Methotika : Jurnal Ilmiah Teknik Informatika
ISSN : 2776 –5792
Vol. 3, No. 2, Oktober 2023, pp. 90-99
http://ojs.fikom-methodist.net/index.php/methotika

Analisis dan Implementasi IDS terhadap Serangan DDOS pada VPS Menggunakan Metode CNN

Obet Leon Siahaan[1], Naikson Fandier Saragih, Jimmy F. Naibaho[3]
[1,2,3]Fakultas Ilmu Komputer, Universitas Methodist Indonesia

Info Artikel

Histori Artikel:

Received, Juli, 2023
Revised, Agustus, 2023
Accepted, September, 2023

Keywords: (10pt)

Convolutional Neural Network, Deep-Learning, Batch Size, Epoch, Klasifikasi, Confusion Matrix.

ABSTRAK

Sistem deteksi serangan DDoS pada umumnya dilakukan pada sebuah server kovensional (*dedicated*) menggunakan *tools Snort* dan juga dengan berbagai pendekatan termasuk menggunakan *Artificial Intelligence Deep Learning*. Saat ini banyak perusahaan yang sudah menggunakan layanan *Virtual Private Server* sebagai pengganti servernya sehingga dibutuhkan riset terkait analisis dan implementasi deteksi serangan DDoS pada sebuah *Virtual Private Server*. Dengan Metode CNN dataset yang digunakan bersumber dari uji coba beberapa varian serangan DDoS pada Virtual Private Server selama 30 menit menggunakan tools LOIC versi 1.0.8.0. Data serangan dicapture menggunakan wireshark versi 3.6.7.0 sebanyak 39920 record yang selanjutnya diekstraksi dengan menggunakan CICFlowMeter 4.0, Hasil ekstraksi dataset sebanyak 38726 baris data. Pada python proses dilanjutkan dengan melakukan pembersihan data (*pre-processing)* didapatkan jumlah data menjadi 38704 dan normalisasi data dilakukan menggunakan min-max untuk mendapatkan nilai seluruh data minimum sebesar 0 dan nilai maksimum sebesar 1. Dari dataset sebanyak 38704 data dibagi menjadi data *training* dan data *testing* dengan perbandingan 70 : 30. Diperoleh 27093 data untuk training dan 11611 data untuk testing. Pengujian prediksi dalam hal ini deteksi dilakukan menggunakan algoritma CNN 1-Dimensional dengan mengatur jumlah epoch 20 dan batch size 32 didapatkan hasil *klasifikasi* dengan tingkat akurasi menggunakan *confusion matrix* yaitu 99.673%. Bila menggunakan Dataset serangan DDoS pada tanggal 21-02-2018 dari situshttps://www.unb.ca/cic/datasets/ids-2018.html sebagai *training* berjumlah 387040 baris data dan Dataset percobaan serangan DDoS pada VPS sebagai *testing* berjumlah 38704 baris data yang keduanya memiliki perbandingan 90 : 10, dan pengujian deteksi menggunakan algoritma CNN dengan mengatur jumlah epoch 5 dan batch size 64 didapatkan hasil *klasifikasi* dengan nilai akurasi 60.73%.

Penulis Koresponden:

Naikson Fandier Saragih,
Fakultas Ilmu Komputer,
Universitas Methodist Indonesia, Medan,
Jl. Hang Tuah No.8, Medan - Sumatera Utara.
Email: saragihnaikson@gmail.com

1. PENDAHULUAN

Intrusion detection system (IDS) merupakan suatu sistem yang dapat mendeteksi aktivitas yang abnormal dalam suatu sistem atau jaringan. Jika ditemukan kegiatan –

kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan [1][2].

Distributed Denial of Service (DDoS) adalah tindakan yang dapat mengakibatkan penurunan tingkat keamanan pada server atau sistem. Tujuan dari serangan DDoS adalah melumpuhkan sistem target dengan menghabiskan sumber daya jaringan atau sumber daya sistem yang dimiliki oleh pengguna tersebut. Kejadian serangan DDoS cukup umum terjadi di perusahaan dan instansi pemerintahan. Oleh karena itu, penelitian difokuskan pada serangan ini dengan tujuan mendeteksi dan mengklasifikasinya melalui data log jaringan.

Virtual Private Server (VPS) adalah teknologi virtualisasi yang memungkinkan pembuatan sebuah server virtual dengan alokasi pasti untuk *Central Processing Unit* (CPU), *Random-Access Memory* (RAM), dan penyimpanan tanpa memerlukan keberadaan fisik server. VPS saat ini telah menjadi pilihan umum bagi instansi pemerintahan dan perusahaan swasta sebagai solusi penyimpanan data secara virtual. Memastikan keamanan VPS sangat penting untuk mencegah potensi kerugian yang mungkin dialami oleh pengguna layanan VPS. [3][4].

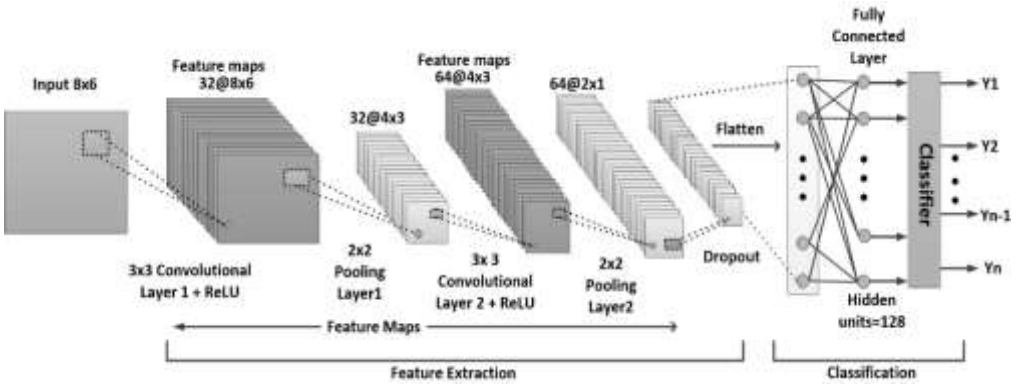
Deep Learning merupakan bagian dari *Neural Network* dengan memakai teknik tertentu yaitu *Restricted Boltzmann Machine* (RBM) menggunakan lapisan *Neural* yang sangat banyak atau bahkan lebih dari 7 lapisan. Waktu dalam melakukan training dengan menggunakan DL akan semakin cepat sebab hilangnya gradien pada masa tunggu (*Propagasi*) sehingga semakin cepat dalam memproses. *Deep learning* umumnya digunakan dalam menyelesaikan permasalahan yang terdapat pada data, mampu melakukan prediksi dalam jumlah dataset yang sangat besar [5].

Dalam beberapa tahun terakhir, istilah baru yang telah muncul dan menjadi fokus penelitian adalah *Deep Learning* berbasis IDS. Tantangan utama yang dihadapi adalah mendeteksi serangan jaringan dengan memanfaatkan kemampuan klasifikasi yang dimiliki oleh deep learning. Salah satu jenis *Deep Learning* yang banyak digunakan dalam klasifikasi serangan jaringan adalah *Convolutional Neural Network* (CNN). CNN adalah metode yang menggunakan Jaringan Saraf Tiruan (JST) untuk menyelesaikan masalah dengan memahami pola-pola melalui data [6]. Dalam sistem IDS, CNN bekerja dengan mengubah data log serangan jaringan menjadi format teks atau angka yang dapat digunakan sebagai dataset. Data log serangan DDoS ini kemudian diproses menggunakan metode CNN untuk memperoleh nilai akurasi yang akurat.

2. METODE PENELITIAN

2.1 Convolutional Neural Network (CNN)

CNN merupakan operasi yang menggabungkan lapisan-lapisan yang beroperasi secara paralel, hal ini terinspirasi dari sistem saraf biologis manusia CNN mepresentasikan setiap neuronnya kedalam bentuk 2 dimensi, sehingga metode ini merupakan pemrosesan input berupa citra [7]. Arsitektur convolutional neural network terlihat pada Gambar 2.4



Gambar 1. Arsitektur Convolutional Neural Network
Sumber M. Elsayed dkk, 2021

Berdasarkan pada gambar 2.4 diatas arsitektur CNN terbagi menjadi dua bagian besar:

1. Feature Extraction

Pada tahap ini, dilakukan proses encoding yang mengubah data input menjadi angka-angka yang merepresentasikan data tersebut. Layer ini terdiri dari dua komponen utama pada CNN, yaitu Convolutional Layer dan Pooling Layer.

2. Convolution Layer

Layer ini terdiri dari 32 filter, masing-masing berukuran 5x5. Oleh karena itu, total parameter yang akan dipelajari adalah 5x5x32=832 parameter. Pada Convolution Layer, data dari input diambil dengan dimensi panjang x tinggi sesuai dengan ukuran filter. Misalnya, jika ukuran filter adalah 3x3 dan ukuran data input adalah 5x5, maka dimensi dari data input yang diambil sesuai dengan ukuran filter yaitu 3x3. Proses perkalian dilakukan sebanyak jumlah filter yang digunakan. Penting dicatat bahwa dalam arsitektur CNN, Convolution Layer umumnya menggunakan lebih dari satu filter [5].

3. Pooling Layer

Pooling layer berfungsi sebagai pencari fitur melalui citra pada layer yang diperoleh sebelumnya. Tugas utama dari Pooling layer adalah mengurangi ukuran data. Terdapat beberapa jenis pooling yang digunakan, yaitu *Sum Pooling, Average Pooling,* dan *Max Pooling*. *Max pooling* bekerja dengan mengambil nilai terbesar dalam suatu area, sedangkan average pooling mengambil nilai rata-rata dari area tersebut. Dari dua metode tersebut, *max pooling* adalah yang paling umum digunakan, sementara *average pooling* jarang ditemui dalam banyak arsitektur jaringan [5]

Classification.

4. Fully Connected Layer

Lapisan tersebut merupakan lapisan yang digunakan sebagai penerapan MLP serta bertujuan sebagai melakukan transformasi dalam dimensi data supaya data mampu diklasifikasikan menjadi linear. Setiap jaringan suatu convolution layer akan bertransformasi sebagai data dalam suatu dimensi terdahulu sebelum dimasukkan pada sebuah fully-connected layer. Karena hal tersebut menyebabkan data kehilangan informasi spasialnya dan tidak reversibel, fullyconnected layer hanya dapat diimplementasikan di akhir jaringan [6].

5. Loss Layer

Loss layer merupakan lapisan terakhir dalam arsitektur CNN di mana pada tahap ini hasil prediksi dan nilai kerugian (loss) dipertimbangkan selama proses pelatihan.

2.2 Confusion Matrix

Confusion Matrix adalah suatu metode yang digunakan dalam pengukuran suatu klasifikasi. Pada *Confusion Matrix* memiliki tabel yang punya 4 kombinasi berbeda dari nilai aktual dan nilai prediksi. Terdapat empat sebutan yang menjadi representasi hasil suatu klasifikasi dalam *confusion matrix* adalah *False Positif* (FP), *False Negatif* (FN), *True Positif* (TP), dan *True Negatif* (TN). Penilaian pada *True-Positive* dan *True-Negative* memberikan informasi ketika *classifier* melakukan klasifikasi data dengan benar, sementara *False-Positive* dan *False-Negative* memberikan informasi ketika classifier melakukan kesalahan dalam klasifikasi data.Berikut confusion matrix ditunjukkan pada Tabel 2.1

Tabel 1. Confusion Matrix

Sample classes		**Prediksi**	
		Positive	**Negative**
Class Benar	**Positive**	**TP**	**FP**
	Negative	**FN**	**TN**

Dalam prediksi yang dilakukan oleh model klasifikasi, Confusion Matrix akan menganalisis seberapa baik model klasifikasi yang dibuat dengan melihat nilai:

a. Accuracy mengukur seberapa akurat model dapat mengklasifikasikan data dengan benar.

Accuracy = (TP) / (Total dataset)

b. Precision (Positive Predictive Value) menggambarkan tingkat keakuratan antara data prediksi benar positif yang diminta dengan hasil prediksi yang diberikan oleh model.

Precision = (TP) / (TP + FP)

c. Recall atau sensitivity (True Positive Rate) menggambarkan keberhasilan model dalam menemukan kembali sebuah informasi.

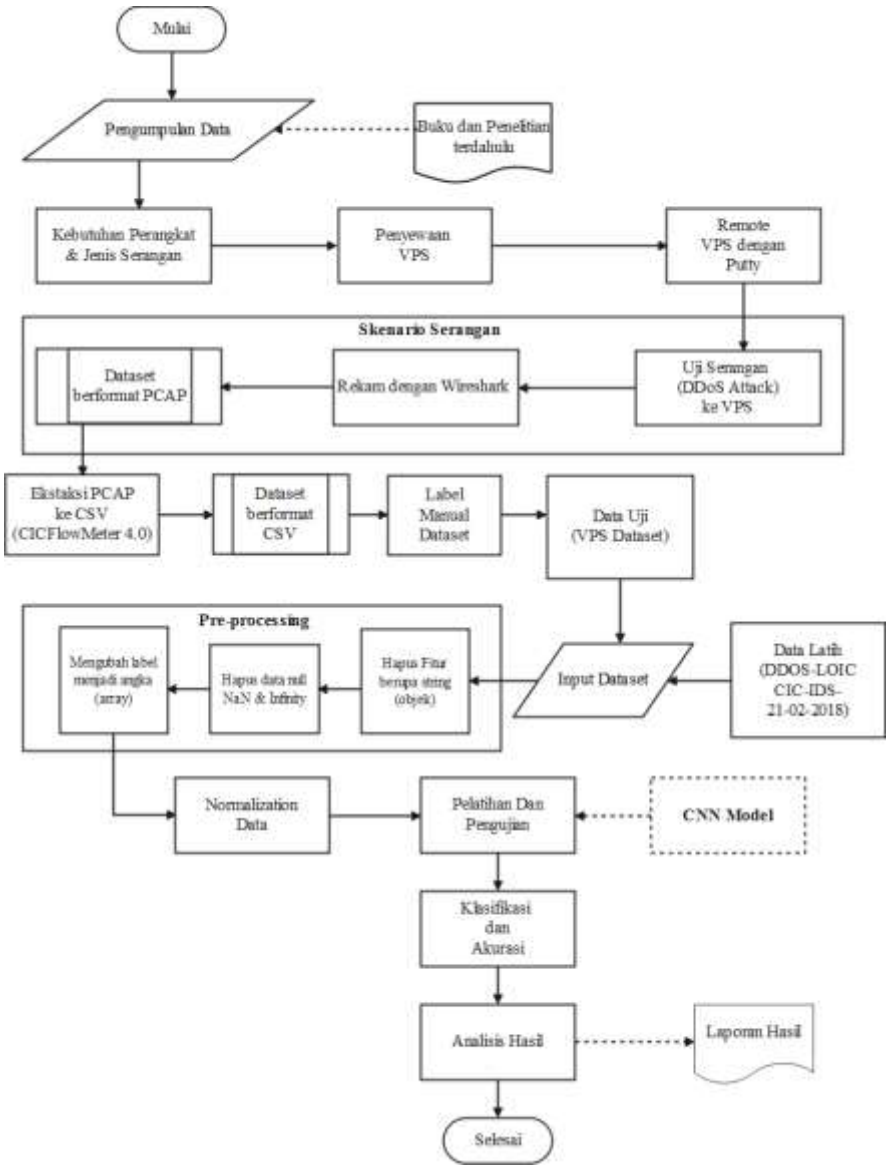
Recall = TP / (TP + FN)

d. F-1 Score menggambarkan perbandingan rata-rata precision dan recall yang dibobotkan.

F-1 Score = (2 * Recall * Precision) / (Recall + Precision)

2.3 Framework Penelitian

Framework penelitian adalah kerangka kerja yang digunakan dalam suatu penelitian, terdiri dari beberapa tahapan yang dijelaskan dalam flowchart seperti yang terlihat pada Gambar 1.berikut :



Gambar 2. Framework Penelitian

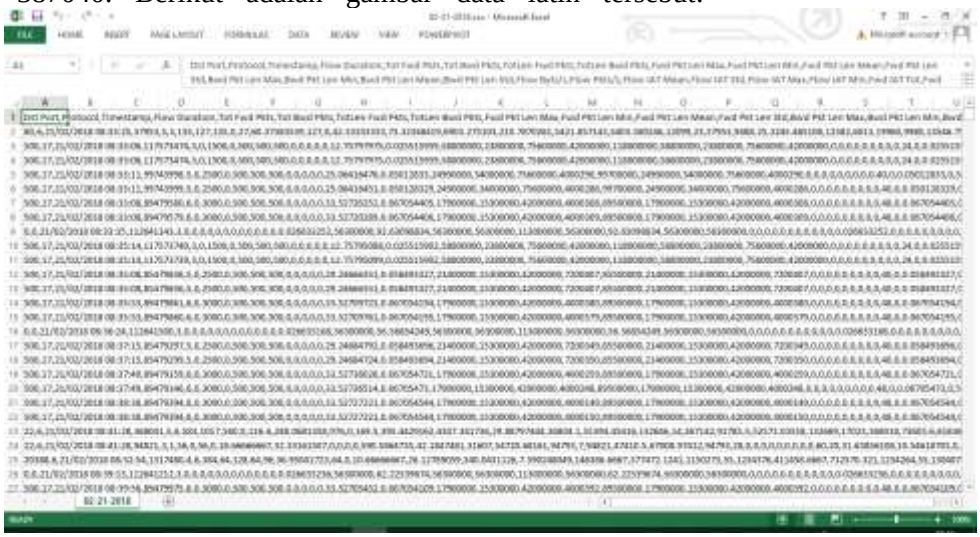
2.4 Dataset

Dataset dibagi menjadi dua bagian, yaitu data latih (Training) dan data uji (Testing), dengan perbandingan pembagian data sebesar 90% untuk data latih dan 10% untuk data uji. Data uji berasal dari hasil pengujian skenario serangan terhadap VPS, sementara data latih diambil dari situs web https://www.unb.ca/cic/datasets/ids-2018.html. Kedua dataset ini digunakan dalam penelitian untuk mengembangkan dan menguji model pengklasifikasi.:

a. Data Latih (Training)

Data latih diperoleh dari situs resmi milik *Canadian Institute for Cybersecurity*. Data yang didwonload yakni daftar serangan harian DDoS berdasarkan pada hari rabu tanggal 21-02-2018. Adapun durasi pengujian dimulai dari pukul 10:09 hingga pukul 10:43. Data

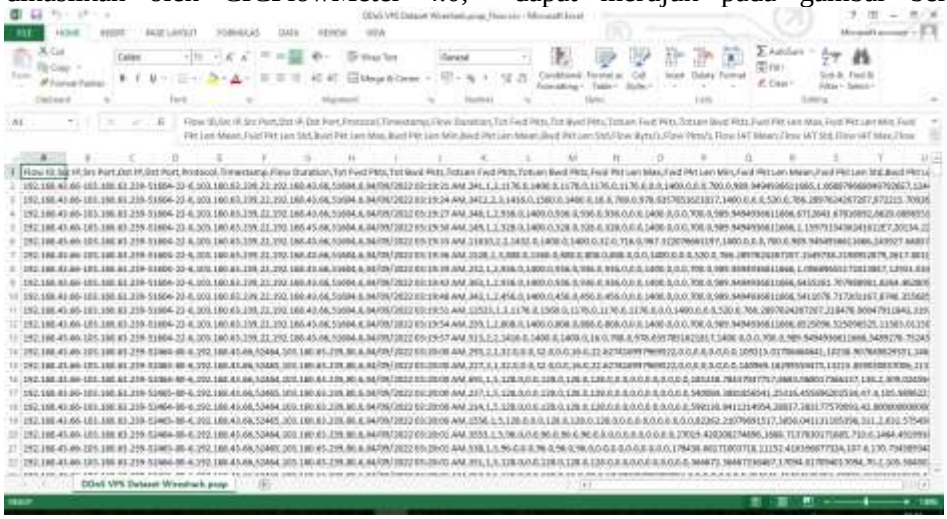
yang diperoleh berjumlah 1048575 baris data, namun data yang digunakan untuk pelatihan berjumlah 387040. Berikut adalah gambar data latih tersebut:



Gambar 4. Data Latih (Training)

b. Data Uji (Testing)

Data uji yang digunakan berasal dari hasil skenario serangan DDoS pada VPS. Pengujian serangan terhadap VPS menghasilkan jumlah 38.725 data. Hasil ini diekstrak menggunakan alat CICFlowMeter 4.0 dan disimpan dalam format CSV. Untuk melihat dataset yang dihasilkan oleh CICFlowMeter 4.0, dapat merujuk pada gambar berikut.:



Gambar 3. Data Uji (Testing)

c. Label Data

Label dalam dataset telah diubah menjadi dua kategori, yaitu "Benign" (Normal) dan "DDOS," dan kemudian diubah menjadi bentuk array seperti yang ditunjukkan dalam tabel transformasi di bawah ini:

Tabel 2. Transformasi Label menjadi angka

Nama Serangan	Representasi Angka	Representasi dengan *label encoder*
Benign (Normal)	0	1,0,0,0
DDOS	1	0,1,0,0

2.5 Skenario pembagian dataset

a. Dataset VPS

Pembagian dataset dilakukan dengan rasio 70:30, di mana 70% dari data digunakan untuk pelatihan (data training) dan 30% digunakan untuk pengujian (data testing). Berikut adalah representasi dari pembagian dataset tersebut:

Tabel 3. Pembagian dataset

Data latih (70%)	**Data uji (30%)**
38704 x 0,7 = 27093 baris data	38704 x 0,3 = 11611 baris data

b. Dataset DDoS 02-21-2018 (training) dan Dataset VPS (testing)

Pemisahan dataset dilakukan dengan rasio 90:10, dimana 90% data digunakan untuk pelatihan dan 10% data digunakan untuk pengujian. Informasi ini dapat ditemukan dalam tabel berikut:

Tabel 4. Pembagian dataset

Data latih (90%)	**Data uji (10%)**
387040 baris data	38704 baris data

6. HASIL DAN PEMBAHASAN

3.1 Normalisasi Data

Normalisasi dilakukan untuk mengubah nilai minimum dan maksimum pada data agar semua nilai pada fitur memiliki rentang nilai yang sama. Metode Min-Max bertujuan untuk normalisasi data dengan menyetarakan range setiap variabel satu dengan variabel lain. Nilai pada data mempunyai nilai minimum sebesar 0 dan nilai maksimum sebesar 1. Persamaan untuk Min-Max adalah sebagai berikut:

$$X' = \frac{(X_n - X_{min})}{(X_{max} - X_{min})}$$

X' : Data hasil normalisasi
X_n : Data Asli
X_{min} : nilai minimum dari data x
X_{max} : nilai maksimum dari data x

Adapun perhitungan normalisasi dari dataset menggunakan rumus min-max pada excell adalah sebagai berikut :

$X'_{Src\ \ Port} = \frac{(X_1 - X_{min})}{(X_{max} - X_{min})} = \frac{(63354-0)}{(63355-0)} = 0{,}999984216$

$X'_{\text{Dst Port}} = \frac{(X_1 - X_{min})}{(X_{max} - X_{min})} = \frac{(80-0)}{(51604-0)} = 0{,}0015503$

$X'_{\text{Protocol}} = \frac{(X_1 - X_{min})}{(X_{max} - X_{min})} = \frac{(17-0)}{(17-0)} = 1$

$X'_{\text{Flow Duration}} = \frac{(X_1 - X_{min})}{(X_{max} - X_{min})} = \frac{(20540-0)}{(71931-0)} = 0.2855514312327091$

$X'_{\text{Tot Fwd Pkts}} = \frac{(X_1 - X_{min})}{(X_{max} - X_{min})} = \frac{(1-0)}{(13-0)} = 0.07692307692307693$

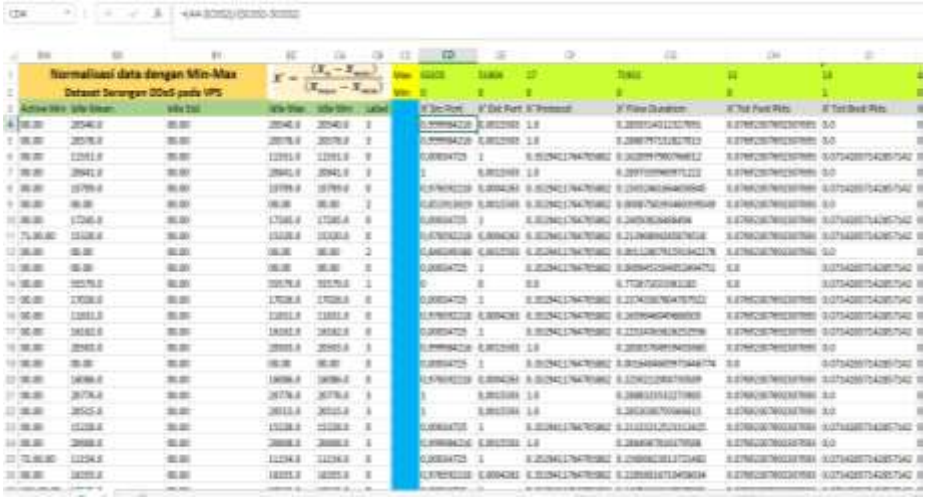
$X'_{\text{Tot Bwd Pkts}} = \frac{(X_1 - X_{min})}{(X_{max} - X_{min})} = \frac{(1-1)}{(13-1)} = 0.0$

Gambar dataset sebelum dilakukannya proses perhitungan normalisasi dengan min-max dapat dilihat pada gambar berikut :

	A	B	C	D	E	F	G	H	I	J	K
1	Src Port	Dst Port	Protocol	Flow Duration	Tot Fwd Pkts	Tot Bwd Pkts	TotLen Fwd Pkts	TotLen Bwd Pkts	Fwd Pkt Len Max	Fwd Pkt Len Min	Fwd Pkt Len Mean
4	61354	80	17	20540	1	1	32.00.00	32.00.00	32.00.00	32.00.00	32.00.00
5	61354	80	17	20578	1	1	32.00.00	32.00.00	32.00.00	32.00.00	32.00.00
6	22	51604	6	11660	1	2	64.00.00	64.00.00	64.00.00	64.00.00	64.00.00
7	61355	80	17	20841	1	1	32.00.00	32.00.00	32.00.00	32.00.00	32.00.00
8	61872	22	6	10813	1	2	00.00	128.00.00	00.00	00.00	00.00

Gambar 5. Dataset sebelum Normalisasi

Dataset hasil setelah dilakukan perhitungan normalisasi dengan menggunakan min-max dapat dilihat pada Gambar berikut :



Gambar 6. Hasil perhitungan normalisasi min-max

3.2 Implementasi Sistem

Tahap implementasi melibatkan penerapan dan pengujian sistem berdasarkan hasil analisis dan perancangan yang telah dilakukan sebelumnya. Dalam penelitian ini, langkah awal dalam membangun sistem adalah dengan menyewa layanan VPS dari provider herza.id.

3.3 Pengujian Sistem

Pengujian sistem telah dilakukan dengan melakukan serangan pada VPS menggunakan tools Loic. Pengujian serangan dilaksanakan pada hari Minggu, tanggal 4 September 2022, mulai dari pukul 03.20.00 hingga 03.55.02, dengan total waktu sekitar 35 menit. Serangan pertama yang dilakukan adalah TCP Flood, berlangsung selama 5 menit. Serangan kedua adalah aliran Normal pertama, berdurasi 6 menit 28 detik. Serangan ketiga adalah UDP Flood, dengan durasi 5 menit. Serangan keempat merupakan aliran Normal kedua, berlangsung selama 5 menit 53 detik. Serangan terakhir adalah ICMP Flood, dengan durasi 10 menit. Berikut adalah tabel yang menunjukkan durasi skenario serangan DDoS dan aliran normal yang telah dilakukan: :

Tabel 5. Durasi pengujian Serangan DDoS dan Aliran Normal

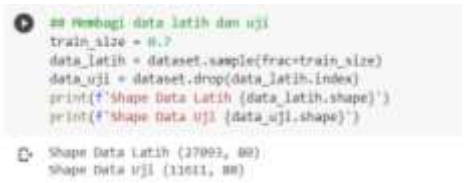
IP Penyerang	IP Tujuan	Nama	Mulai	Selesai
192.168.43.66	103.160.63.239	DDOS attack-LOIC-TCP	03.20.00	03.25.00
192.168.43.66	103.160.63.239	Benign (Normal) Pertama	03.25.01	03.31.29
192.168.43.66	103.160.63.239	DDOS attack-LOIC-UDP	03.32.00	03.37.00
192.168.43.66	103.160.63.239	Benign (Normal) Kedua	03.37.24	03.44.17

192.168.43.66	103.160.63.239	DDOS	attack-ICMP	03.45.01	03.55.02

3.4 Tampilan sistem

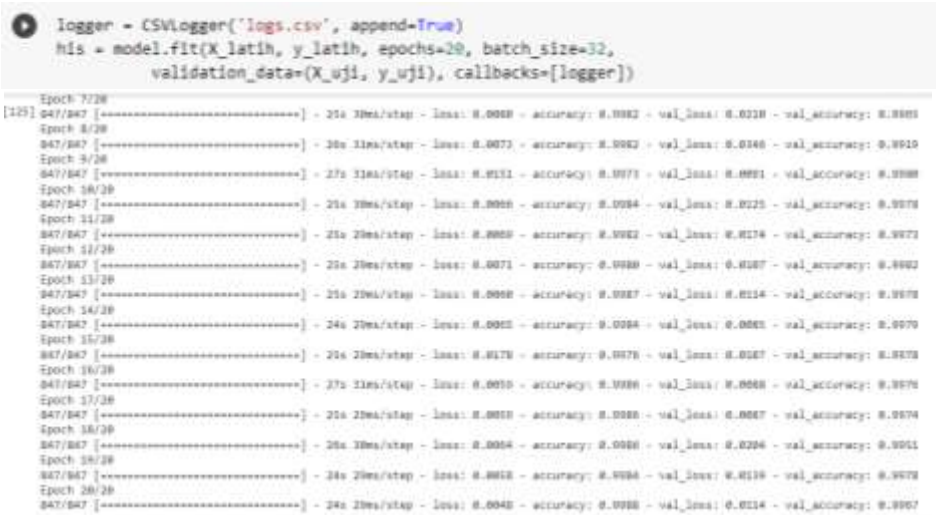
1. Dataset Serangan DDoS VPS

Pembagian dataset Serangan DDoS VPS antara data latih dan data uji yaitu dengan split 70:30. Berikut ini adalah proses pembagian dataset :



Gambar 7. Proses pembagian data latih dan data uji

Dapat dilihat pada gambar 7 proses pembagian dataset dengan split 70:30 mendapatkan jumlah data training 27093 baris data dan jumlah data testing 11611 baris data. Dari hasil setiap epoch tersebut merata tidak ada peningkatan maupun penurunan yang sangat berlebihan. Berikut gambar hasil dari setiap epoch pada saat proses pelatihan dan pengujian :

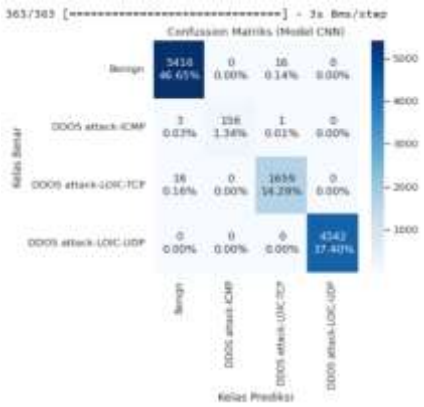


Gambar 8. Hasil dataset VPS dengan epoch 20

Pada gambar 8 telah dilakukan proses pembalajaran mesin dengan menggunakan model CNN, fungsi loss categorical crasstropy, fungsi optimizer adam, metrics accuracy, batchsize 32, dan epoch sebanyak 20. Adapun gambar nilai akurasi dan loss sebagai berikut :

Gambar 9. Hasil Nilai Akurasi dataset VPS

Dapat dilihat pada gambar 9 nilai akurasi yang didapat dari proses pelatihan dan pengujian model CNN adalah 99,673%. Berikut gambar menunjukan hasil dari Confusion Matrix :



Gambar 10. Confusion Matrix kelas benar dan prediksi

Pada gambar ke-10 dari confusion matrix, terdapat hasil pendeteksian klasifikasi serangan DDoS pada dataset VPS. Terdapat total 5416 data yang tergolong dalam kelas Normal (Benign), 156 data terkait serangan ICMP Flood, 1659 data terkait serangan TCP Flood, dan 4342 data terkait serangan *UDP Flood*.

2. Dataset DDoS 02-21-2018 dan Dataset serangan DDoS VPS

Pembagian dataset DDoS pada tanggal 02-21-2018 dilakukan sebagai data latih (training) dan dataset serangan DDoS VPS digunakan sebagai data uji (testing) dengan metode pembagian 90% untuk data latih dan 10% untuk data uji. Berikut adalah ilustrasi pembagian komposisi data latih dan data uji dalam program Python :

```
[ ] #normalisasi data
    from sklearn.preprocessing import MinMaxScaler

    mm = MinMaxScaler()
    X_train = mm.fit_transform(X_train)
    X_test = mm.fit_transform(X_test)
    print(X_train.shape)
    print(X_test.shape)

    (387040, 78)
    (38704, 78)
```

Gambar 11. Jumlah Dataset latih DDoS 02-21-2018 dan dataset uji VPS

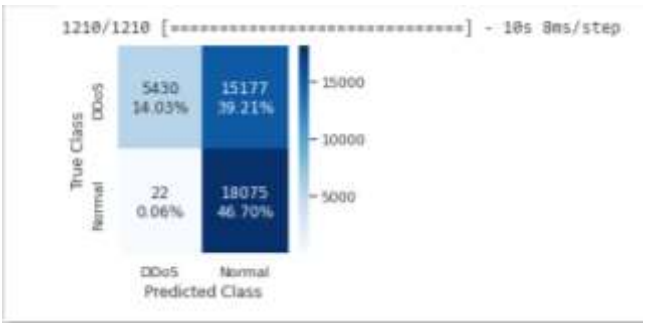
Dapat dilihat pada gambar 11 proses pembagian dataset dengan split 90:30 mendapatkan jumlah data training 387040 baris data dan jumlah data testing 38704 baris data. Berikut hasil gambar proses setiap epoch antara dataset serangan DDoS 02-21-2018 sebagai *training* dan dataset serangan DDoS VPS sebagai *testing*:

Gambar 12. Hasil setiap epoch dataset training DDoS 02-21-2018 dan dataset testing VPS

Pada gambar 12 telah dilakukan proses pembalajaran mesin dengan menggunakan model CNN, fungsi loss categorical crasstropy, fungsi optimizer adam, metrics accuracy, batchsize 64, dan epoch sebanyak 5. Adapun gambar nilai akurasi adalah sebagai berikut :

Gambar 13. Hasil Nilai Akurasi data latih DDoS 02-21-2018 dan data uji VPS

Pada gambar 13 Hasil nilai akurasi yang didapat dari proses pelatihan dan pengujian model CNN adalah 60,73%. Berikut gambar menunjukan hasil dari Confusion Matrix deteksi serangan DDoS:



Gambar 14. Confusion Matrix kelas benar dan prediksi

Dapat dilihat pada gambar 14 hasil confusion matrix dataset serangan DDoS 02-21-2018 sebagai training 90% dan dataset serangan DDoS pada VPS sebagai *testing* 10% hasil pendeteksian klasifikasi prediksi benar didapat sebanyak 5416 data untuk kelas serangan DDoS, dan sebanyak 18075 data untuk kelas Normal (Benign).

KESIMPULAN

Berdasarkan hasil percobaan klasifikasi serangan DDoS menggunakan metode CNN, beberapa temuan signifikan dapat diidentifikasi:

1. Dalam pengujian menggunakan dataset serangan DDoS pada VPS, dilakukan pembagian data dengan rasio 70:30, yaitu 27093 baris data untuk pelatihan dan 11611 baris data untuk pengujian. Model CNN dijalankan dengan 20 epoch dan batch size 32. Hasil pengujian menggunakan confusion matrix menunjukkan tingkat akurasi sebesar 99.673%. Dengan hasil ini, dapat disimpulkan bahwa model CNN yang digunakan sangat baik, hampir mendekati nilai 100%.
2. Selanjutnya, pada pengujian menggunakan Dataset DDoS 02-21-2018 sebagai data pelatihan dan dataset serangan DDoS VPS sebagai data pengujian, dilakukan pembagian data dengan rasio 90:10, yaitu 387040 data untuk pelatihan dan 38704 data untuk pengujian. Model CNN dijalankan dengan 5 epoch dan batch size 64. Hasil pengujian menggunakan confusion matrix menunjukkan tingkat akurasi sebesar 60.73%. Dapat disimpulkan bahwa hasil yang diperoleh dapat dikategorikan sebagai predikat sedang.

Demikianlah hasil dari percobaan klasifikasi serangan DDoS menggunakan metode CNN yang dilakukan..

REFERENSI

[1] H. Aliyasa Almaj Duddin and A. Senja Fitrani, “Pengamanan Proses Input Output Pada Web Untuk Meminimalisir Serangan SQL-Injection dan XSS Menggunakan Metode IDS dan IPS,” *Network, Comput. Sci.* |, vol. 4, no. 1, pp. 6–12, 2021.

[2] L. Feronika Nainggolan, N. F. Saragih, F. G. N. Larosa, and H. Artikel, “Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort

IDS," *J. Ilm. Tek. Inform.*, vol. 2, no. 2, pp. 1–10, 2022, [Online]. Available: http://ojs.fikom-methodist.net/index.php/METHOTIKA

[3] M. Syani, "Implementasi Intrusion Detection System (Ids) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (Vps)," *J. Inkofar*, vol. 1, no. 1, pp. 13–20, 2020, doi: 10.46846/jurnalinkofar.v1i1.155.

[4] N. F. Saragih, R. Agus, W. Nanda, and M. J. Purba, "FORENSIC NETWORK ANALYSIS AND IMPLEMENTATION OF SECURITY ATTACKS ON VIRTUAL PRIVATE SERVERS," vol. 6, no. 2, pp. 28–35, 2023.

[5] A. Ahmad Hania, "Mengenal Artificial Intelligence, Machine Learning, & Deep Learning," *J. Teknol. Indones.*, vol. 1, no. June, pp. 1–6, 2017, [Online]. Available: https://amt-it.com/mengenal-perbedaan-artificial-inteligence-machine-learning-deep-learning/

[6] Y. B. E. Purba, N. F. Saragih, A. P. Silalahi, and Et al, "Perancangan Alat Pendeteksi Kematangan Buah Nanas Dengan Menggunakan Mikrokontroler Dengan Metode Convolutional Neural Network (CNN)," *J. Ilm. Tek*, vol. 2, no. 1, pp. 13–21, 2022.

[7] X. Zhang, J. Ran, and J. Mi, "An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic," *Proc. IEEE 7th Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2019*, pp. 456–460, 2019, doi: 10.1109/ICCSNT47585.2019.8962490.

[8] Michelucci, Umberto, and Umberto Michelucci. "Fundamentals of convolutional neural networks." Advanced Applied Deep Learning: Convolutional Neural Networks and Object Detection (2019): 79-123

[9] Suartika, E. P. I. W., A. Y. Wijaya, and R. Soelaiman. "Image Classification Using Convolutional Neural Network (CNN) on Caltech 101." Jurnal Teknik ITS 5.1 (2016).

[10] Putri, B. (2021). *Klasifikasi Serangan Brute Force Menggunakan Metode Convolutional Neural Network (CNN)*. Indralaya : *Universitas Sriwijaya*.

[11] Lashkari A. H. *et al.* (2017). Characterization *of Tor Traffic using Time based Features.*
Fredericton : *Canadian Institute for Cybersecurity (CIC) & University of New Brunswick (UNB).*

[12] Ali, S. (2022, Juli). *Intrusion Detection System Using CNN feee44*. Retrieved from Kaggle : https://www.kaggle.com/code/shamshairali007/intrusion-detection-system-using-cnn-feee44
/notebook.