JUMANJI
ISSN (p): 2598-8050
ISSN (e): 2598-8069
| Vol. 7 | No. 2 | Halaman 61 - 71
Oktober 2023

Kecerdasan Buatan untuk Klasifikasi Serangan Siber pada Internet of Things Network Traffic

Randi Rizal[1], Nur Widiyasono[2], Siti Yuliyanti[3]

[1,2,3]Departemen Informatika, Fakultas Teknik, Universitas Siliwangi, Indonesia

Email: randirizal@unsil.ac.id

ABSTRAK

Internet of Things (IoT) merupakan arsitektur yang menghubungkan perangkat pintar dalam jumlah yang banyak pada sistem jaringan global modern saat ini. Serangan Distributed denial of services (DDoS) menjadi salah satu jenis serangan siber yang paling umum dengan menargetkan server atau jaringan dengan tujuan mengganggu aktivitas normalnya. Meskipun deteksi dan mitigasi serangan DDoS secara real-time sulit dicapai, solusinya akan sangat berharga karena serangan dapat menyebabkan kerusakan yang signifikan. Penelitian ini memanfaatkan artificial intelligence (AI) untuk mengklasifikasi serangan pada lalu lintas jaringan Internet of Things (IoT). Dihasilkan klasifikasi serangan DDOS dari semua jenis serangan yaitu SYN, ACK, UDP, dan UDPplain. Penerapan model deep learning dengan algoritma Convolutional Neural Network (CNN) digunakan untuk mengklasifikasikan lalu lintas normal dari serangan siber DDoS. Algoritma CNN berkinerja sangat baik dalam proses pengklasifikasi dengan akurasi 99%. Penelitian selanjutnya, berencana membangun model baru untuk memblokir atau memitigasi serangan DDoS berdasarkan keluaran dari algoritma klasifikasi CNN yang digunakan dalam penelitian ini.

***Kata kunci**: IoT, DDoS, CNN, Artificial Intelligence (AI).*

ABSTRACT

Internet of Things (IoT) is an architecture that connects large numbers of smart devices in today's modern global network system. Distributed denial of services (DDoS) attacks are one of the most common types of cyber attacks, targeting servers or networks with the aim of disrupting their normal activities. Although real-time detection and mitigation of DDoS attacks is difficult to achieve, the solution would be invaluable as attacks can cause significant damage. This research utilizes artificial intelligence (AI) to classify attacks on Internet of Things (IoT) network traffic. The resulting classification of DDOS attacks from all types of attacks, namely SYN, ACK, UDP, and UDPplain. The application of a deep learning model with the Convolutional Neural Network (CNN) algorithm is used to classify normal traffic from DDoS cyber attacks. The CNN algorithm performs

very well in the classification process with an accuracy of 99%. Next, we plan to build a new model to block or mitigate DDoS attacks based on the output of the CNN classification algorithm used in this research.

***Keywords**: IoT, DDoS, CNN, Artificial Intelligence (AI).*

1. PENDAHULUAN

Internet of Things (IoT) merupakan arsitektur yang menghubungkan perangkat pintar dalam jumlah yang banyak pada sistem jaringan global modern saat ini (Vashi et al., 2017), (Goyal et al., 2021). Ketika Internet of Things (IoT) diimplementasikan, perangkat fisik atau *node* IoT terhubung ke internet sehingga memungkinkan mereka mengumpulkan dan bertukar data dengan node lain di jaringan tanpa memerlukan partisipasi manusia (Al-Masri et al., 2020). Menurut Gartner teknologi IoT berkembang dengan sangat cepat, pada tahun 2015 sebanyak 15 miliar perangkat saling terhubung dengan kemungkinan peningkatan menjadi 38 miliar perangkat pada tahun 2025. IoT adalah jaringan objek yang dihubungkan oleh *sensor*, *actuator, gateway* dan layanan *cloud* yang memberikan layanan kepada pengguna (Belli et al., 2020), (Sethi & Sarangi, 2017).

Intrusion Detection System (IDS) secara tradisional hanya berhasil ketika berhadapan dengan data yang bergerak lambat atau dengan volume data yang kecil (Alam & Awan, 2018), sehingga tidak efisien ketika berhadapan dengan data atau jaringan besar dan tidak mampu menangani transmisi data berkecepatan tinggi. Oleh karena itu, teknologi yang mampu menangani data dalam jumlah besar dan mengidentifikasi indikasi penetrasi jaringan menjadi sangat penting. Ketika berhubungan dengan data dalam jumlah besar, keamanan dan privasi data menjadi masalah yang sangat mendesak, terutama dalam konteks serangan jaringan (Privalov et al., 2019). Serangan *Distributed denial of services (DDoS)* adalah salah satu jenis serangan siber yang paling umum dengan menargetkan server atau jaringan dengan tujuan mengganggu aktivitas normalnya (Nishanth & Mujeeb, 2021). Meskipun deteksi dan mitigasi serangan DDoS secara *real-time* sulit dicapai, solusinya akan sangat berharga karena serangan dapat menyebabkan kerusakan yang signifikan (Gupta et al., 2021).

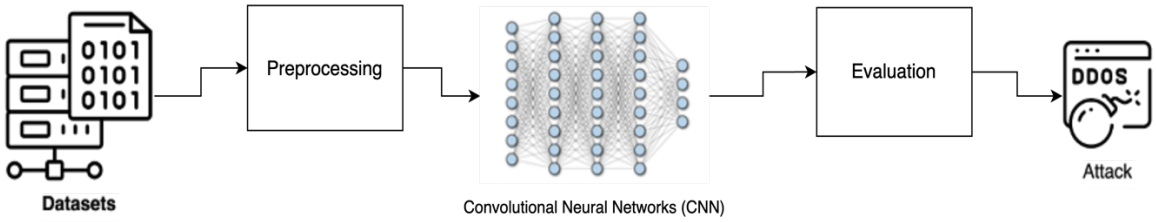
Penelitian *Machine Learning (ML)* yang dianggap sebagai komponen *Artificial Intelligence (AI)* selalu ditingkatkan melalui penggunaan data pelatihan dan eksploitasi informasi yang tersedia. Bergantung pada informasi yang diberikan, berbagai jenis pembelajaran dapat dilakukan, termasuk pembelajaran yang diawasi. Misalnya, algoritma Support Vector Machine (SVM) dan algoritma K-Nearest Neighbour (KNN), pembelajaran Semi-Supervised dan unsupervised. Model *Deep learning (DL)* yang dikombinasikan dengan teknik ML memberikan hasil yang luar biasa dalam sistem keamanan siber yang digunakan untuk mendeteksi serangan. Teknik ML digunakan dalam berbagai konteks, seperti dalam layanan kesehatan. Misalnya, data ini digunakan untuk memperkirakan wabah covid-19 dan masalah kesehatan lainnya.

Banyak peneliti menggunakan algoritma klasifikasi untuk mendeteksi dan mengatasi serangan DDoS dengan tujuan mengurangi jumlah serangan. Serangan DDoS mudah dilakukan karena memanfaatkan kelemahan jaringan dan menghasilkan permintaan layanan perangkat lunak (Sestrem Ochôa et al., 2021). Serangan DDoS membutuhkan waktu lama untuk diidentifikasi dan diklasifikasi (Sanmorino, 2019). Terdapat kelemahan yang signifikan pada metode yang saat ini digunakan untuk mendeteksi serangan DDoS, seperti biaya pemrosesan yang tinggi dan ketidakmampuan menangani sejumlah data besar yang mencapai server. Dengan menggunakan berbagai metode klasifikasi, algoritma klasifikasi membedakan paket DDoS dari jenis paket lainnya. Untuk mengamankan jaringan IoT dari serangan musuh yang tidak wajar, berbagai solusi peningkatan keamanan dikembangkan. Pendekatan ini sering digunakan untuk mendeteksi serangan di jaringan IoT dengan memantau operasi node IoT, seperti kecepatan pengiriman data.

Dalam penelitian ini, dibahas tentang penerapan *Artificial Intelligence (AI)* untuk identifikasi dan klasifikasi serangan siber pada lalu lintas jaringan Internet of Things (IoT). Kontribusi dalam penelitian ini menggunakan pendekatan *Deep Learning* untuk deteksi serangan dengan algoritma CNN dalam menghasilkan akurasi yang lebih baik.

2. METODOLOGI

Metodologi dalam penelitian ini diilustrasikan pada Gambar 1. Dimulai dari persiapan *dataset*, kemudian proses *preprocessing*, dan proses pemodelan. Tahap terakhir adalah mengevaluasi hasil proses pemodelan.



Gambar 1. Metodologi

2.1. Dataset

Pengumpulan *dataset* dikumpulkan dari berbagai sumber. Dalam penelitian ini, sumber yang digunakan hanya *dataset* publik yang berasal dari *UCI Repository* https://archive.ics.uci.edu. Semua informasi dalam *dataset* dikumpulkan dan diatur berdasarkan fungsi dan jenisnya.

Tabel 1. Perangkat IoT

Nama Perangkat IoT	Spesifikasi Perangkat
Provision PT-737E	- Wireless support 802.11b/g/n - Port 80 UDP - Camera Quality 1MP(720p) - Kode Pro 7
Provision PT-838	- Wireless support 802.11b/g/n - Port 80 UDP - Camera Quality 2MP(1080p) - Kode Pro 8
SimpleHome XCS7-1002- WHT	- Wireless support 802.11b/g/n - Port 80 UDP

	- Camera Quality 1MP(720p) - Kode Sam 7
SimpleHome XCS7-1003- WHT	- Wireless support 802.11b/g/n - Port 80 UDP - Camera Quality 1MP(720p) - Kode Sam 8

Tabel 1 adalah daftar perangkat IoT yang terinfeksi botnet dengan jenis serangan Bashlite dan Mirai. Empat perangkat IoT terinfeksi Bashlite dan Mirai Botnet di kumpulan kedalam dataset N-BaIoT. Jenis serangan pada tahap ini adalah mengumpulkan dan mengklasifikasi jenis serangan DDOS yang akan diselidiki pada beberapa perangkat IoT. Serangan Bashlite dan Mirai adalah serangan yang dipilih untuk implementasi pada penelitian ini.

Tabel 2. Jenis Serangan IoT

Nama Serangan	Deskripsi
Bashlite	
Scan	Memindai kerentanan perangkat IoT
Junk	Membanjiri dengan mengirim data spam
UDP	Membanjiri perangkat IoT dengan paket IP yang berisi datagram UDP
TCP	Membanjiri perangkat IoT dengan mengirimkan paket TCP
Combo	Mengirim data spam dan membuka koneksi ke alamat IP dan port tertentu.
Mirai	
Scan	Pemindaian otomatis untuk perangkat yang rentan
ACK	Membanjiri perangkat IoT dengan mengirimkan paket ACK palsu
SYN	Membanjiri perangkat IoT dengan mengirimkan paket SYN
UDP	Membanjiri perangkat IoT dengan paket IP yang berisi datagram UDP
UDPplain	Serangan UDP tetapi dengan jumlah paket yang lebih banyak

Tabel 2 adalah jenis serangan botnet Bashlite dan Mirai yang diluncurkan pada perangkat IoT dengan tipe serangan tersebut memiliki 10 tipe serangan, yang mana cara kerjanya membanjiri server perangkat IoT, dan jenis serangan sisanya adalah memindai perangkat IoT yang rentan secara otomatis. Pada tabel 3 menjelaskan tentang jumlah kejadian untuk setiap jenis serangan untuk setiap jenis perangkat IoT.

Tabel 3. Jumlah Kejadian untuk Setiap Jenis Serangan pada Perangkat IoT

Botnet	Attack	Doorbell	Thermostat	Baby Monitor	Security Camera
Benign		88,648	13,113	175,240	226,781
Bashlite	**Combo**	112,732	53,012	58,152	232,591
	Junk	58, 865	30,312	28,349	115,958
	Scan	57, 969	27,494	27,859	114,091
	TCP	193,677	95,021	92,581	380,788
	UDP	209,807	104,791	105,782	415,369
Mirai	**ACK**	102,195	113,285	91,123	337,218
	Scan	107,685	43,192	103,621	283,481
	SYN	122,573	116,807	118,128	375,791
	UDP	237,665	151,481	217,034	623,819
	UDP-Plain	81,982	87,368	80,808	273,146
Total		**1,373,798**	**835,876**	**1,098,677**	**3,379,033**

2.2. *Preprocessing*

IoT memiliki format yang sangat kompleks karena terhubung ke jaringan yang berbeda. Oleh karena itu, diperlukan pendekatan pra-pemrosesan untuk menangani fitur-fitur dataset. Untuk fitur kategorikal, kami menggunakan fungsi *hot coding* untuk mengubah fitur ini menjadi bentuk numerik. Hot coding mengonversi fitur-fitur kategorikal menjadi representasi numerik, memungkinkan algoritma machine learning untuk bekerja lebih efektif. Dengan representasi numerik, model dapat dengan lebih mudah mengenali pola dan hubungan dalam data. Normalisasi standar digunakan untuk menskalakan data ke format yang sama, sehingga memudahkan algoritma klasifikasi untuk memperoleh akurasi yang tinggi. Hal ini dilakukan dengan mengurangkan data dari mean dan membaginya dengan standar deviasi.

2.3. Pemodelan dengan Algoritma CNN

CNN memiliki lima lapisan: lapisan masukan untuk menangani data pelatihan serangan, lapisan konvolusional yang menggunakan filter data pelatihan, lapisan pengumpulan, lapisan terhubung penuh, dan lapisan keluaran. Ada berbagai macam kombinasi lapisan CNN yang dapat dipilih.

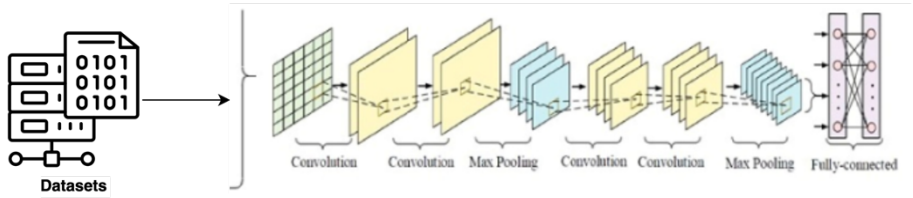
$$x_i = f\ (w_i \otimes x_{i-1} + b_i,) \tag{1}$$

Dimana x_i adalah data jaringan IoT yang diterima dari filter konvolusi l, i adalah kernel konvolusi lapisan CNN, dan $\otimes$ adalah operasi konvolusi. Untuk mentransfer keluaran dari

lapisan CNN hingga memperoleh keluaran akhir, digunakan fungsi aktivasi $f(x)$. Tujuan utama konvolusi adalah mengekstrak fitur-fitur penting dari data yang diterimanya. Kernel konvolusi dapat terdiri dari beberapa lapisan yang digunakan untuk memfilter data masukan, yang masing-masing memiliki bobot dan koefisien deviasi yang berbeda. Nilai parameter tertimbang menunjukkan w_i, dan b_i adalah nilai bias. Berikut ekspresi proses konvolusi:

$$f(x) = \tanh(x) = {}^{2} - 1, (3)1 + e^{-2x} \quad (2)$$

dimana $tanh$ adalah fungsinya dan x adalah data masukan pelatihan. Xi merupakan keluaran yang diperoleh dari filter CNN I yang melambangkan proses konvolusi, dan fungsi aktivasi dilambangkan dengan f(x). Unit yang relatif besar (ReLU) dipilih untuk fungsi aktivasi lapisan konvolusional. Pada saat implementasi model, kami menggunakan semua fungsi aktivasi, antara lain sigmoid dan tanh. Kami menemukan bahwa fungsi aktivasi ReLU sesuai untuk memproses data kami, karena fungsi ini menunjukkan pelatihan model yang lebih cepat dan pencegahan hilangnya gradien yang lebih efisien selama proses pelatihan. Struktur pemodelan algoritma CNN yang digunakan dalam penelitian ini diilustrasikan pada Gambar 2.



Gambar 2. Struktur *Convolutional Neural Networks (CNN)*

Tujuan utama dari lapisan pengumpulan maksimal adalah untuk mencapai invarian dan meminimalkan kompleksitas lapisan konvolusi CNN dengan menghilangkan informasi yang berlebihan melalui pengambilan sampel ke bawah dan mengurangi jumlah lapisan. Untuk menyelesaikan pengumpulan, ada dua metode dasar: pengumpulan rata-rata dan pengumpulan maksimum. Penggabungan rata-rata, metode yang paling umum, melibatkan pemilihan nilai rata-rata dalam area komputasi sebagai hasil penggabungan area, sedangkan pengumpulan maksimal melibatkan pemilihan nilai maksimum dalam area komputasi sebagai hasil pengumpulan area. Karena pengumpulan maksimum dapat menyimpan lebih banyak informasi penting daripada pengumpulan rata-rata, metode pengumpulan maksimum dibangun pada model CNN. Pengumpulan maksimum dapat didefinisikan sebagai berikut:

$$Q_j = Max\left(P_j^0, P_j^1, P_j^2, P_j^3, \ldots P_j^t\right) \quad (3)$$

dimana Qj adalah output dari kumpulan data keamanan siber IoT, j adalah area pengumpulan, Max adalah operasi, dan Pjt adalah elemen dari elemen t dari wilayah pengumpulan. Lapisan FC berfungsi sebagai "pengklasifikasi" di seluruh CNN. Lapisan FC digunakan untuk memetakan nilai fitur dari lapisan filter dan kumpulan maksimal ke dalam satu lapisan. Ketika overfitting terjadi pada lapisan FC, metode dropout digunakan untuk menghilangkan neuron secara acak untuk mencegah terjadinya overfitting.

2.3. Evaluasi

Model deep learning yang telah dibangun dievaluasi menggunakan laporan klasifikasi. Laporan klasifikasi adalah evaluasi kinerja dalam pembelajaran mesin yang menunjukkan presisi, perolehan, Skor F1, dan dukungan model klasifikasi. Ada beberapa kategori kasus yang mungkin terjadi:

- True Positive (TP): kasus dimana diprediksi menurut kelas (Positif) dan cocok dengan kelas (Benar).
- True Negative (TN): kasus dimana diprediksi tidak sesuai (Negatif) untuk kelasnya dan tidak cocok (Benar) kelasnya.
- False Positive (FP): kasus dimana diprediksi cocok dengan kelas (Positif), dan ternyata keluar menjadi kelas yang tidak pantas (Salah).
- False Negative (FN): kasus dimana diprediksi tidak sesuai (Negatif) untuk kelasnya, dan ternyata benar (True) untuk kelasnya.

Presisi (P) adalah rasio prediksi yang benar terhadap hasil prediksi positif secara keseluruhan. Presisi menjelaskan, "Berapa persentase menurut golongannya dari total prediksi menurut golongannya. Akurasi (A) adalah perbandingan ketepatan prediksi dengan data sebenarnya. Misalnya, akurasi menjelaskan berapa persentase serangan yang diprediksi menurutnya kelasnya dari total data. Akurasi menggunakan fungsi pada persamaan (4).

$$Accuracy = \frac{True\ Positive\ (TP) + True\ Negative\ (TN)}{TP+FP+FN+TN} \quad (4)$$

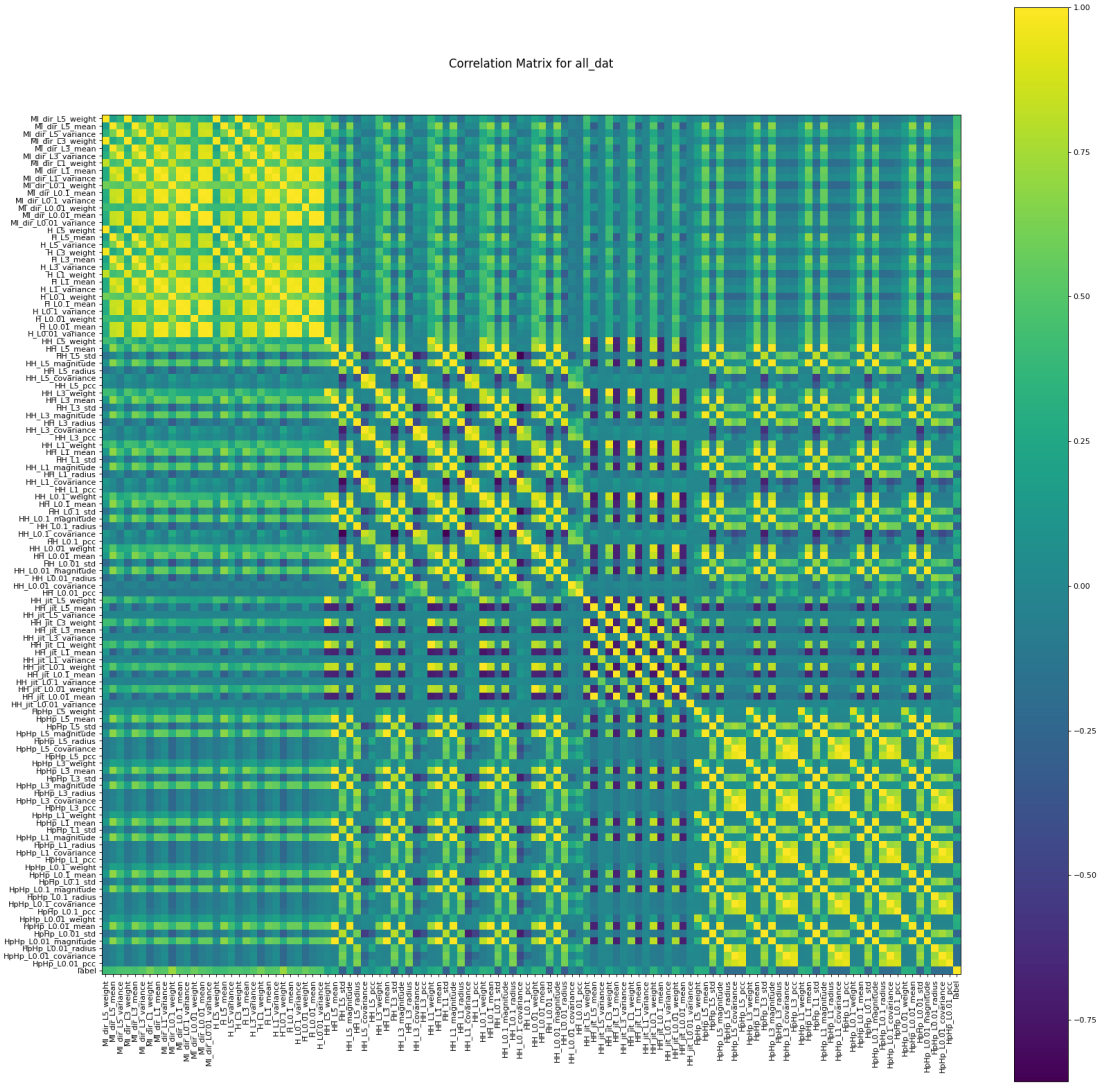
3. HASIL DAN PEMBAHASAN

Percobaan untuk menghasilkan dan mengembangkan sistem keamanan, diperlukan lingkungan yang kuat. Platform yang digunakan untuk menjalankan sistem yang diusulkan pada penelitian ini ditampilkan pada Tabel 4.

Tabel 4. Prakondisi dan persyaratan lingkungan sistem

Kebutuhan Perangkat Keras	Kebutuhan Perangkat Lunak
RAM 16 GB	Python 3.8
CPU AMD Ryzen 9	Numpy Version 1.19.3
	TensorFlow Version 2.12
	Keras Library 3.8

Pada lingkungan percobaan ini, digunakan sebuah laptop dengan sistem operasi Windows 11 64-bit sebagai platform utama, RAM 16 GB dengan dukungan prosesor AMD Ryzen 9 berjalan maksimal menggunakan GPU dari Google Collaboratory. Google Collaboratory juga memberikan keuntungan aksesibilitas dan kolaborasi. Dengan menjalankan eksperimen di platform ini, peneliti dapat bekerja secara bersamaan dan berbagi hasil secara real-time, memfasilitasi kolaborasi dan iterasi cepat dalam pengembangan proyek. Dalam penelitian ini, setiap kumpulan data berisi gabungan lalu lintas normal dan berbahaya dengan jumlah sampel berbeda seperti yang ditunjukkan pada dataset. Gambar 3 menunjukan korelasi matrix untuk semua data yang terdapat dalam dataset. Data suatu matriks korelasi tersebut memberikan informasi tentang sejauh mana variabel-variabel dalam dataset ini saling berkaitan. Matriks korelasi biasanya digunakan untuk mengevaluasi hubungan antara setiap pasangan variabel dalam dataset, dengan nilai korelasi berkisar antara -1 hingga 1.



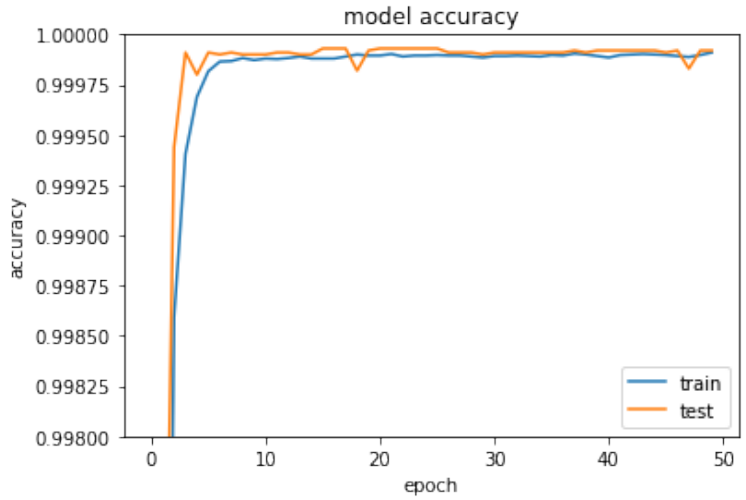
Gambar 3. *Correlation Matrix* dengan Model *CNN*

Dalam penelitian ini, peneliti menggunakan dataset yang diunduh untuk tujuan penelitian kemudian diolah dan disimpan dalam format .Pcap, yang merupakan format file yang umumnya digunakan untuk menyimpan data lalu lintas jaringan. Setelah proses pengolahan, dataset ini diekspor ke format .CSV yang merupakan format tabel yang lebih umum dan mudah diakses. Implementasi model CNN dan semua pengklasifikasi lainnya dimasukkan oleh file csv yang telah diekspor. Model CNN membagi sampel masukan ke data latih (*train*) dan data uji (*test*) menggunakan pengoptimal Adadelta, data uji = 0,2 dari data terlatih.

Fungsi *Rectified Linear Unit (Relu)* digunakan sebagai fungsi aktivasi untuk lapisan konvolusional dan lapisan terhubung penuh (*fully connected*), sedangkan softmax digunakan untuk lapisan keluaran. Setelah melatih model selama 50 epoch dengan dataset pertama. Hasil evaluasi model menunjukkan bahwa akurasi model adalah 99% dan hasil akurasi dan loss data dengan model *Convolutional Neural Network (CNN)* ditunjukkan pada gambar 4, dan gambar 5. Akurasi ini mencerminkan sejauh mana model dapat memprediksi dengan benar pada data yang belum pernah dilihat selama proses pelatihan.

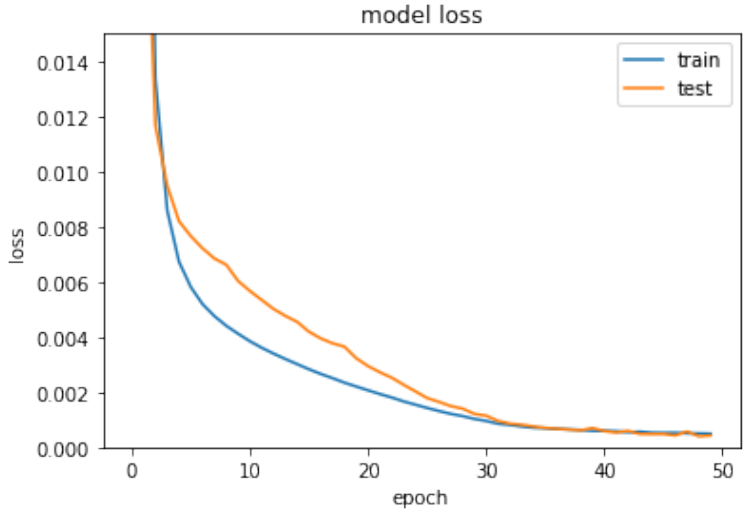
Pada Gambar 4, grafik atau plot menggambarkan bagaimana akurasi model berevolusi seiring berjalannya epoch selama pelatihan. Akurasi meningkat secara stabil atau mencapai

tingkat yang tinggi, ini menunjukkan bahwa model secara efektif mempelajari pola dan fitur pada dataset pelatihan. Grafik ini memberikan wawasan tentang sejauh mana model mampu mengadaptasi diri terhadap data yang kompleks dengan akurasi tinggi sebesar 99%.



Gambar 4. Akurasi dengan Model *CNN*

Di sisi lain, Gambar 5 menampilkan informasi tentang loss data selama pelatihan. Loss data menggambarkan seberapa baik atau buruk model dapat membuat prediksi. Jika grafik loss menunjukkan penurunan yang stabil, ini diartikan bahwa model secara progresif meningkatkan kemampuannya untuk melakukan prediksi yang akurat. Dengan memonitor loss data, peneliti dapat mengidentifikasi titik di mana model mencapai tanda-tanda overfitting atau underfitting.



Gambar 5. *Loss* dengan Model *CNN*

4. KESIMPULAN

Identifikasi dan klasfikasi serangan siber dengan kasus serang DDoS dianggap sebagai salah satu ancaman paling serius dan tersebar luas yang dihadapi oleh mereka yang bertanggung

jawab mengamankan jaringan. Berdasarkan hasil pengujian, telah berhasil mengklasifikasikan serangan DDOS dari semua jenis serangan yaitu SYN, ACK, UDP, dan UDPplain dengan pendekatan Artificial Intelligence (AI). Dalam penelitian ini, penerapan model deep learning dengan algoritma Convolutional Neural Network (CNN) digunakan dan diperkenalkan untuk mengklasifikasikan lalu lintas normal dari serangan siber DDoS. Berdasarkan analisis dan hasil, kami menemukan bahwa CNN berkinerja sangat baik proses pengklasifikasi dengan akurasi 99%. Untuk pekerjaan selanjutnya, kami berencana membangun model baru untuk memblokir atau memitigasi serangan DDoS berdasarkan keluaran dari algoritma klasifikasi CNN yang digunakan dalam penelitian ini.

UCAPAN TERIMA KASIH

Terimakasih kepada Lembaga Penelitian dan Pengabdian Masyarakat (LPPM), Universitas Siliwangi yang telah mendukung penelitian ini sesuai dengan daftar penerima hibah internal no surat keputusan rektor 1656/UN58/PP/2023.

DAFTAR RUJUKAN

Alam, T. M., & Awan, M. J. (2018). Domain Analysis of Information Extraction Techniques. *INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING*, *9*(6). www.ijmse.org

Al-Masri, E., Kalyanam, K. R., Batts, J., Kim, J., Singh, S., Vo, T., & Yan, C. (2020). Investigating Messaging Protocols for the Internet of Things (IoT). *IEEE Access*, *8*, 94880–94911. https://doi.org/10.1109/ACCESS.2020.2993363

Belli, L., Cilfone, A., Davoli, L., Ferrari, G., Adorni, P., Di Nocera, F., Dall'Olio, A., Pellegrini, C., Mordacci, M., & Bertolotti, E. (2020). IoT-Enabled Smart Sustainable Cities: Challenges and Approaches. *Smart Cities*, *3*(3), 1039–1071. https://doi.org/10.3390/smartcities3030052

Goyal, P., Sahoo, A. K., & Sharma, T. K. (2021). Internet of things: Architecture and enabling technologies. *Materials Today: Proceedings*, *34*, 719–735. https://doi.org/10.1016/j.matpr.2020.04.678

Gupta, M., Jain, R., Arora, S., Gupta, A., Javed Awan, M., Chaudhary, G., & Nobanee, H. (2021). AI-enabled COVID-9 Outbreak Analysis and Prediction: Indian States vs. Union Territories. *Computers, Materials & Continua*, *67*(1), 933–950. https://doi.org/10.32604/cmc.2021.014221

Nishanth, N., & Mujeeb, A. (2021). Modeling and Detection of Flooding-Based Denial-of-Service Attack in Wireless *Ad Hoc* Network Using Bayesian Inference. *IEEE Systems Journal*, *15*(1), 17–26. https://doi.org/10.1109/JSYST.2020.2984797

Privalov, A., Lukicheva, V., Kotenko, I., & Saenko, I. (2019). Method of Early Detection of Cyber-Attacks on Telecommunication Networks Based on Traffic Analysis by Extreme Filtering. *Energies*, *12*(24), 4768. https://doi.org/10.3390/en12244768

Sanmorino, A. (2019). A study for DDOS attack classification method. *Journal of Physics: Conference Series*, *1175*, 012025. https://doi.org/10.1088/1742-6596/1175/1/012025

Sestrem Ochôa, I., Reis Quietinho Leithardt, V., Calbusch, L., De Paz Santana, J. F., Delcio Parreira, W., Oriel Seman, L., & Albenes Zeferino, C. (2021). Performance and Security Evaluation on a Blockchain Architecture for License Plate Recognition Systems. *Applied Sciences*, *11*(3), 1255. https://doi.org/10.3390/app11031255

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, *2017*, 1–25. https://doi.org/10.1155/2017/9324035

Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash, C. (2017). Internet of Things (IoT): A vision, architectural elements, and security issues. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 492–496. https://doi.org/10.1109/I-SMAC.2017.8058399