Infotekmesin
Vol.13, No.02, Juli 2022
p-ISSN: 2087-1627, e-ISSN: 2685-9858
DOI: 10.35970/infotekmesin.v13i2.1396, pp.301-307

Pengembangan Perangkat Lunak Untuk Deteksi DDoS Berbasis *Neural Network*

Arif Wirawan Muhammad[1*], Muhammad Nur Faiz[2], Ummi Athiyah[3]
[1]Program Studi Teknik Informatika, Fakultas Informatika, IT Telkom Purwokerto
[2]Program Studi Rekayasa Keamanan Siber, Jurusan Teknik Informatika, Politeknik Negeri Cilacap
[3]Program Studi Sains Data, Fakultas Informatika, IT Telkom Purwokerto
[1,3]Jl. DI Pandjaitan 128 Purwokerto Selatan, Banyumas 53147, Indonesia
[2]Jln. Dr. Soetomo No.1 Karangcengis Sidakaya, Kabupaten Cilacap, 53212, Indonesia
E-mail: arif@ittelkom-pwt.ac.id[1], faiz@pnc.ac.id[2] , ummi@ittelkom-pwt.ac.id[3]

Info Naskah:
Naskah masuk: 1 Juli 2022
Direvisi: 13 Juli 2022
Diterima: 15 Juli 2022

Abstrak

Masalah keamanan sistem merupakan faktor vital yang perlu dipertimbangkan dalam pengoperasian system dan jaringan, yang nantinya untuk mitigasi bencana dan mencegah serangan pada jaringan. *Distributed Denial of Services* (DDoS) adalah sebuah bentuk serangan yang dilakukan oleh individu atau kelompok untuk merusak data melalui server atau malware dalam bentuk membanjiri paket sehingga dapat melumpuhkan sistem jaringan yang digunakan. Keamanan jaringan merupakan faktor yang harus dijaga dan dipertimbangkan dalam sebuah sistem informasi. DDoS bisa berbentuk Ping of Death, flood, Remote serangan, banjir *User Data Protocol* (UDP), dan Serangan Smurf. Penelitian ini bertujuan untuk mengembangkan perangkat lunak untuk mendeteksi adanya serangan DDoS berdasarkan log trafik jaringan. Perangkat lunak telah diuji dan berjalan sesuai algoritma *neural network*. Perangkat lunak ini dikembangkan dengan tampilan antarmuka yang memudahkan pengguna dalam mendeteksi IP sumber apakah IP tersebut melakukan serangan DDoS atau normal.

Keywords:
DDoS;
detect;
software;
neural network.

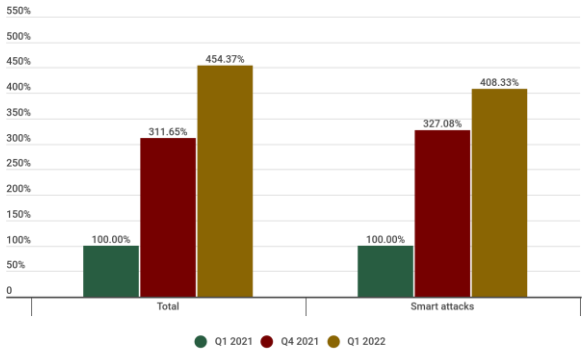
Abstract

System security issues are a vital factor that needs to be considered in the operation of systems and networks, which will later be used for disaster mitigation and preventing attacks on the network. Distributed Denial of Services (DDoS) is a form of attack carried out by individuals or groups to damage data through servers or malware in the form of flooding packets, therefore it can paralyze the network system used. Network security is a factor that must be maintained and considered in an information system. DDoS can take the form of Ping of Death, flood, Remote control attack, User Data Protocol (UDP) flood, and Smurf Attack. This study aims to develop software to detect DDoS attacks based on network traffic logs. The software has been tested and run according to the neural network algorithm. This software was developed with an interface that makes it easier for users to detect the source IP whether the IP is carrying out a DDoS attack or normal.

***Penulis korespondensi:**
Arif Wirawan Muhammad
E-mail: arif@ittelkom-pwt.ac.id

1. Pendahuluan

Distributed *denial-of-service* (DDoS) merupakan jenis serangan yang telah ada sejak tahun 1990-an. Dalam beberapa tahun terakhir, jumlah ancaman berbasis jaringan termasuk volume dan intensitas DDoS telah meningkat secara signifikan [1]. Pada Gambar 1 berdasarkan data dari [2] menunjukkan perbandingan jumlah serangan DDoS per kuartal, pada gambar tersebut terlihat peningkatan hampir 1,5 kali lipat (46%) dalam jumlah serangan relatif terhadap rekor tersebut, dan peningkatan 4,5 kali lipat dibandingkan periode yang sama tahun lalu. Alasan untuk pertumbuhan ini jelas krisis di Ukraina menyebabkan perang dunia maya, yang hampir tidak dapat gagal memengaruhi statistik. Melihat distribusi serangan DDoS berdasarkan kuartal dan tahun, dapat dilihat bahwa puncak serangan baru terjadi pada Q1 tahun 2022.



Gambar 1. Perbandingan jumlah serangan DDoS, Q1 2022, Q1 dan Q4 2021.

DDoS merupakan ancaman utama dunia maya dan merupakan masalah utama keamanan cyber [3]. DDoS disebut sebagai senjata pilihan utama hacker untuk melumpuhkan target dan telah terbukti menjadi ancaman permanen bagi pengguna, organisasi dan infrastruktur di Internet [4]. Di sisi lain, serangan DDoS merupakan risiko untuk integritas, kerahasiaan dan ketersediaan sumber daya yang disediakan oleh organisasi [5].

Deteksi dini serangan DDoS adalah proses fundamental yang dilakukan secara otomatis oleh *Intrusion Detection System* (IDS) [6], dengan menggunakan teknik deteksi berbasis *signature* yang bisa dikatakan masih jauh dari sempurna jika dibandingkan dengan teknik serangan cyber yang semakin modern. Sistem deteksi pada IDS, hanya memantau dan memberikan tag/penanda terhadap aktivitas jaringan yang mencurigakan dan langsung dilaporkan sebagai *alert*, sehingga memberikan dampak adanya volume alert yang terlalu besar dengan tingginya tingkat rata-rata kesalahan pengenalan paket data normal sebagai paket DDoS atau sebaliknya, disebabkan oleh lalu lintas data jaringan yang bersifat *non-stasioner* [7]

Deteksi intrusi umumnya terdiri dari dua pendekatan, yang pertama adalah deteksi berbasis signature karena alert dihasilkan berdasarkan atas *signature* serangan yang spesifik. Dalam proses deteksi dari pendekatan yang berbasis *signature*, IDS tidak dapat mendeteksi serangan yang belum dikenal, disebabkan oleh *database signature* yang telah kadaluwarsa atau karena *signature* memang belum tersedia. Pendekatan kedua adalah deteksi berbasis anomali. Dalam metode anomali perlu diciptakan suatu profil perilaku khas dalam taraf tertentu dari fitur aktivitas jaringan. Profil ini kemudian dijadikan sebagai dasar untuk mendefinisikan aktivitas jaringan normal. Jika ada aktivitas jaringan menyimpang terlalu jauh dari profil, maka *alert* akan terbentuk. IDS Berbasis anomali memiliki keunggulan yaitu dapat mendeteksi teknik serangan baru. Di sisi lain, IDS berbasis anomali lebih kompleks dibandingkan dengan signature-based IDS [8] [9]

IDS dianggap kurang baik jika satu jenis serangan saja dapat menimbulkan beberapa jenis *alert*, sedangkan pada umumnya IDS menghasilkan volume *alert* yang cukup tinggi, sehingga pada saat ini peneliti di bidang keamanan jaringan mengembangkan berbagai teknik deteksi DDoS untuk menyempurnakan metode deteksi IDS yang berbasis signature misalnya dengan menggunakan metode fuzzy, metode SVM, ataupun dengan metode anomali parametrik dengan tujuan akhir yaitu menghasilkan suatu mekanisme deteksi terhadap serangan DDoS yang memiliki tingkat akurasi tinggi seiring dengan minimalnya konsumsi resource yang digunakan dan rendahnya nilai false negative atau false positive [10]. Selain metode fuzzy, metode SVM, ataupun metode anomali parametrik terdapat pula metode *neural network* atau yang disebut juga dengan jaringan syaraf tiruan yang dapat digunakan sebagai sebuah metode alternatif untuk mendeteksi serangan DDoS [11].

Serangan DDoS ini sangat membutuhkan hasil dari *capture* trafik jaringan. Kunci utama dalam sistem pengenalan DDoS adalah adanya kemampuan untuk mendeteksi serangan yang sifatnya baru (novel attack) yang disebut juga dengan zero-day attack. Algoritma deteksi serangan DDoS yang berbasis *neural network* mampu digunakan untuk mendeteksi tingkah laku trafik jaringan yang sifatnya anomali dengan beberapa kelebihan yaitu adanya sifat adaptif dan fleksibel dari algoritma *neural network*

Beberapa penelitian sebelumnya mengenai deteksi serangan DDoS, yaitu penelitian yang dilakukan oleh Ridho [8] memanfaatkan kemampuan *neural network* untuk mendeteksi serangan DDoS atau normal berdasarkan traffic log yang diolah menggunakan Fixed Moving Window. Setiap data DDoS dan normal terdiri dari 27 traffic log dengan total jumlah dataset sebanyak 54 data dengan jumlah data uji masing – masing sebanyak 10 data DDoS dan Normal. Pengambilan dataset dilakukan menggunakan LOIC, HOIC, dan DoS HTTP dengan pemantauan traffic selama 300 detik. Hasil pengolahan Fixed Moving Window didapatkan nilai ekstraksi yang akan di masukkan ke dalam *neural network* yang memiliki nilai input sebanyak 6 nilai, satu hidden layer dengan neuron berjumlah 300 dan 2 output yang terdiri dari dataset normal dan dataset DDoS. Hasil pengujiannya menunjukkan bahwa *neural network* dapat mendeteksi serangan DDoS dan Normal dengan nilai accuracy sebesar 95%.

Tiga algoritma dalam klasifikasi DDoS pada penelitian [14] yaitu, Naive Bayesian, K-means clustering dan Random Forest. Ketiga algoritma ini diiuji dengan dataset dari mengumpulkan secara langsung menggunakan wireshark, kemudian diekstraksi dan dilatih sesuai dengan

algoritma masing-masing. Hasilnya akurasi dari Naive Bayesian adalah 97,65%, K-means clustering adalah 99,88% dan Random Forest 100%. Ketiga algoritma ini dipilih karena algoritma ini membutuhkan lebih sedikit atribut dan jumlah data pelatihan yang rendah untuk dijalankan proses deteksi dibandingkan dengan algoritma yang lain.

Penelitian mengenai DDoS lainnya [15], hasil dari penelitian yang dilakukan yaitu sistem yang dibangun dapat mendeteksi serangan DDoS dan Port Scanning dengan memanfaatkan Snort sebagai tool pendeteksi serangan. Sistem juga dapat mengirimkan notifikasi peringatan kepada administrator melalui SMS dengan menggunakan layanan SMS Gateway Nexmo SMS *Application Programming Interface* (API) berdasarkan serangan yang terdeteksi dan mampu melakukan penanganan serangan dengan memanfaatkan IPTables berdasarkan analisa yang dilakukan oleh administrator.

Penelitian [16] mengusulkan metode teknik *Advanced Support Vector Machine* (ASVM) sebagai penyempurnaan dari Support Vector Machine (SVM) yang sudah ada. Teknik ASVM merupakan metode klasifikasi multiclass yang terdiri dari tiga kelas. Dalam makalah ini, kami berhasil mendeteksi dua jenis serangan DDoS berbasis flooding. Teknik deteksinya dapat mengurangi waktu pelatihan serta waktu pengujian dengan menggunakan dua fitur utama, yaitu fitur volumetrik dan asimetris. Penelitian ini mengevaluasi hasil dengan mengukur tingkat false alarm, tingkat deteksi, dan akurasi. Akurasi deteksi teknik deteksi ini sekitar 97% dengan waktu pelatihan dan waktu pengujian tercepat. Dataset yang digunakan berasal dari eksperimen yang dilakukan

Penelitian selanjutnya [17], dengan memanfaatkan bot telegram untuk notifikasi jika ada indikasi serangan DDoS pada server. Penelitian ini berfokus bagaimana mitigasi bencana secara cepat, pengujian penelitian dengan serangan DDoS menggunakan UDP ang mengakibatkan lonjakan lalu lintas 53,5 Mbps.

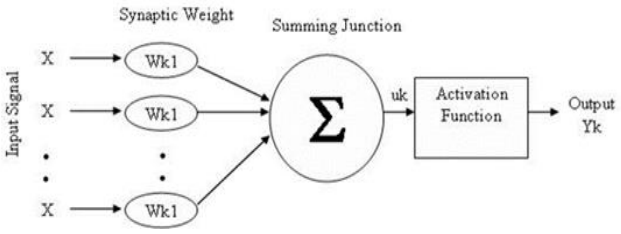
Penelitian relevan lainnya dilakukan oleh Procopiou [18], penelitian menyajikan algoritma deteksi serangan DDoS Layer Aplikasi baru menggunakan teori *exponential smoothing* dan chaos. Pendekatan ini mampu mendeteksi serangan DDoS jenis Flooding dan pada layer aplikasi Slow-Rate di jaringan IoT S*mart Home*. Pendekatan ini sangat cepat dan akurat dalam mendeteksi serangan (10 hingga 40 detik setelah serangan dimulai), menghasilkan jumlah false-positive yang sangat rendah dan tidak memerlukan kumpulan data yang besar untuk membangun pendekatan ini.

Penelitian ini berfokus pada pengembangan Perangkat lunak deteksi DDoS untuk dapat digunakan mendeteksi adanya serangan DDoS berdasarkan log trafik jaringan.

2. Metode

2.1 Neural Network

Neural network atau jaringan syaraf tiruan adalah paradigma pemrosesan informasi yang terinspirasi oleh sistem sel syaraf biologi, sama seperti otak yang memproses suatu informasi [12]. Pada jaringan otak manusia terdapat sel syaraf (neuron) yang memiliki tiga komponen penyusun yang saling bekerja sama untuk mengolah sinyal-sinyal informasi. Tiga komponen tersebut adalah dendrit (input), badan sel (pengolah input), dan akson (output) [13], seperti yang tersaji pada Gambar 2.



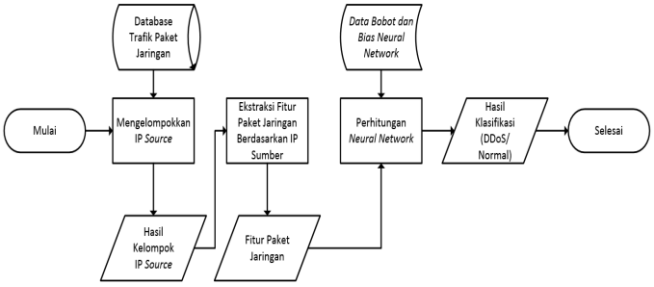
Gambar 2. Komponen *Neural Network*.

Keterangan dari Gambar 2 adalah sebagai berikut:

- X adalah input akan dikirim ke neuron dengan bobot kedatangan tertentu.
- Input ini akan diproses oleh suatu fungsi perambatan yang menjumlahkan nilai semua bobot yang datang yang disimbolkan dengan Wk1.
- Hasil penjumlahan dari poin kedua akan dibandingkan dengan suatu nilai ambang (threshold) tertentu melalui fungsi aktifasi setiap neuron.
- Apabila input melewati nilai ambang tertentu, maka neuron akan diaktifkan, tetapi kalau tidak, neuron dinonaktifkan.
- Bila neuron diaktifkan, neuron mengirimkan output melalui bobot-bobot output-nya ke semua neuron yang berhubungan dengannya yang disimbolkan dengan Yk.

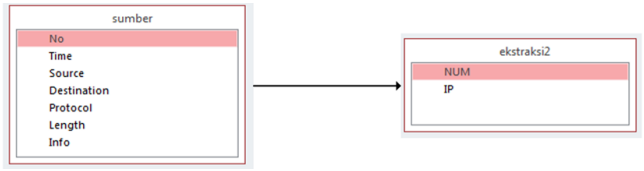
2.2 Proses Penelitian

Metode penelitian ini adalah Alur proses perangkat lunak dalam mendeteksi DDoS, diperlihatkan Gambar 3.

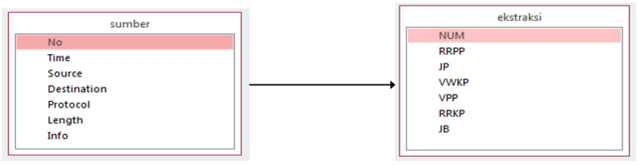


Gambar 3. Alur Proses Perangkat Lunak Deteksi DDoS.

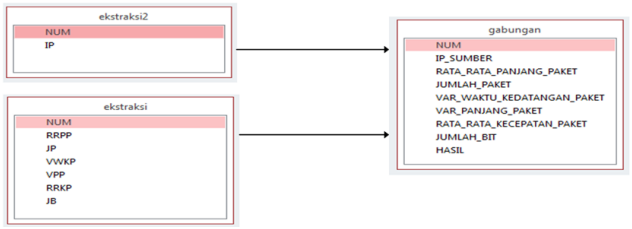
Berdasarkan Gambar 3, perincian alur proses perangkat lunak deteksi DDoS adalah pertama perangkat lunak deteksi DDoS menggunakan data trafik paket jaringan yang telah disimpan dalam bentuk tabel dengan nama tabel ‘sumber’ pada database Ms Access dengan nama ‘DB1’. Berdasarkan tabel ‘sumber’, perangkat lunak mengelompokkan IP source. Hasil pengelompokan *IP source* disimpan dalam tabel dengan nama ‘ekstraksi2’, dapat dilihat pada Gambar 4.



Gambar 4. Pengelompokan *IP Source*.



Gambar 5. Ekstraksi Fitur Paket Jaringan.



Gambar 6. Penggabungan Tabel Ekstraksi dan Ekstraksi2.

Proses Selanjutnya Perangkat lunak deteksi DDoS melakukan ekstraksi fitur paket jaringan ternormalisasi berdasarkan kelompok IP source yang dihasilkan dari langkah pertama. Proses ekstraksi fitur paket jaringan dilaksanakan dengan perintah yang tersaji pada algoritma 1.

Algoritma 1 Ekstraksi Fitur Berdasarkan Kelompok IP *Source*

```
1 SELECT (AVG(LENGTH)/1053) AS RRP_PAKET,
2 (COUNT(NO)/41929) AS J_PAKET,
3 (VAR(TIME)/111247) AS VWK_PAKET,
4 (VAR(LENGTH)/1000296) AS VP_PAKET,
5 ((COUNT(*)/5)/8385) AS RRK_PAKET,
6 (SUM(LENGTH)/23135589) AS J_BIT
7 FROM SUMBER WHERE SOURCE = :IP
```

Fitur paket jaringan yang diekstraksi berdasarkan perintah Algoritma berikut adalah:

a) Rata-rata panjang paket, yang diaplikasikan dengan perintah "*(AVG(LENGTH)/1053) AS RRP_PAKET".* Pada baris pertama.
b) Jumlah paket, yang diaplikasikan dengan perintah "*(COUNT(NO)/41929) AS J_PAKET".* Pada baris kedua.
c) Variansi waktu kedatangan paket, yang diaplikasikan dengan perintah "*(VAR(TIME)/111247) AS VWK_PAKET".* Pada baris ketiga.
d) Variansi panjang paket, yang diaplikasikan dengan perintah "*(VAR(LENGTH)/1000296) AS VP_PAKET".* Pada baris keempat.
e) Rata-rata kecepatan paket, yang diaplikasikan dengan perintah "*((COUNT(*)/5)/8385) AS RRK_PAKET".* Pada baris kelima.
f) Jumlah bit, yang diaplikasikan dengan perintah "*(SUM(LENGTH)/23135589) AS J_BIT".* Pada baris keenam.
g) Pengelompokan fitur berdasarkan IP *source* diaplikasikan dengan perintah "*FROM SUMBER WHERE SOURCE = :IP".* Pada baris ketujuh.

Hasil ekstraksi fitur paket jaringan disimpan dalam tabel dengan nama 'ekstraksi' seperti pada Gambar 5. Berdasarkan hasil dari langkah pertama dan kedua, perangkat lunak deteksi DDoS melaksanakan penggabungan tabel 'ekstraksi' dan 'ekstraksi2' menjadi tabel 'gabungan'. Berdasarkan tabel 'gabungan', perangkat lunak deteksi DDoS melaksanakan perhitungan *neural network* berdasarkan data bias dan bobot *neural network*, diperlihatkan pada Gambar 6. Proses terakhir adalah perangkat lunak deteksi DDoS menghasilkan klasifikasi paket jaringan.

3. Hasil dan Pembahasan

3.1 Skema Input Neural Network

Input *neural network* berupa data fitur jaringan yang berasal dari dataset trafik jaringan normal dan DDoS yang berjumlah enam jenis, ekuivalen dengan jumlah neuron input *neural network*. Input *neural network* ekuivalen dengan jumlah neuron input neural network disajikan pada Tabel 1.

Tabel 1. Input Neural Network – Neuron Input Neural Network

No.	Nama *Input*	*Neuron Neural Network* ke-
1.	Rata-rata ukuran panjang paket dalam jeda sampling.	1
2.	Jumlah total paket dalam jeda sampling.	2
3.	Variansi waktu kedatangan paket dalam jeda sampling.	3
4.	Variansi ukuran panjang paket dalam jeda sampling.	4
5.	Rata-rata kecapatan paket dalam jeda sampling.	5
6.	Jumlah total bit paket dalam jeda sampling.	6

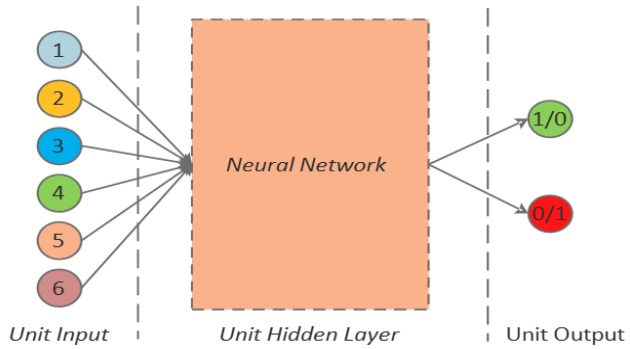
Tabel 2. Perincian Target dan Kondisi

No.	Pasangan Bilangan Target	Kondisi	Keterangan
1.	1-0	Normal	Mewakili kondisi trafik jaringan yang bersifat normal.
2.	0-1	DDoS	Mewakili kondisi trafik dimana terjadi serangan DDoS.

3.2 Skema Target Neural Network

Target *neural network* dalam penelitian ini adalah bilangan biner yang terdiri dari dua jenis pasangan. Setiap pasangan bilangan biner mewakili kondisi trafik yang akan dikenali oleh *neural network* [19].

Visualisasi arsitektur *neural network* dalam penelitian ini disajikan pada Gambar 7, dengan unit input sesuai dengan Tabel 1 dan unit output sesuai dengan Tabel 2.



Gambar 7. Visualisasi Arsitektur *Neural Network*.

Tabel 3. Skema Arsitektur Neural *Network Network*

Tipe ke-	Neuron *Input*	Variasi *Hidden Layer*	Total Neuron *Hidden*	Neuron *Output*
1.		13		
2.	6	8-5	13	2
3.		9-2-2		
4.		12		
5.	6	8-4	12	2
6.		9-2-1		
7.	6	6	6	2
8.		3-3		
9.	6	3	3	2
10.		2-1		

3.3 Skema Layer Neural Network

Arsitektur neural network pada penelitian ini divariasikan menjadi enam jenis dengan jumlah neuron dan hidden layer yang berbeda-beda dengan tujuan untuk mendapatkan arsitektur *neural network* optimal dalam mengenali trafik jaringan normal dan DDoS. Variasi tersebut dibentuk karena tidak adanya kepastian mengenai jumlah hidden layer terbaik yang digunakan dalam menyelesaikan suatu permasalahan dengan *neural network* [20]. Skema arsitektur *neural network* dan variasi *hidden layer* disajikan pada Tabel 3. Secara teori, hidden layer pada layer *neural network* berfungsi meningkatkan kemampuan *neural network* dalam memecahkan suatu problem. Konsekuensi dari adanya lapisan ini adalah pelatihan menjadi makin sulit atau lama. Semakin banyak hidden layer yang digunakan, maka akan dapat digunakan untuk memecahkan masalah yang kompleks, namun di sisi lain memperlama proses pembelajaran dan menurunkan kinerja dari *neural nework*. Pembentukan variasi arsitektur *neural network* seperti yang tersaji pada Tabel 3 didasarkan pada teori bahwa penggunaan satu *hidden layer* pada *neural network* sudah cukup untuk menyelesaikan sebuah kasus prediksi [13].

Target *neural network* dalam penelitian ini adalah bilangan biner yang terdiri dari dua jenis pasangan. Setiap pasangan bilangan biner mewakili kondisi trafik yang akan dikenali oleh *neural network* [19]. Kolmogorov [21] menyebutkan bahwa jumlah *hidden layer* terbaik untuk menyelesaikan suatu permasalahan dengan neural network adalah 2n+1, dimana n adalah jumlah neuron input. Berdasarkan teori yang dipaparkan oleh Fausset dan Kolmogorov tersebut, pada penelitian ini dibentuk variasi jaringan *neural network* untuk mencari arsitektur neural network yang mampu memberikan akurasi tertinggi dalam menyelesaikan permasalahan deteksi DDoS [22].

3.4 Hasil Perbandingan dari Pelatihan dan Pengujian Neural Network

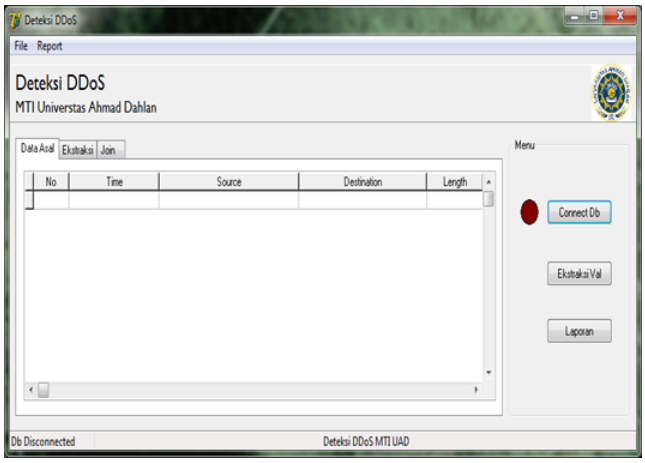
Masing-masing variasi arsitektur *neural network* pada penelitian ini dilatih dengan data hasil ekstraksi dataset paket DDoS dan dataset paket normal yang berasal dari simulasi mandiri. Data pelatihan terbagi menjadi tiga skema yaitu skema 1 berjumlah 40% dari keseluruhan data hasil ekstraksi, skema 2 berjumlah 50% dari keseluruhan data hasil ekstraksi, dan skema 3 berjumlah 70% dari keseluruhan data hasil ekstraksi, sesuai dengan Tabel 4.

Tabel 4. Perbandingan Hasil Skema 1-2-3

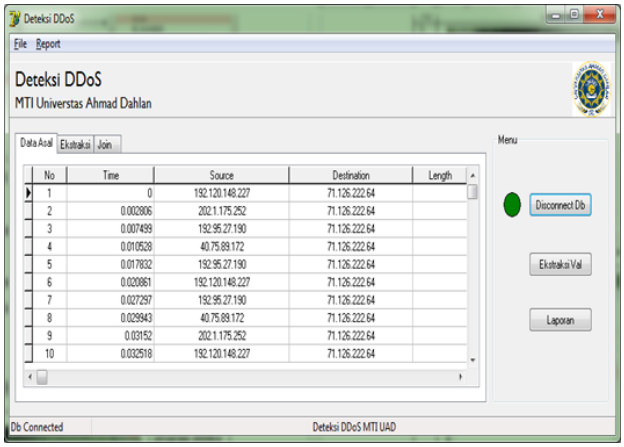
Skema Data Pelatihan-Pengujian **Data Normal = 2.175 (100%)** **Data DDoS = 1.635 (100%)**	**Nilai *Accuracy* Tertinggi (%)**	**Arsitektur *Neural Network***
(Skema 1) Data Pelatihan Paket Normal = 870 data (40%) Data Pelatihan Paket DDoS = 654 data (40%)	99,04	6-(2-1)-2
Data Pengujian Paket Normal = 1.305 data (60%) Data Pengujian Paket DDoS = 981 data (60%)		6-(3)-2
(Skema 2) Data Pelatihan Paket Normal = 1.088 data (50%) Data Pelatihan Paket DDoS = 818 data (50%)	98,74	6-(3)-2 6-(6)-2 6-(8-5)-2
Data Pengujian Paket Normal = 1.087 data (50%) Data Pengujian Paket DDoS = 817 data (50%)		6-(9-2-2)-2 6-(13)-2
(Skema 3) Data Pelatihan Paket Normal = 1.523 data (70%) Data Pelatihan Paket DDoS = 1.145 data (70%)	99,74	6-(9-2-2)-2
Data Pengujian Paket Normal = 652 data (30%) Data Pengujian Paket DDoS = 490 data (30%)		

Pada penelitian ini didapatkan bahwa *neural network* dengan skema 6-(9-2-2)-2 yang dilatih dan diuji dengan skema pembagian data pelatihan sebanyak 70% dan data

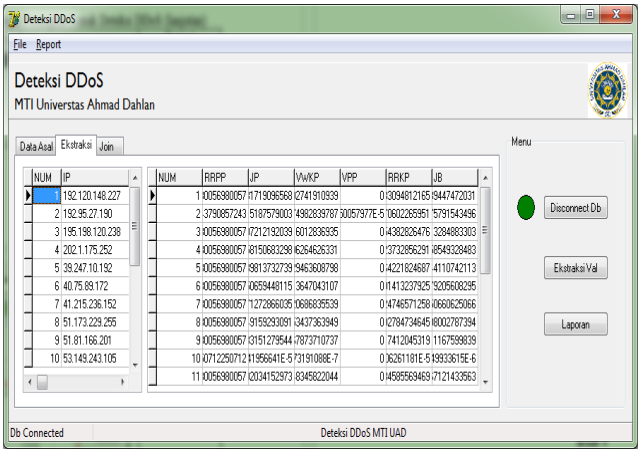
pengujian sebanyak 30% memberikan nilai accuracy yang paling tinggi yaitu 99,74%.



Gambar 8. Antarmuka awal program deteksi DDoS.



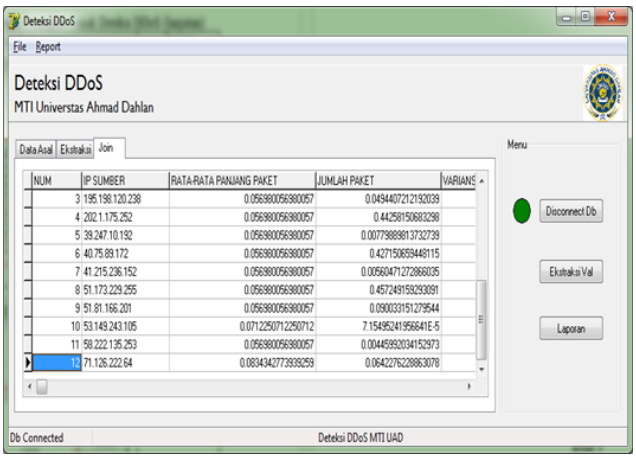
Gambar 9. Antarmuka untuk menampilkan data paket jaringan yang belum diolah dari tabel ‘sumber’.



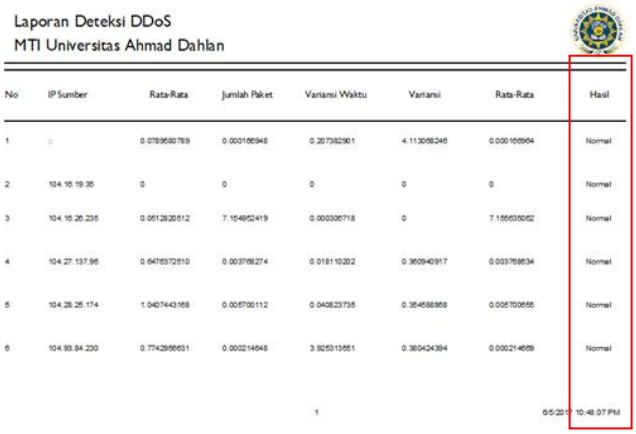
Gambar 10. Antarmuka untuk menampilkan hasil ekstraksi dari tabel ‘ekstraksi ’dan hasil pengelompokan IP source pada tabel ‘ekstraksi2’

Bobot dan bias dari *neural network* tipe 9 dengan layer 6-(9-2-2)-2 yang memberikan nilai akurasi terbaik. Selanjutnya diimplementasikan menjadi sebuah perangkat lunak deteksi DDoS yang dibangun dengan bahasa pemrograman Delphi untuk mempermudah penggunaan. Interface perangkat lunak deteksi DDoS. Pada gambar 8 merupakan antarmuka awal dari aplikasi deteksi serangan DDoS, aplikasi ini terdapat 3 tab, yaitu Data awal, Ekstraksi dan Join. Pada perangkat lunak ini terdapat 3 tombol, yaitu Connect Db, Ekstraksi Val dan Laporan.

Pada gambar 9 merupakan antarmuka setelah menghubungkan antara perangkat lunak dan *database*. Pada gambar ini menampilkan data paket jaringan yang belum diolah dari tabel ‘sumber’, hal ini didapatkan setelah menekan tombol Connect Db. Pada gambar 10 merupakan antarmuka yang menampilkan hasil ekstraksi fitur paket jaringan pada tabel ‘ekstraksi ’dan hasil pengelompokan IP source pada tabel ‘ekstraksi2’, hal ini setelah menekan tab Ekstraksi.



Gambar 11. Hasil penggabungan tabel ‘ekstraksi’ dan tabel ‘ekstraksi2’.



Gambar 12. Antarmuka untuk menampilkan hasil ekstraksi fitur paket jaringan

Pada gambar 11 menampilkan hasil, setelah pindah tab ke join, maka hasilnya adalah tabel ‘gabungan ’ yang merupakan penggabungan inner join antara tabel ‘ekstraksi’ dan tabel ‘ekstraksi2’. Kemudian menekan tombol Ekstaksi Val maka aplikasi akan memproses untuk mengklasifikasi DDoS/normal berdasarkan *IP source* dan fitur paket jaringan yang dimiliki oleh *IP source* tersebut.

Pada gambar 12 menampilkan laporan, Laporan tersebut didasarkan dari hasil ekstraksi fitur paket jaringan pada tabel ‘ekstraksi ’dan hasil pengelompokan IP source pada tabel ‘ekstraksi2’. Pada tanda merah (hasil) sudah ada hasil dari klasifikasi apakah IP sumber melakukan serangan DDoS atau normal. Perangkat lunak ini dapat berjalan dengan baik, dan dapat digunakan untuk mendeteksi adanya serangan DDoS berdasarkan log trafik jaringan.

4. Kesimpulan

Secara umum, *neural network* mampu diaplikasikan pada perangkat lunak yang dikembangkan untuk mendeteksi serangan DDoS. Pada penelitian ini perangkat lunak telah diuji dan berjalan sesuai algoritma *neural network*. Perangkat lunak ini dikembangkan dengan tampilan antarmuka yang memudahkan pengguna dalam mendeteksi IP sumber apakah IP tersebut melakukan serangan DDoS atau tidak. Saran untuk penelitian selanjutnya dapat mengembangkan aplikasi yang sekaligus menjadi alert untuk mengamankan server dan jaringan dengan algoritma lainnya.

Daftar Pustaka

[1] M. N. Faiz, O. Somantri, A. R. Supriyono, and A. W. Muhammad, “Impact of Feature Selection Methods on Machine Learning-based for Detecting DDoS Attacks : Literature Review,” *J. Informatics Telecommun. Eng.*, vol. 5, no. 2, pp. 305–314, 2022, doi: 10.31289/jite.v5i2.6112.

[2] Kaspersky, “DDoS attacks hit a record high in Q4 2021,” 2022. [Online]. Available: https://www.kaspersky.com/about/press-releases/2022_ddos-attacks-hit-a-record-high-in-q4-2021

[3] A. D. Lopez, “Network Traffic Behavioral Analytics for Detection of DDoS Attacks,” *SMU Data Sci. Rev.*, vol. 2, no. 1, p. 25, 2019.

[4] A. Banitalebi Dehkordi, M. R. Soltanaghaei, and F. Z. Boroujeni, *The DDoS attacks detection through machine learning and statistical methods in SDN*, vol. 77, no. 3. Springer US, 2021. doi: 10.1007/s11227-020-03323-w.

[5] 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.

[6] A. Yudhana, I. Riadi, and F. Ridho, “DDoS classification using neural network and naïve bayes methods for network forensics,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, 2018.

[7] M. Odusami, S. Misra, O. Abayomi-Alli, A. Abayomi-Alli, and L. Fernandez-Sanz, “A survey and meta-analysis of application-layer distributed denial-of-service attack,” *Int. J. Commun. Syst.*, vol. 33, no. 18, pp. 1–24, 2020, doi: 10.1002/dac.4603.

[8] M. A. Ridho and M. Arman, “Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan,” *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 3, pp. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.

[9] A. Wirawan, C. Feresa, M. Foozy, and A. Azhari, “Machine Learning-Based Distributed Denial of Service Attack Detection on Intrusion Detection System Regarding to Feature Selection,” *Int. J. Artif. Intelegence Res.*, vol. 4, no. 1, pp. 1–8, 2020, doi: 10.29099/ijair.v4i1.156.

[10] P. Kaur, M. Kumar, and A. Bhandari, “A review of detection approaches for distributed denial of service attacks,” *Syst. Sci. Control Eng.*, vol. 5, no. 1, pp. 301–320, 2017, doi: 10.1080/21642583.2017.1331768.

[11] M. Aamir and S. M. A. Zaidi, “DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation,” *Int. J. Inf. Secur.*, vol. 18, no. 6, pp. 761–785, 2019, doi: 10.1007/s10207-019-00434-1.

[12] M. F. Mridha *et al.*, “A Comprehensive Survey on Deep-Learning-Based Breast Cancer Diagnosis,” *Cancers (Basel).*, vol. 13, no. 23, p. 6116, Dec. 2021, doi: 10.3390/cancers13236116.

[13] L. V. Fausset, *Fundamental of Neural Networks Architectures, Algorithms, and Application*. Englewood Cliffs, New York: Prentice-Hall, 1994.

[14] S. S. Priya, M. Sivaram, D. Yuvaraj, and A. Jayanthiladevi, “Machine Learning based DDOS Detection,” in *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, Mar. 2020, pp. 234–237. doi: 10.1109/ESCI48226.2020.9167642.

[15] R. Achmad, E. V. Manullang, and E. R. Sanmas, “Rancang Bangun Aplikasi Deteksi Dan Penanganan Serangan Ddos Dan Port Scanning Memanfaatkan Snort Pada Jaringan Komputer,” *J. Teknol. Inf.*, vol. 8, no. 1, pp. 2–11, 2020.

[16] M. Myint Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, “Advanced Support Vector Machine-(ASVM-) based detection for Distributed Denial of Service (DDoS) attack on Software Defined Networking (SDN),” *J. Comput. Networks Commun.*, vol. 2019, 2019, doi: 10.1155/2019/8012568.

[17] M. Taufan Asri Zaen, A. Tantoni, M. Ashari, P. Studi Studi Sistem Informasi, and S. Lombok, “DDoS Attack Mitigation With Intrusion Detection System (Ids) Using Telegram Bots,” *JISA (Jurnal Inform. dan Sains)*, vol. 04, no. 02, pp. 149–154, 2021.

[18] A. Procopiou, N. Komninos, and C. Douligeris, “ForChaos: Real Time Application DDoS Detection Using Forecasting and Chaos Theory in Smart Home IoT Network,” *Wirel. Commun. Mob. Comput.*, vol. 2019, pp. 1–14, Feb. 2019, doi: 10.1155/2019/8469410.

[19] A. Saied, R. E. Overill, and T. Radzik, “Detection of known and unknown DDoS attacks using Artificial Neural Networks,” *Neurocomputing*, vol. 172, pp. 385–393, 2015, doi: 10.1016/j.neucom.2015.04.101.

[20] C. J. Hsieh and T. Y. Chan, “Detection DDoS attacks based on neural-network using Apache Spark,” *2016 Int. Conf. Appl. Syst. Innov. IEEE ICASI 2016*, pp. 1–4, 2016, doi: 10.1109/ICASI.2016.7539833.

[21] J. Schmidt-Hieber, “The Kolmogorov–Arnold representation theorem revisited,” *Neural Networks*, vol. 137, pp. 119–126, May 2021, doi: 10.1016/j.neunet.2021.01.020.

[22] M. Aslam, “Introducing Kolmogorov-Smirnov Tests under Uncertainty: An Application to Radioactive Data,” *ACS Omega*, vol. 5, no. 1, pp. 914–917, 2020, doi: 10.1021/acsomega.9b03940.