Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi
Volume.1, Nomor.1 Tahun 2023
e-ISSN: 3031-898X; p-ISSN: 3031-8998, Hal 01-11
DOI: https://doi.org/10.61132/neptunus.v2i4.67
Available online at: https://journal.arteii.or.id/index.php/Neptunus

Identifikasi Serangan DDOS pada Jaringan Komputer Menggunakan Algoritma Artificial Neural Network

Kelik Sussolaikah[1*], Pitrasacha Adytia [2], Wahyuni[3] , Lisda Aulia Rahmi[4]
[1] Universitas PGRI Madiun, Indonesia
[2,3,4] STMIK Widya Cipta Darma, Indonesia

Alamat: Jl. Setia Budi No.85, Kanigoro, Kec. Kartoharjo, Kota Madiun, Jawa Timur 63118
Korespondensi penulis: vikaelisabeth@gmail.com

Abstract. *DDOS (Distribute Denial of Service) is a type of structured attack. This attack has been around since 1990. DDoS attacks are capable of paralyzing servers by flooding network traffic and causing it to go down. To overcome this problem, the way to detect DDoS attacks has several methods and algorithms, one of which is the Artificial Neural Network algorithm and uses the Machine learning method due to the fast computing process, high accuracy, and this research uses the SKKNI research method Number 299 of 2020. The analysis was carried out uses training data from the latest dataset, namely CICIDS2017, which is a development of a previously existing dataset. DDoS attack detection testing using the confusion matrix method obtained bot precision of 0.99, recall of 0.99, and f1score of 0.99, 3*

Keywords: *Implementation of Swallow Nest Quality, Wighted Product, TOPSIS*

Abstrak. DDOS (Distribute Denial of Service) merupakan jenis serangan yang terstruktur, Serangan ini telah ada sejak tahun 1990. Serangan DDoS mampu melumpuhkan server dengan membanjiri lalu lintas jaringan dan mengakibatkan down. Untuk mengatasi masalah tersebut, cara mendeteksi serangan DDoS memiliki beberapa metode dan algoritma, salah satunya algoritma *Artificial Neural Network* dan memakai metode *Machine learning* dikarenakan proses komputasi yang cepat, akurasi yang tinggi, dan penelitian ini menggunakan metode penelitian SKKNI Nomor 299 Tahun 2020. Analisis dilakukan menggunakan data latih dari dataset terbaru yaitu CICIDS2017 yang merupakan pengembangan dari dataset yang sudah ada sebelumnya. Pengujian deteksi serangan DDoS menggunakan metode *confusion matrix* didapatkan Bot *precision* nya 0.99 *recall* 0.99, dan *f1score* 0.99, 3

Kata kunci: *DDoS (distributed denial of service), Python, Artificial Neural Network, Machine Learning.*

1. LATAR BELAKANG

DDOS (*Distribute Denial of Service*) merupakan jenis serangan yang terstruktur, serangan DDoS adalah serangan yang mungkin bisa sering kita jumpai diantara serangan lainnya. Serangan DDoS merupakan teknik yang paling populer dan menjadi senjata pilihan *hacker* karena telah terbukti menjadi ancaman di internet, serangan ini telah ada sejak tahun 1990. Serangan DDoS mampu melumpuhkan server dengan membanjiri lalu lintas jaringan dan mengakibatkan down. Metode *Neural Network* secara algoritma EM (*Expectation-Maximization*) digunakan untuk mendeteksi adanya serangan DDoS. Menurut dataset DARPA ada 21 kelompok serangan yang dapat dikelompokkan menjadi 13 kelompok serangan, sehingga terjadi kesalahan pemisahan alert dari jenis serangan yang sama, sehingga menjadi serangan yang berbeda.

Secara sederhana, DDoS adalah sebuah upaya untuk menghambat kinerja *server* yang dilakukan oleh seorang penyerang atau attacker. DDoS tersebut menarget server atau jaringan

Received: Janauri 28, 2023; Revised: Februari 12, 2023; Accepted: Februari 26, 2023; Published: Februari 28, 2023

dan membanjirinya dengan t*rafic*. Serangan yang diakibatkan oleh DDoS akan menghambat akses ke *server* bahkan membuat jaringan internet berhenti total. Setelah penyerang berhasil mendapatkan targetnya, ia menggunakan kumpulan perangkat yang berhasil diretas yang disebut dengan botnet. Jaringan botnet yang berisi puluhan ribu perangkat tersebut dapat dikendalikan dan diperintah oleh penyerang. Ketika sebuah alamat IP telah menjadi target serangan, setiap bot akan mengirimkan *trafic* ke target secara berulang. *Trafic* yang dikirim oleh penyerang akan memenuhi jalur data sehingga akses ke jaringan server menjadi lambat atau bahkan mati.

Untuk mengatasi serangan yang berkelanjutan tersebut, DomaiNesia telah melakukan mitigasi terhadap berbagai bentuk serangan semacam DDoS. Mitigasi adalah sebuah upaya untuk meminimalisir dampak serangan. Upaya tersebut dilakukan dengan memanfaatkan jaringan yang dirancang khusus untuk menyerap trafic serangan namun tetap memperbolehkan trafik bersih untuk melalui jaringan server, lapisan ini kami sebut dengan layer Anti-DDoS. Dengan Anti- DDoS, *website* yang ditargetkan oleh penyerang dapat terlindungi dan dapat diakses ketika terjadi serangan ini (Yulianto, 2020).

Untuk mengatasi permasalahan tersebut, deteksi serangan DDoS pada jaringan komputer dapat dilakukan melalui pendekatan pembelajaran mesin (machine learning). Penelitian ini bertujuan untuk mengembangkan pendekatan baru yang mampu mendeteksi serangan DDoS secara efisien dengan memanfaatkan metode Artificial Neural Network sebagai fungsi deteksi. Data yang digunakan untuk pelatihan dan pengujian diambil dari dataset CICIDS2018. Diharapkan, penelitian ini dapat mendeteksi serangan DDoS secara efektif serta melindungi jaringan dari ancaman DDoS (Dharma, 2014).

2. KAJIAN TEORITIS

Intrusion Detection System (IDS)

Menurut Muhammad (2016), *Intrusion Detection System* (IDS) adalah proses pemantauan peristiwa yang terjadi pada sistem komputer atau jaringan dan menganalisisnya untuk menentukan kegiatan ini, termasuk normal atau intrusi. Model proses IDS memiliki 3 fungsi dasar, yaitu: pertama, pengambilan data dari berbagai tingkatan sistem seperti jaringan, *host*, dan aplikasi. *Intrusion Detection system* (IDS) adalah kemampuan yang dimiliki oleh perangkat keras atau perangkat lunak yang berfungsi untuk mendeteksi aktivitas mencurigakan pada jaringan dan menganalisis dan mencari Secara umum, IDS dibagi menjadi dua bentuk yang digunakan saat ini dan keduanya me-miliki perbedaan dalam hal mendeteksi dan menangguhkan kejahatan. kegiatan. Keduanya harus dikembangkan, sehingga

hasilnya lebih efektif dalam mendeteksi setiap *infiltrasi* dan menyiapkan strategi yang tepat. Berikut adalah tiga bentuk Sistem Deteksi Intrusi (IDS).

Machine Learning

Menurut Simon (2020), *Machine Learning* merupakan pelatihan untuk membantu software melakukan sesuatu tanpa pemograman atau aturan yang *eksplisit*. Dalam pemograman tradisional, programmer harus menentukan aturan yang digunakan, jadi sangat berbeda dengan *Machine Learning. Machine Learning* ini sangat mengfokuskan terhadap analisis data, dimana pemograman menyediakan serangkaian contoh dan komputer mempelajari pola dari data tersebut. Proses pembelajaran *Machine Learning* dimulai dengan mengobservasi data seperti contoh-contoh, pengalaman langsung, dan arahan hingga mengerti pola dari data supaya dapat membuat keputusan yang lebih baik di masa yang akan datang sesuai dengan data yang diberikan. *Machine Learning* dapat disebut sebagai pemograman dengan data. Tujuan utama dari *Machine Learning* adalah komputer mampu belajar dengan sendiri tanpa bantuan dari manusia dan penyesuaian tindakan

Dataset CCIDS 2017

Dataset CCIDS 2017 adalah kumpulan data yang berisi serangan umum yang jinak dan paling mutakhir yang menyerupai data dunia nyata (PCAP) yang sebenarnya. Dataset CICICDS 2017 dibangun menggunakan NetFlowMeter Network Traffic Flow Analyzer yaitu alat mengumpulkan lebih dari 80 fitru dan dukungan lalu lintas jaringan aliran dua arah mencakup hasil analisis lalu lintas dengan aliran berlabel berdasarkan stempel waktu, sumber dan IP tjuan port sumber dan tujuan protokol dan serangan.

ANN (Artificial Neural Network) atau Jaringan Saraf Tiruan

Menurut Mulyawan (2019), *Artificial Neural Network* adalah upaya untuk mensimulasikan jaringan neuron yang membentuk otak manusia sehingga komputer akan dapat mempelajari berbagai hal dan membuat keputusan dengan cara yang mirip manusia. ANN (*Artificial Neural Network*) dibuat dengan memprogram komputer biasa untuk berperilaku seolah- olah mereka sel-sel otak yang saling berhubungan.

SKKNI Nomor 299 Tahun 2020

Menurut Monica, (2015) metode Weighted Product merupakan suatu metode pengambilan keputusan yang efisien dalam perhitungan,selain itu waktu yang dibutuhkan lebih singkat dan banyak digunakan untuk menyelesaikan permasalahan dengan menggunakan perkalian antar nilai kriteria yang telah ditentukan, yang dimana nilai dari setiap kriteria harus dipangkatkan terlebih dahulu dengan bobot kriteria yang telah ditetapkan diawal. Proses ini sama dengan proses normalisasi.

Keputusan Menteri Ketenagakerjaan Republik Indonesia Nomor 299 Tahun 2020 tentang penetapan standar kompetensi kerja nasional indonesia kategori informasi dan komunikasi golongan pokok aktivitas pemrograman, konsultasi komputer dan kegiatan yang berhubungan dengan itu (YBDI) bidangkeahlian *Artificial Intelligence Subbidang Data Science*

3. METODE PENELITIAN

Tahapan penelitian perlu melakukan pemetaan kompetensi, perlu juga untuk melakukan perhitungan akurasi dengan konsep data mining. Penjelasan tiap tahap dapat dilihat sebagai berikut ini:

Tabel 1. Pemetaan Standar Kompetensi

Tujuan Utama	**Fungsi Kunci**	**Fungsi Utama**	**Fungsi Dasar**
Menemu kan pengetah uan, *insight* atau pola yang bermanfa at dari data untuk berbagai keperluan	Menganalisis kebutuhan organisasi	*Business understan ding*	Menentukan objektif bisnis
			Menentukan tujuan teknis *data science*
			Membuat rencana proyek *data science*
		Data understan ding	Mengumpulkan data
			Menelaah data
			Memvalidasi data
	Mengemban gkan model	*Data preparatio n*	Memilih data
			Membersihkan data
			Mengkonstruksi data
		Modeling	Menentukan label
			Mengintegrasikan data
			Membangun skenario pengujian
			Membangun model
		Model evaluation	Mengevaluasi hasil pemodelan

			Melakukan *review* proses pemodelan Membangun skenario pengujian
	Menggunakan model yang dihasilkan	*Deployment*	Membuat rencana *deployment* model
			Melakukan *deployment* model
			Membuat rencana pemeliharaan
			Melakukan pemeliharaan model
		Evaluation	Melakukan *review* proyek *data science*
			Membuat laporan akhir proyek *data science*
			Melakukan *review* proyek *data science*

Confusion Matrix

Menurut Rosandy (2016), *Confusion matrix* merupakan suatu metode yang digunakan untuk melakukan perhitungan akurasi pada konsep data mining. *Confusion matrix* berisikan informasi mengenai hasil klasifikasi akutal dan telah di prediksi oleh sistem klasifikasi. Performa dari sistem tersebut biasanya dievaluasi menggunakan data dalam sebuah matrix. Dibawah ini menampilkan sebuah confusion matrix untuk pengklasifikasian ke dalam dua kelas

Kelas	Terklasifikasi *Positif*	Terklasifikasi Negatif
Positif	TP (*True Positive*)	FN *(False Negatif)*
Negatif	FP(*False Positive*)	TN *(True Negatif)*

Tabel 2. Visualisasi Confusion Matrix

Keterangan bisa diuraikan sebagai berikut:

a. Nilai *True Negatif* (TN) merupakan jumlah data *negatif* yangterdeteksi dengan benar.
b. *False Positive* (FP) merupakan data *negatif* namun terdeteksi sebagai data *positif*.
c. *True Positive* (TP) merupakan data *positif* yang terdeteksi benar.
d. False Negatif (FN) merupakan kebalikan dari True Positive, sehingga data positif namun terdeteksi sebagai data negatif.

Berdasarkan nilai *True Negatif* (TN),*False Positive* (FP),*False Negatif* (FN),dan *True Positive* (TP) dapat diperoleh nilai *akurasi,presisi,recall* dan *f-measure*

Python

Menurut Foundation (2019), *Python* adalah bahasa pemrograman yang *interpretatif*, berorientasi objek dan semantik dinamis. Python memiliki *high-level* struktur data, *dynamic typing* dan *dynamic binding*. *Python* memiliki sintaks sederhana dan mudah dipelajari untuk penekanan pada kemudahan membaca dan mengurangi biaya perbaikan program.

4. HASIL DAN PEMBAHASAN

Hasil penelitian dalam mengimplementasikan sistem deteksi serangan DDoS menggunakan Artificial Neural Network (ANN). Dengan metode pengembangan sistem SKKNI Nomor 299 Tahun 2020 yang dimulai dari tahap *Business Understanding*, *Data understanding*, *Data Preparation, Modelling*, *Model Evaluation*.

Business Understanding

Serangan DDoS adalah bentuk serangan yang dilakukan dengan mengirim paket secara terus menerus kepada mesin bahkan jaringan komputer. Serangan ini akan mengakibatkan sumber daya mesin ataupun jaringan tidak bisa diakses atau digunakan oleh pengguna. Serangan DdoS terhadap satu entitas di jaringan berpotensi berdampak terhadap entitas lain. Misalnya, jika *host* atau *server* dalam jaringan diserang dengan strategi DDoS tertentu, ada kemungkinan bahwa Entitas lain, seperti *switch* dan *controller* juga terkena dampaknya.

Dampak awal dari serangan ini adalah jumlah spam yang meningkat secara tiba-tiba. Pada saat trafik normal, *website* akan jarang atau hampir tidak pernah ada spam. Secara sederhana, DDoS adalah sebuah upaya untuk menghambat kinerja *server* yang dilakukan oleh seorang penyerang atau attacker. DDoS tersebut menarget *server* atau jaringan dan membanjirinya dengan t*rafic*. Serangan yang diakibatkan oleh DDoS akan menghambat akses ke *server* bahkan membuat jaringan internet berhenti total.

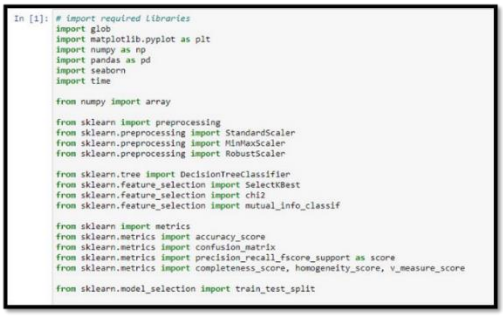
Untuk mengatasi masalah tersebut, maka mendeteksi adanya serangan DDoS yang diterima oleh jaringan komputer memiliki beberapa metode dan berbagai macam algoritma, salah satunya algoritma *Artificial Neural Network* dan pemilihan metode *machine learning* dikarenakan proses omputasi yang cepat, akurasi yang tinggi, dan juga bisa melakukan proses komputasi dengan data yang sangat banyak. penelitiannya membuat sistem deteksi menggunakan algortima *Artificial Neural Network*. UDP *Flood* menjadi fokus utama dalam proses deteksi dan mitigasi. Pendeteksian yang dibangun melalui proses *learning* mendapatkan akurasi sebesar 99.95 % dan dibuktikan dengan simulasi serangan dan pengujian.

Tabel 3 Grup Serangan

No.	Group	Label	Deskripsi
1.	Benign	Benign	Lalu lintas normal.
2.	Dos	Dos Hulk	Penyerang menggunakan alat hulk penolakan layanan terhada web server.
		Dos Golden Eye	Penyerang menggunakan alat goldeneye untuk melakukan serangan penolakan layanan.
		Dos Slowhttptest	Penyerang mengeksploitasi permintaan mendapatkan Http, mencegah klien lain mengakses dan memberi penyerang kesempatan untuk koneksi http ke server yang sama.
		Dos Slowloris	Penyerang menggunakan alat slowloris untuk melakukan serangan penolakan layanan.
3.	Probe	Portscan	Penyerang mengumpulkan informasi dengan mesin korban seperti jenis sistem operasi dan menjalankan layanan dengan mengirimkan paket dengan berbagai port tujuan.
4.	DDoS	DDoS	Penyerang menggunakan beberapa mesin yang beroperasi bersama untuk menyerang satu mesin korban.
5.	Brute Force	FTP-Patator	Penyerang melakukan serangan brute force untuk menebak kata sandi login FTP.
		SSH-Patator	Penyerang menggunakan ssh patator untuk menebak kata sandi login ssh.
6.	Botnet	Bot	Penyerang menggunakan Trojan untuk menembus. keamanan beberapa mesin korban.
7.	Web Attack	Brute Force	Seraangan yang dilakukan untuk bisa masuk ke suatu website dengan cara membobol password website.
		XSS	Serangan injeksi kode pada sisi klien dengan menggunakan sarana halaman website.

Data Understanding

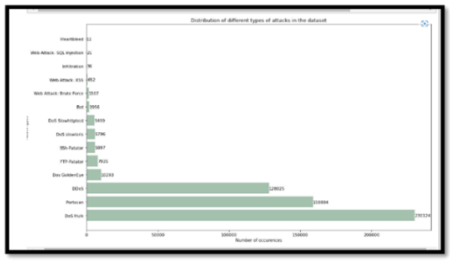
Data untuk machine learning berasal dari dataset CCIDS 2017. Peneliti menggunakan variabel independen untuk memprediksi variabel dependen. Dalam penelitian ini, variabel independen adalah atribut serangan DDoS dan variabel dependen adalah apakah termasuk serangan DDoS atau tidak. Pada dataset CCIDS 2017 terdapat data trafik normal dan serangan. Jika penelitian mencapai akurasi 75% dalam memprediksi apakah termasuk serangan DDoS atau tidak, maka model layak digunakan. Selanjutnya *features* pada tahap ini, langkah yang umum adalah dengan membuat kamus data (*data dictionary*).



```
In [1]: # import required libraries
        import glob
        import matplotlib.pyplot as plt
        import numpy as np
        import pandas as pd
        import seaborn
        import time

        from numpy import array

        from sklearn import preprocessing
        from sklearn.preprocessing import StandardScaler
        from sklearn.preprocessing import MinMaxScaler
        from sklearn.preprocessing import RobustScaler

        from sklearn.tree import DecisionTreeClassifier
        from sklearn.feature_selection import SelectKBest
        from sklearn.feature_selection import chi2
        from sklearn.feature_selection import mutual_info_classif

        from sklearn import metrics
        from sklearn.metrics import accuracy_score
        from sklearn.metrics import confusion_matrix
        from sklearn.metrics import precision_recall_fscore_support as score
        from sklearn.metrics import completeness_score, homogeneity_score, v_measure_score

        from sklearn.model_selection import train_test_split
```

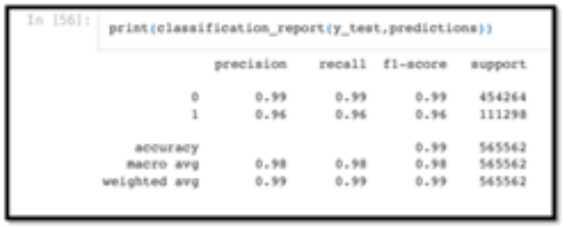
Gambar 1. Library

Pada Gambar 1 *import* merupakan *library python* untuk data analisis seperti data *science*, visualisasi data, manipulasi gambar dan data dan juga untuk membuat tabel, mengubah dimensi data, mengecek data, dan lainnya. *Import glob* untuk membuat daftar file atau urutan secara rekursif (proses pemanggilan), *import matplotlib* digunakan untuk membuat beberapa perubahan pada gambar yang fokus pada visualisasi data seperti membuat plot grafik, *import numpy* as np adalah *library python* untuk membuat objek kelas array tunggal dan multidimensi (operasi numerik), *Import seaborn* digunakan untuk membangun visualisasi data yang dibangun diatas *matplotlib* dan *import time* digunakan untuk meng*import* modul time (waktu)



Gambar 2. Distribusi Jenis Serangan Kumpulan Data (2)

Gambar 2 grafik distribusi berbagai jenis serangan merupakan kumpulan jenis data serangan yang dapat dilihat serangan DDoS mencapai 12.802.5 sedangkan BENIGN, Dos GoldenEye 10.293, Dos Hulk 23.012.4, Portscan 15.880.4, FTP Patator 7.935, SSH Patator 5.897, Dos Slowloris 5.796, Bot 1.956, Web Attack Brute Force 1.507, Web Attack XSS 652, Infiltration 36, Web Attack Sql Injection 21, dan Heartbleed 11.



```
In [56]: print(classification_report(y_test,predictions))

                  precision    recall  f1-score   support

               0       0.99      0.99      0.99    454264
               1       0.96      0.96      0.96    111298

        accuracy                           0.99    565562
       macro avg       0.98      0.98      0.98    565562
    weighted avg       0.99      0.99      0.99    565562
```

Gambar 3. *Precision, recall, f1-score, support*

Pada gambar 3 merupakan hasil dari perhitungan *Precision, recall, f1-score. Precision* Merupakan rasio prediksi benar *positif* dibandingkan dengan keseluruhan hasil yang diprediksi positf, Recall Merupakan rasio prediksi benar *positif* dibandingkan dengan keseluruhan data yang benar positif, F1 Score merupakan perbandingan rata-rata presisi dan *recall* yang dibobotkan, Fungsi *print*() berfungsi untuk mencetak atau menampilkan objek ke perangkat keluaran (layar) atau ke file teks. *Classification* adalah teknik di mana kita bisa mengkategorikan data ke dalam sejumlah kelas yang telah ditentukan sebelumnya. Tujuan utama dari klasifikasi adalah untuk membantu praktisi data dalam menentukan kelas atau kategori dari data baru berdasarkan karakteristik data yang telah ada sebelumnya

Precision menggambarkan akurasi antara data yang diminta dengan hasil prediksi yang diberikan oleh model.

Precision = (TP) / (TP + FP)
= 107211 / (107211 + 450216)
= 0.19
= 0.19 * 100% = 0.19%

Recall atau *sensitivity* menggambarkan keberhasilan model dalam menemukan kembali sebuah informasi.

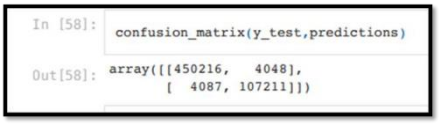
Recall = TP / (TP + FN)
= 107211 /(107211+4048)
= 0.96
= 0.96 * 100% = 0.96%

F-1 *Score* menggambarkan perbandingan rata- rata precision dan recall yang dibobotkan. Accuracy tepat kita gunakan sebagai acuan performansi algoritma jika dataset kita memiliki jumlah data False Negatif dan False Positif yang sangat mendekati (*symmetric*). Namun jika jumlahnya tidak mendekati, maka sebaiknya kita menggunakan F1 *Score* sebagai acuan.

F-1 *Score* = (2 * *Recall* * *Precision*) / (*Recall* + *Precision*)
= (2* 0.19 * 0.96) / (0.19 + 0.96)
= 0.3648 / 1.15
= 0.31 *100%
= 31%

Tabel 5 Hasil Perhitungan

Jenis Evaluasi	**Nilai %**
Precision	0.99 %
Recall	0.99 %
F1 Score	0.99 %



Gambar 4. Model Confusion Matrix

Matrix pada masing - masing serangan, serangan dapat dilihat pada serangan Bot precisionnya 0.99 *recall* 0.99, dan f1score 0.99

5. KESIMPULAN DAN SARAN

Pada pengujian deteksi serangan DDoS menggunakan metode *confusion matrix* didapatkan Bot *precision* nya 0.99 *recall* 0.99, dan *f1score* 0.99. Pada tahap implementasi Jaringan Saraf Tiruan menggunakan train tool pada aplikasi Matlab 2017 b terhadap hasil feature extraction metode *Fixed Moving Window* yang disimpan dengan nama "dataLatih" sehingga Jaringan Saraf Tiruan dapat mengenali data latih. Analisis dilakukan dengan menggunakan data latih dari dataset terbaru yaitu CICIDS2017 yang merupakan pengembangan dari dataset yang sudah ada sebelumnya. Sedangkan untuk data uji diperoleh dari hasil simulasi serangan DDoS ke *server web* yang diekstrak menggunakan Bahasa Pemograman *Python* sehingga menghasilkan data dengan format yang sama seperti data latih. Dua percobaan berbeda dilakukan pada penelitian ini, pada percobaan pertama, pelatihan dan pengujian dilakukan dengan menggunakan semua fitur yang ada pada data latih dan data uji yaitu sebanyak 40 fitur

DAFTAR REFERENSI

Dharma, M. A. A. (2014). Keamanan Jaringan Komputer "DOS, DDOS & cara penaggulangannya Disusun, (8053111064).

Muhammad, A. W. (2016). Analisis Statistik Log Jaringan Untuk Deteksi Serangan Ddos Berbasis Neural Network. Jurnal Ilmiah ILKOM, 8(Desember), 220–225. https://doi.org/10.13140/RG.2.2.19805.10723.

Mulyawan, Rifqi. (2019). "Mengenal Pengertian Smart me: Fungsi, Manfaat, Karakteristik, Kelebihan dan Kekurangannya".

Python Software Foundation, (2019) "General Python FAQ," Python SoftwareFoundation, [Online]. Available: https://docs.python.org/3/faq/general.html

Rosandy. T. (2016). Perbandingan Metode Naive Bayes Classifier Dengan Metode Decision Tree (C4.5) Untuk Menganalisa Kelancaran Pembiayaan (Study Kasus: Kspps / Bmt Al-Fadhila). Jurnal TIM Darmajaya.

Simon, Hendra Son (2020) Penentuan Posisi Objek Berbasis Image Processing Dengan Menggunakan Metode Convolutional Neural Network. UIB Repository.

Yulianto, A., Sukarno, P., Suwastika, N.A. 2018. *Improving AdaBoost-based Intrusion Detection System (IDS) Performance on CIC IDS 2017 Dataset*. IOP Conf. Series: Journal of Physics: Conf. Series 1192 (2019) 012018.