain itu, peneliti juga menandakan bagian script yang akan diubah sesuai dengan skenario uji coba. Jika program berjalan dengan baik tanpa error, maka dapat dilanjutkan ke tahap selanjutnya.

5. Testing Program

Pada tahap ini, peneliti melakukan proses skenario untuk dapat menentukan arsitektur ANN dan fungsi training yang terbaik pada kasus penelitian ini. Tolak ukur untuk menentukan arsitektur ANN dan fungsi training yang terbaik adalah pada nilai error yang paling rendah.

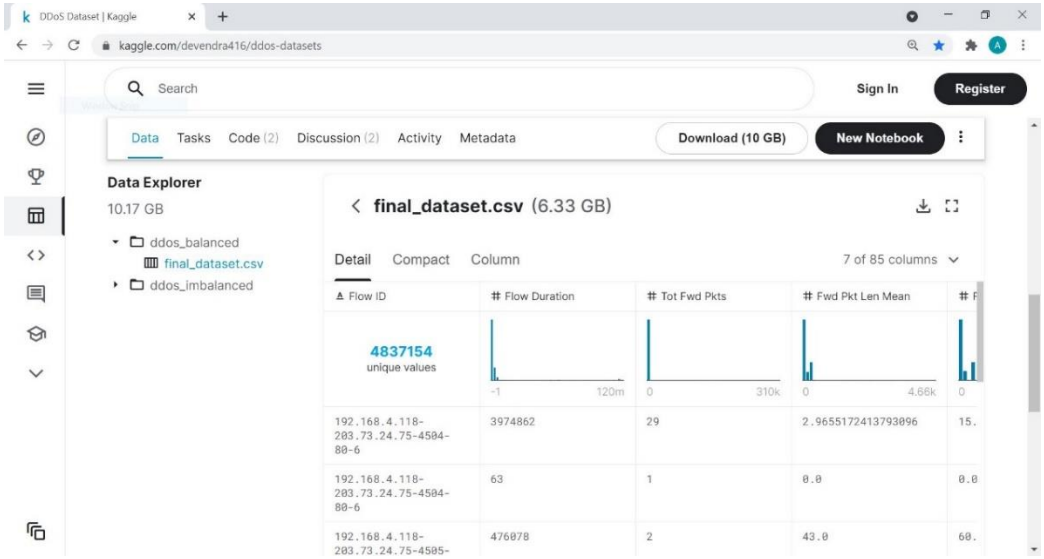
3.3. Dokumentasi Data

Dataset yang digunakan pada penelitian ini didapatkan dari website Kaggle dengan alamat situs https://www.kaggle.com/devendra416/ddos-datasets. Data yang didapatkan memiliki banyak variabel tetapi yang digunakan dalam penelitian ini adalah sebanyak enam variabel, yakni Fwd_Pkt_Len_Mean, Tot_Fwd_Pkts, Fwd_IAT_Std, Fwd_Pkt_Len_Std, Flow_Pkts_s, Flow_Duration, dan Label. Dikarenakan seusai dengan Analisa Masalah yang telah disebutkan sebelumnya. Untuk penjelasan nama variabel serta variabel yang telah dijelaskan pada Analisa Masalah adalah sebagai berikut:

a. Fwd_Pkt_Len_Mean rata-rata ukuran Panjang paket yang didapatkan dalam satuan frame waktu tertentu.
b. Tot_Fwd_Pkts jumlah total paket dalam frame waktu tertentu.
c. Fwd_IAT_Std nilai akar dari deviasi waktu kedatangan paket.
d. Fwd_Pkt_Len_Std nilai akar dari deviasi panjang paket.
e. Flow_Pkts_s besar kecepatan paket per detik dalam satuan frame waktu tertentu.
f. Flow_Duration durasi aliran paket pada satuan frame waktu tertentu.
g. Label merupakan tanda bahwa paket tersebut merupakan DDoS atau tidak.

Sehingga untuk variabel a hingga f menjadi variabel independen dalam kasus ini untuk menentukan variabel dependen yakni variabel g.

Gambar 3 menunjukkan dataset yang diambil dari Kaggle dengan format .csv dapat disaring sesuai dengan keenam variabel yang disebutkan sebelumnya.



Gambar 3. Dataset Kaggle

Dataset tersebut kemudian diubah ke dalam format .sql agar dapat diimpor ke MySQL Workbench lalu akan dihubungkan ke MATLAB untuk mengolah data-data apa saja yang akan digunakan untuk penelitian. Dari MySQL Workbench, data dapat ditarik oleh MATLAB dengan memasukkan query yang diperlukan dan diurut berdasarkan Timestamp.

3.4. Konfigurasi Neural Network Toolbox

Setelah melakukan pengolahan dataset, maka selanjutnya akan dilakukan konfigurasi terhadap Aplikasi MATLAB Fitur Neural-Network ToolBox. Langkah-langkah konfigurasinya akan dijelaskan sebagai berikut.

1. Menentukan jenis aktivasi dan fungsi training
   Fungsi aktivasi yang digunakan pada penelitian ini adalah logsig dan purelin.
2. Menentukan neuron dan layer pada hidden layer.
   Hal ini akan menentukan hasil dari output pada sistem yang digunakan.
3. Penentuan Iterasi

Iterasi adalah merupakan proses pengulangan untuk menganalisa secara terus menerus hingga didapatkan hasil yang mendekati nilai batas kesalahan yang telah ditentukan. Iterasi dibatasi agar proses analisa tidak menghabiskan waktu yang lama. Pada penelitian ini ditentukan 100 atau 1000 iterasi.

4. Penentuan Learning rate atau momentum
   Pada penelitian ini ditetapkan nilai learning rate sebesar 0,5. Hal ini dikarenakan nilai learning rate kecil dapat menyebabkan waktu proses semakin lambat. Sedangkan learning rate yang terlalu besar akan menyebabkan hasil dari setiap iterasi yang tidak linier.
5. Titik perhentian
   Sistem akan berhenti melakukan proses analisa saat iterasi atau perulangan proses telah mencapai batas maksimum yang telah ditentukan atau jika nilai error sudah lebih kecil dari batas kesalahan yang telah ditentukan.

3.5. Metode Pengujian Konfigurasi dan Hasil

Pada tahap ini, konfigurasi dari Neural Network Toolbox agar dapat sesuai dengan dataset yang digunakan. Fungsi dari tahap ini adalah agar hasil keluaran dari system dapat memberikan akurasi yang terbaik dari berbagai banyak konfigurasi yang disediakan. Konfigurasi yang menjadi target untuk diuji coba adalah Jumlah Hidden Layer, Jumlah Neuron pada Hidden Layer dan Function Training pada konfigurasi tersebut. Error tersebut dihitung menggunakan MSE (Mean Square Eror). Hal ini dapat dilakukan dengan cara mengkonfigurasi terlebih dahulu pada script fitur Neural Network Toolbox. Batasan MSE yang ditentukan adalah 0,95. Hal ini digunakan untuk membatasi proses iterasi agar tidak keluar dari batasan MSE yang ditentukan tersebut.

Kemudian hasil dari uji coba antara Hidden Layer dan Training Function, error terkecil yang *dihasilkan adalah error dari hasil.*

3.6. Skenario Uji Coba Hidden Layer

Jumlah Neuron Hidden Layer ditentukan berdasarkan instruksi di dalam Jurnal "Approximating Number of Hidden layer neurons in Multiple Hidden Layer BPNN Architecture". Terdapat tiga instruksi yakni (1) Jumlah Neuron pada satu Hidden Layer adalah 2/3 dari jumlah neuron input; (2) Jumlah Neuron Total maksimal dua kali dari jumlah neuron input; (3) Jumlah Neuron pada Hidden Layer berkisar diantara jumlah neuron pada Input Layer dan Output Layer. Kemudian untuk jumlah dari Hidden Layer yang akan digunakan, berdasarkan dari jurnal yang sama, untuk mengurangi kompleksitas dari pengerjaan system, Jumlah Hidden Layer tidak boleh lebih dari atau sama dengan empat. Oleh karena itu peneliti akan menggunakan kombinasi dari jumlah neuron yang akan digunakan untuk Hidden Layer berjumlah 3 berdasarkan instruksi yang telah dijelaskan sebelumnya.

Dari ketiga instruksi tersebut, peneliti akan menggunakan scenario sebagai berikut [18]:

1. Dua Hidden Layer dengan masing – masing Hidden Layer terdapat empat Neuron.
2. Tiga Hidden Layer dengan masing – masing Hidden Layer terdapat empat Neuron
3. Satu Hidden Layer dengan terdapat delapan Neuron

3.7. Skenario Uji Coba Training Function

Kemudian tahap selanjutnya adalah memilih jenis training function yang cocok dengan dataset yang digunakan. Pada Fitur Neural Network Toolbox MATLAB versi R2018a, terdapat dua belas jenis training function seperti pada Gambar 4.

Training Function	Algorithm
'trainlm'	Levenberg-Marquardt
'trainbr'	Bayesian Regularization
'trainbfg'	BFGS Quasi-Newton
'trainrp'	Resilient Backpropagation
'trainscg'	Scaled Conjugate Gradient
'traincgb'	Conjugate Gradient with Powell/Beale Restarts
'traincgf'	Fletcher-Powell Conjugate Gradient
'traincgp'	Polak-Ribiére Conjugate Gradient
'trainoss'	One Step Secant
'traingdx'	Variable Learning Rate Gradient Descent
'traingdm'	Gradient Descent with Momentum
'traingd'	Gradient Descent

Gambar 4. Daftar Jenis Training Function pada MATLAB Neural Network Toolbox

Dari dua belas jenis training function tersebut, pada setiap jenis training function dilakukan percobaan sebanyak lima kali untuk masing – masing function dan menghitung rata – rata dari masing – masing errornya. Kemudian dipilih function dengan hasil nilai rata – rata error terkecil sebagai training function yang terbaik untuk penelitian ini. Untuk penggunaan arsitektur Hidden Layer yang akan digunakan pada tahap ini adalah arsitektur hidden layer yang terbaik berdasarkan uji coba sebelumnya.

Dari penjelasan diatas, peneliti membuat scenario untuk uji coba sebagai berikut:

1. Melakukan lima kali uji coba dengan Traning Function trainlm kemudian dihitung rata – rata errornya.
2. Melakukan lima kali uji coba dengan Traning Function trainbr kemudian dihitung rata – rata errornya.
3. Melakukan lima kali uji coba dengan Traning Function traingf kemudian dihitung rata – rata errornya.
4. Melakukan lima kali uji coba dengan Traning Function trainrp kemudian dihitung rata – rata errornya.
5. Melakukan lima kali uji coba dengan Traning Function trainscg kemudian dihitung rata – rata errornya.
6. Melakukan lima kali uji coba dengan Traning Function traincgb kemudian dihitung rata – rata errornya.
7. Melakukan lima kali uji coba dengan Traning Function traincgf kemudian dihitung rata – rata errornya.
8. Melakukan lima kali uji coba dengan Traning Function traincgp kemudian dihitung rata – rata errornya.
9. Melakukan lima kali uji coba dengan Traning Function trainoss kemudian dihitung rata – rata errornya.
10. Melakukan lima kali uji coba dengan Traning Function traindx kemudian dihitung rata – rata errornya.
11. Melakukan lima kali uji coba dengan Traning Function traindm kemudian dihitung rata – rata errornya.
12. Melakukan tiga kali uji coba dengan Traning Function traingd kemudian dihitung rata – rata errornya.

4. HASIL DAN PEMBAHASAN

Dalam proses mengimplementasikan sistem pendeteksian serangan DDOS yang telah dirancang diperlukan serangkaian perangkat lunak (software) sebagai berikut:

1. Sistem Operasi Windows 10
2. MATLAB R2018a

Kemudian untuk perangkat keras (hardware) yang diperlukan dalam tahap implementasi aplikasi adalah sebuah laptop dengan spesifikasi sebagai berikut:

1. Intel i5-8250U 8th Gen
2. 512 GB SSD dan 1 TB Hard Disk
3. 8192 MB RAM DDR

4.1. MATLAB

MATLAB atau Matrix Laboratory adalah sebuah perangkat lunak yang berfungsi untuk komputasi numerik dan visualisasi data. MATLAB memiliki fitur Neural Network Toolbox yang memiliki fungsi untuk menganalisa, mendesain, dan mensimulasi sistem berbasis Artificial Neural Network. Fitur Neural Network Toolbox (NN Toolbox) pada MATLAB merupakan sebuah fitur untuk menganalisa, mendesain dan mensimulasikan sistem berbasis Artificial Neural Network. Terdapat fitur dimana NN Toolbox menyediakan pengaturan konfigurasi dengan jendela GUI, tetapi pada penelitian ini melakukan konfigurasi dengan menggunakan script dari MATLAB itu sendiri.

A. Implementasi Sistem

Sistem untuk mendeteksi DDOS dibuat dengan menggunakan Bahasa Pemrograman MATLAB itu sendiri. Pada tahapan ini, peneliti lebih memfokuskan pengaturan konfigurasi yang tepat berdasarkan jurnal acuan yang digunakan pada penelitian ini.

I. Proses Pengolahan Data

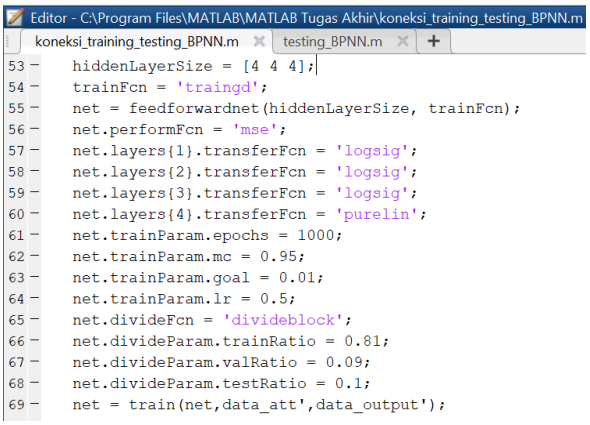
Pada tahap ini, peneliti melakukan proses pengolahan data agar siap digunakan untuk sistem yang akan dikembangkan. Tahapan ini diawali dengan menarik dataset yang telah dimasukkan ke dalam MySQL Workbench ke dalam variable MATLAB itu sendiri. Hal ini dilakukan dengan cara membangun koneksi antara MATLAB dengan database server kemudian menariknya dengan serangkaian Query. Data yang didapatkan dari Database server memiliki format Cursor, sehingga perlu diubah menjadi dalam bentuk Table. Setelah diubah menjadi format table agar lebih mudah diolah dalam MATLAB itu sendiri. Tahap selanjutnya adalah mengubah tipe data yang belum sesuai. Pada kasus ini, tiga variable yang merupakan decimal tetapi masih dalam bentuk string. Agar variable tersebut dapat dipakai di tahap selanjutnya, maka diperlukan perubahan tipe data. Kemudian, tahap selanjutnya adalah mengubah bentuk format table menjadi bentuk array. Hal ini dikarenakan sistem dari Neural Network Toolbox, input yang digunakan harus berupa array. Lalu langkah terakhir dari pengolahan data adalah merapikan list array dari input menjadi satu variable dan list array output menjadi satu variable juga.

II. Konfigurasi pada Artificial Neural Network

Pada tahap ini, dilakukan beberapa konfigurasi pada Artificial Neural Network yang akan dipakai pada penelitian ini. Konfigurasi yang akan dilakukan adalah menentukan Jumlah Hidden Layer beserta Neuronnya, Training Function, Uji Performa dengan metode apa, Transfer Function pada setiap Layer, maksimal epoch, batas dari Peformanya, Momentum

Konstan, Learning Rate, Fungsi untuk ratio pembagian dari data input menjadi Data Training, Validasi dan Uji Coba.

Konfigurasi tersebut dituliskan dengan script Bahasa Pemrograman MATLAB seperti pada Gambar 5.



Gambar 5. Konfigurasi Artificial Neural Network

B. *Uji Coba Sistem*

Pada tahap ini, Skenario Uji Coba Kelayakan Konfigurasi yang sudah dijelaskan pada BAB 3 dilaksanakan. Hal ini dilakukan agar konfigurasi dari sistem pendeteksian DDOS dapat memberikan akurasi yang terbaik. Terdapat dua skenario yaitu Uji Coba pada Hidden layer dan Uji Coba pada Training Function yang akan digunakan. Hasil perhitungan error dilakukan dengan metode MSE.

I. Uji Coba pada Hidden Layer

Sesuai dengan skenario yang sudah dituliskan pada bagian 3. Uji Coba untuk mengetahui arsitektur Hidden Layer yang terbaik dilakukan sebanyak tiga kali oleh peneliti. Kemudian menghitung hasil rata – rata error dari masing – masing arsitektur dan mengambil arsitektur yang terbaik berdasarkan nilai rata – rata error terendah. Pengerjaan Tahap Uji Coba ini dilakukan dengan memasang Training Function trainlm, dikarenakan mengikuti konfigurasi awal dari jurnal yang dijadikan acuan pada penelitian ini.

Tabel 1. Uji Coba Arsitektur Hidden Layer

Test	Hidden Layer			Aktivasi Output Layer	MSE					Rata - Rata MSE
	Layer Ke -	Jumlah Neuron	Aktivasi		Test 1	Test 2	Test 3	Test 4	Test 5	
1	1	4	Logsig	Purelin	0,1767	0,1707	0,1409	0,15	0,1553	0,15872
	2	4	Logsig							
2	1	4	Logsig	Purelin	0,1491	0,1508	0,1497	0,1841	0,156	0,15794
	2	4	Logsig							
	3	4	Logsig							
3	1	8	Logsig	Purelin	0,1992	0,1881	0,1653	0,1429	0,1478	0,16866

II. Uji Coba pada Training Function

Sesuai dengan skenario yang telah dijabarkan pada bagian 3, Uji Coba untuk mengetahui Training Function terbaik dilakukan sebanyak dua belas kali dengan masing – masing Training Function menjalani lima kali Uji Coba. Kemudian menghitung hasil rata – rata error dari masing – masing Training Function dan mengambil Training Function yang terbaik berdasarkan nilai rata – rata error terendah. Pada Tahap Uji Coba ini dilakukan dengan memasang arsitektur Hidden Layer yang terbaik berdasarkan Tahap Uji Coba sebelumnya yaitu terdapat 3 Hidden Layer dengan masing – masing Hidden Layer terdapat 4 Neuron.

Tabel 2. Uji Coba Training Function

Train Function	Jenis	MSE		
		Test Ke-1	Test Ke-2	Test Ke-3
Trainlm	Training	0,118	0,111	0,118
	Testing	0,1418	0,172	0,1418
Trainbr	Training	0,0539	0,0542	0,0417
	Testing	0,0652	0,0734	0,0585
Trainbfg	Training	0,116	0,119	0,119
	Testing	0,1408	0,1518	0,1432
Trainrp	Training	0,119	0,114	0,119
	Testing	0,1516	0,1458	0,1739
Trainscg	Training	0,121	0,119	0,12
	Testing	0,1444	0,1518	0,1456
Traincgb	Training	0,114	0,117	0,118
	Testing	0,14	0,1397	0,1408
Traincgf	Training	0,117	0,119	0,12
	Testing	0,1445	0,1408	0,1544
Traincgp	Training	0,119	0,116	0,119
	Testing	0,1408	0,1445	0,1421
Trainoss	Training	0,12	0,117	0,116
	Testing	0,1899	0,1472	0,1513
Traingdx	Training	0,122	0,121	0,125
	Testing	0,1518	0,1536	0,1587
Traingdm	Training	0,12	0,12	0,157
	Testing	0,1958	0,1516	0,2725
Traingd	Training	0,12	0,12	0,12
	Testing	0,1421	0,1417	0,1431

III. Tingkat Akurasi Sistem

Tingkat akurasi sistem yang telah dibangun diambil berdasarkan Arsitektur Hidden Layer yang terbaik dan Training Function yang terbaik. Hasil akurasi dari kedua variable Uji Coba terbaik itu adalah dengan nilai error sebesar **0.0585**.

5. KESIMPULAN

Berdasarkan model yang telah berhasil dibangun serta sudah melewati tahap-tahap untuk mendapatkan akurasi tertinggi, maka dapat diambil kesimpulan:

1. Model untuk mendeteksi DDoS berhasil dibuat dengan menggunakan metode Artificial Neural Network dengan menggunakan dataset traffic jaringan sebagai data latih dan data tes, serta dengan bantuan Toolbox dari Aplikasi MATLAB. Beberapa konfigurasi juga dilakukan oleh peneliti sesuai dengan instruksi dari beberapa jurnal dan sumber-sumber terpercaya.
2. Tingkat akurasi Model diuji berdasarkan dua aspek secara berurutan yaitu, struktur hidden layer dan jenis train function. Pada kasus penelitian ini, model dapat menghasilkan nilai MSE (Mean Square Error) terkecil adalah dengan struktur terdapat 3 hidden layer dengan masing-masing hidden layer terdapat 4 neurons, serta menggunakan train function, yakni Bayesian Regularization (trainbr). Model tersebut menghasilkan nilai rata-rata MSE dari tiga kali uji coba sebesar 0.0585.

REFERENSI

[1] P. Potocnik, Neural Networks: MATLAB examples Neural. Neural Networks course (practical examples), 2012.

[2] B. C, Panduan Penanganan Insiden Keamanan Jaringan. Indonesia: CSIRT-Badan Pengkajian dan Penerapan Teknologi, 2014.

[3] S. N. Hutagalung, “Menggunakan Aplikasi Matlab Metode Simulink Siti Nurhabibah Hutagalung Jurusan Teknik Informatika, STMIK Budi Darma,” J. Sci. Soc. Res., vol. 1, no. 1, pp. 30–35, 2018.

[4] I. Parinduri, “Model Dan Simulasi Rangkaian RLC Menggunakan Aplikasi Matlab Metode Simulink,” J. Sci. Soc. Res., vol. 1, no. 1, pp. 42–47, 2018.

[5] M. Chambali, A. W. Muhammad, and Harsono, “Klasifikasi Paket Jaringan Berbasis Analisis Statistik dan Neural Network,” J. Pengemb. IT, vol. 3, no. 1, pp. 67–70, 2018.

[6] J. T. Syafiie Nur LuthfieInformatika and U. Gunadarma, “Implementasi Jaringan Saraf Tiruan Backpropagation Pada Aplikasi Pengenalan Wajah Dengan Jarak Yang Berbeda Menggunakan MATLAB 7.0,” Universitas Gunadarma, 2007.

[7] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, “DoS and DDoS in named data networking,” Proc. - Int. Conf. Comput. Commun. Networks, ICCCN, 2013, doi: 10.1109/ICCCN.2013.6614127.

[8] J. Chris, J. Sihombing, D. P. Kartikasari, and A. Bhawiyuga, “Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software- Defined Network (SDN),” J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 3, no. 10, pp. 9608–9613, 2019.

[9] A. W. Muhammad, I. Riadi, and S. Sunardi, “Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window,” JISKA (Jurnal Inform. Sunan Kalijaga), vol. 1, no. 3, p. 115, 2017, doi: 10.14421/jiska.2017.13-03.

[10] N. A. Tindriyani, “Implementasi Neural Network Pada Matlab Untuk Peramalan Konsumsi Beban Listrik Kabupaten Ponorogo Jawa Timur,” Universitas Negeri Semarang, 2017.

[11] Y. Pan, Y. Wang, P. Zhou, Y. Yan, and D. Guo, “Activation functions selection for BP neural network model of ground surface roughness,” J. Intell. Manuf., vol. 31, no. 8, pp. 1825–1836, 2020, doi: 10.1007/s10845-020-01538-5.

[12] F. Pramudhito, Y. Purwanto, and A. Novianty, "Perbandingan Metode Sampling Dan Dimensionality Reduction Untuk Mereduksi Kompleksitas Algoritma Deteksi Pada Ddos," in e-Proceeding of Engineering, 2017, vol. 4, no. 1, pp. 924–931.
[13] A. Tjolleng, Pengantar pemrograman MATLAB: Panduan praktis belajar MATLAB. Jakarta: Elex Media Komputindo, 2017.
[14] I. Adesty, "Penerapan Intrusion Prevention System Sebagai Pengamanan Dari Serangan Ddos (Distributed Denial Of Service)," Institut Teknologi Telkom Purwokerto, 2019.
[15] M. A. Kurniawan, "Penerapan Metode Feed Forward Neural Network (Ffnn) Backpropagation Untuk," Universitas Negeri Semarang, 2017.
[16] S. Dwiyatno, A. P. Sari, A. Irawan, and S. Safig, "Pendeteksi Serangan DDOS (Distributed Denial Of Service) Menggunakan Honeypot Di PT. Torini Jaya Abadi," J. Sist. Inf. dan Inform., vol. 2, no. 2, pp. 64–80, 2019, doi: 10.47080/simika.v2i2.606.
[17] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," in Proceedings - 21st IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2020, 2020, pp. 391–396, doi: 10.1109/WoWMoM49955.2020.00072.
[18] J. Li, Y. Liu, and L. Gu, "DDoS attack detection based on neural network," 2010 2nd Int. Symp. Aware Comput., pp. 196–199, 2010, doi: 10.1109/ISAC.2010.5670479.
[19] S. Karsoliya, "Approximating Number of Hidden layer neurons in Multiple Hidden Layer BPNN Architecture," Int. J. Eng. Trends Technol., vol. 3, no. 6, pp. 714–717, 2012.
[20] H. Effendi, "Aplikasi Logika Fuzzy untuk Peramalan Beban Listrik Jangka Pendek Menggunakan Matlab," Sainstek, vol. 12, no. 1, pp. 52–58, 2009, [Online]. Available: http://ejournal.unp.ac.id/index.php/sainstek/article/view/149.
[21] B. Mardiyanto, T. Indriyani, and I. M. Suartana, "Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless," Integer J., vol. 1, no. 2, pp. 32–42, 2016.
[22] A. W. Muhammad, "Analisis Statistik Log Jaringan Untuk Deteksi Serangan Ddos Berbasis Neural Network," J. Ilm. Ilk., vol. 8, no. 3, pp. 220–225, 2016, doi: 10.33096/ilkom.v8i3.76.220-225.