IMEIJ
*Indo-MathEdu Intellectuals Journal*

p-ISSN: 2808 – 5604
e-ISSN: 2808 – 5078
**Volume. 6, No. 6, 2025**

# DETEKSI SERANGAN DDOS MENGGUNAKAN DEEP LEARNING DALAM ADMINISTRASI JARINGAN

Zulkipli Zulkipli[1], Aprila Kusuma Riskila[2], Eko Saputra[3],
Muh Syaikhurrahman[4], Bimo Prasetyo[5]
[1, 2, 3, 4, 5]Universitas Bumigora, Jl. Ismail Marzuki No.22, Cilinaya, Mataram, Nusa Tenggara Barat, Indonesia
Email: zulkipli@universtasbumigora.ac.id

***Article History***

Received: 19-08-2025

Revision: 31-08-2025

Accepted: 02-09-2025

Published: 04-09-2025

***Abstract.*** The DDoS (Distributed Denial-of-Service) attack detection system aims to enhance network security across all aspects of internet technology utilization. One of its applications is in SPKLU (Public Electric Vehicle Charging Stations). This research aims to detect DDoS attacks using deep learning in network administration. The study employs a deep learning approach utilizing Convolutional Neural Network (CNN) on a public dataset. Based on our study and analysis results, CNN has a precision rate of 95%. The high accuracy and balanced performance against various types of attacks indicate the potential application of this model in real-world situations. This model shows promising performance in detecting various network traffic anomalies, providing important insights related to its potential practical use. Further research is still needed to enhance resilience against evolving DDoS attack tactics and to address potential limitations that may exist.

**Keywords:** Convolutional Neural Network, DDoS attacks, Deep Learning

***Abstrak.*** Sistem deteksi serangan *DDoS (Distributed Denial-of-Service)* bertujuan untuk meningkatkan keamanan jaringan di seluruh aspek pemanfaatan teknologi internet. Salah satunya adalah pada SPKLU (Stasiun Pengisian Kendaraan Listrik Umum). Penelitian ini bertujuan untuk mendeteksi serangan DDOS menggunakan *deep learning* dalam administrasi jaringan. Penelitian ini menggunakan pendekatan deep learning dengan memanfaatkan *Convolutional Neural Network (CNN)* pada sebuah dataset publik. Berdasarkan hasil studi dan analisis kami, CNN memiliki tingkat presisi sebesar 95%. Akurasi yang tinggi dan kinerja yang seimbang terhadap berbagai jenis serangan menunjukkan potensi penerapan model ini dalam situasi nyata. Model ini menunjukkan performa yang menjanjikan dalam mendeteksi berbagai anomali lalu lintas jaringan, memberikan wawasan penting terkait potensi penggunaannya secara praktis. Penelitian lanjutan tetap diperlukan untuk memperkuat ketahanan terhadap taktik serangan DDoS yang terus berkembang dan untuk mengatasi berbagai keterbatasan yang mungkin ada.

**Kata Kunci:** Convolutional Neural Network, DDoS attacks, Deep Learning

***How to Cite***: Zulkipli, Z., Riskila, A. K., Saputra, E., Syaikhurrahman, M., & Prasetyo, B. (2025). Deteksi Serangan DDoS Menggunakan *Deep Learning* dalam Administrasi Jaringan. *Indo-MathEdu Intellectuals Journal,* 6 (6), 8995-9003. http://doi.org/10.54373/imeij.v6i6.4112

## PENDAHULUAN

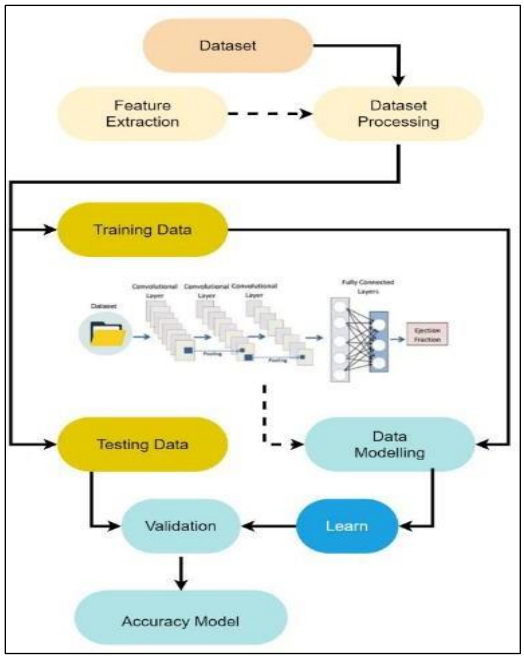
Keamanan jaringan merupakan komponen penting dalam bidang teknologi informasi karena memberikan strategi preventif untuk melindungi infrastruktur fisik dan perangkat lunak dari serangan. Dengan masifnya penggunaan Jaringan komputer sampai skala global

(internet), mengakibatkan jumlah data yang dihasilkan oleh jaringan terus meningkat. Termasuk juga peningkatan penggunaan komponen (Suartana, 2022). Keamanan siber bertanggung jawab untuk melindungi sistem komputer dan jaringan dari penyusupan tanpa izin, pencurian, kerusakan, dan gangguan layanan. Dalam lanskap di mana ancaman siber menjadi semakin kompleks dan canggih, perlindungan aset digital menjadi sangat penting. Serangan siber dapat menimbulkan konsekuensi ekonomi yang signifikan, kerusakan reputasi, dan bahkan hilangnya informasi rahasia. Serangan-serangan ini dapat menargetkan individu, organisasi, atau pemerintah, dan dampaknya bisa sangat luas (Becerra-Suarez et al., 2024).

*Deep learning* belakangan ini menjadi terkenal karena potensinya untuk pembelajaran mesin. *Deep learning* dapat dijadikan bagian integral dari keamanan jaringan karena memastikan evaluasi yang menyeluruh dan meyakinkan dari sistem keamanan jaringan. *Deep learning* dapat didefinisikan sebagai penggunaan jaringan syaraf tiruan secara mendalam yang dihubungkan menggunakan beberapa lapisan untuk menghasilkan output (Hernandez et al., 2025). Hasil dari fase sebelumnya dijadikan sebagai input agar dapat menghasilkan suatu luaran. Algoritma *Deep Learning (DL)* telah membentuk peran kunci dalam memecahkan masalah yang rumit, berkat berbagai keunggulannya dibandingkan dengan teknik *Machine Learning (ML)* tradisional lainnya. DL didefinisikan sebagai beberapa algoritma ML multi-lapis yang kuat dalam mempelajari abstraksi tingkat tinggi dari data skala besar yang kompleks. Algoritma DL biasanya mempelajari representasi fitur menggunakan banyak lapisan tersembunyi non-linear yang membuat rekayasa fitur otomatis (Suartana, 2022). Penelitian ini bertujuan untuk mendeteksi serangan DDOS menggunakan *deep learning* dalam administrasi jaringan.

## METODE

Artikel ini menyajikan sebuah metode untuk mendeteksi serangan DDoS dengan menggunakan *Convolutional Neural Network (CNN)* berbasis *deep learning*. Model yang diusulkan bertujuan untuk mengoptimalkan proses deteksi. Proses lengkapnya digambarkan pada Gambar 1 (Widodo et al., 2024).




**Gambar 1.** *The block diagram of DDoS attacks detection with deep learning approach*

***Dataset***

Dataset CICEV2023, yang dikenal sebagai DDoS Attack Dataset, merupakan sumber daya komprehensif dan andal yang secara khusus dibuat untuk mendukung penelitian keamanan siber pada infrastruktur pengisian daya kendaraan listrik (EV). Dataset ini terdiri dari banyak titik data, yang menunjukkan sejumlah besar log aktivitas jaringan. Abstrak tidak memberikan jumlah pasti titik data, namun dataset semacam ini umumnya berisi jutaan entri untuk memastikan gambaran menyeluruh lalu lintas jaringan, baik dalam skenario normal maupun saat serangan. Dataset ini memiliki 384.934 titik data, mencakup 33 kategori berbeda dari serangan DDoS pada sistem jaringan SPKLU. Dataset ini terdiri dari tiga kelas: *regular attack* (serangan normal), *gaussian assault* (serangan gaussian), dan *standard* (pengguna asli). Normal class mengacu pada antrean permintaan pada server yang dieksekusi oleh pengguna sah.Normal Attack class mengacu pada serangan DDoS tidak terencana yang sengaja dirancang agar mudah terlihat dalam log server atau sistem pemantauan.Gaussian Attack merupakan manuver ofensif yang dipersiapkan dengan baik dan menimbulkan tantangan signifikan dalam hal deteksi. Serangan ini menunjukkan penggunaan taktik yang lebih maju dan rumit oleh penyerang DDoS.Dalam dataset ini ditemukan adanya ketidakseimbangan pada kelas Gaussian Attack. Teknik *Synthetic Minority Over- Sampling Technique (SMOTE)* digunakan untuk melakukan *oversampling* dengan menambahkan sampel baru pada kelas minoritas agar distribusi kelas menjadi lebih seimbang. Teknik ini

memfasilitasi pengisian realistis pada kelas yang tidak seimbang tanpa mengubah kelas asli (Ramzan et al., 2023).

Dataset ini mencakup banyak klasifikasi, yang terutama dibagi menjadi tiga kelas: normal attack, gaussian assault, dan normal. Dataset ini berisi beragam fitur yang diperlukan untuk analisis menyeluruh dan pelatihan model. Karakteristik berikut termasuk di dalamnya:

- *Timestamp* (Penanda Waktu): Menangkap penanda waktu yang tepat dari setiap peristiwa jaringan, yang penting untuk memantau pola lalu lintas dan menentukan waktu terjadinya serangan.
- Alamat IP sumber (*source IP address*): digunakan untuk mengidentifikasi asal lalu lintas jaringan dan membantu dalam mengenali potensi sumber aktivitas berbahaya.
- Alamat IP tujuan (*destination IP address*): mengacu pada lokasi spesifik ke mana lalu lintas jaringan dikirim. Digunakan untuk mengidentifikasi elemen spesifik dari infrastruktur yang menjadi target serangan.
- Nomor port *(port numbers):* untuk mengidentifikasi titik akhir komunikasi dan layanan yang menjadi target serangan. Nomor port, baik sumber maupun tujuan, sangat penting.
- Protokol *(protocol):* menentukan protokol komunikasi yang digunakan (misalnya TCP, UDP), memberikan informasi mengenai karakteristik lalu lintas.
- Informasi *payload* (*payload information):* terdiri dari jumlah data dan jenis konten, yang sangat penting untuk membedakan antara lalu lintas jaringan normal dan abnormal.
- Metrik volume lalu lintas *(traffic volume metrics):* tingkat paket *(packet rate)* dan jumlah *byte* sangat penting untuk mengidentifikasi serangan berbasis volume (*volumetric attacks*).

Dataset CICEV2023 merupakan sumber daya yang sangat penting untuk melakukan penelitian di bidang keamanan siber. *Dataset* ini menyediakan kombinasi yang menyeluruh dan seimbang antara lalu lintas normal dan lalu lintas serangan, serta himpunan fitur yang luas. Dataset ini sangat esensial untuk mengembangkan metode deteksi dan mitigasi DDoS yang lebih canggih, yang krusial dalam melindungi integritas dan ketersediaan infrastruktur pengisian daya kendaraan listrik (EV) (Suartana, 2022)

### *Dataset Processing*

Dataset mengekstraksi parameter *timestamp* yang unik. *Timestamp* tersebut kemudian dikonversi ke epoch time. Perbedaan waktu digunakan sebagai tambahan fitur dengan cara mengamati selisih waktu antarbaris data. Untuk menentukan perbedaan waktu antara serangan DDoS dan aktivitas normal, perlu diketahui selisih waktu pada setiap baris. Fitur

yang dimaksud adalah perbedaan durasi antara baris pertama dengan baris-baris berikutnya, yang direpresentasikan sebagai $P_i$ (Hernandez, et al., 2025). Persamaan yang mengonversi *datetime* ke tipe data ditandai sebagai $T_i$. Waktu POSIX untuk $T_i$ adalah nilai waktu pada entri ke- $T_i$ dalam sebuah kolom dengan format *datetime POSIX time*, yang dirumuskan sebagai berikut:

$$P_i = POSIX\_Time\ (T_i) \tag{1}$$

$$\Delta T_i = P_i + 1 - P_i \tag{2}$$

$$\Delta T_i = \begin{cases} P_{i+1} - P_i & if\ i < n \\ 0 & if\ i = n \end{cases} \tag{3}$$

Perhitungan selisih waktu antarbaris diperoleh dengan mengurangkan waktu antarbaris, sebagaimana ditunjukkan pada Persamaan (3). n merepresentasikan jumlah total baris dalam kolom dengan tipe data *datetime*. Selanjutnya, dilakukan normalisasi data untuk memperoleh data yang konsisten dan memastikan bahwa setiap fitur memiliki bobot yang sama dalam model (Widodo et al., 2024).

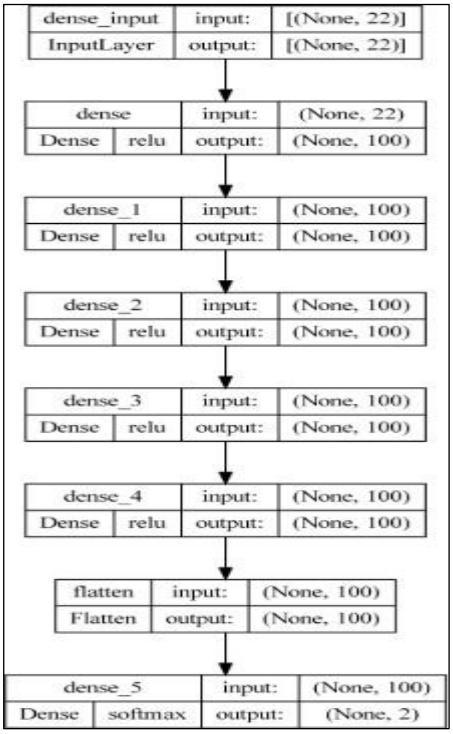
***Deep Learning and Convolutional Neural networks Deep***

*Deep learning* adalah sebuah metode yang memanfaatkan lapisan *artificial neural network*. Teknik ini diterapkan pada skenario dengan data yang melimpah dan kompleks, seperti dataset yang dihasilkan dari penelitian sebelumnya, karena *deep learning* mampu secara otomatis mengidentifikasi representasi atau fitur data. Penelitian-penelitian terdahulu telah mengimplementasikan teknik *deep learning* untuk mendeteksi serangan DDoS. *Deep learning* merupakan cabang dari *machine learning* yang menggunakan *artificial neural networks* untuk memperoleh pengetahuan dari data. Metode ini terinspirasi dari organisasi dan cara kerja otak manusia, serta unggul dalam menangani informasi yang kompleks, seperti gambar, sinyal, teks, dan suara

*Convolutional Neural Networks (CNNs)* sangat cocok untuk tugas yang melibatkan pemrosesan citra dan sinyal, sehingga sangat berguna dalam mengevaluasi pola pada lalu lintas jaringan. Arsitektur CNN terdiri dari lapisan konvolusi dan lapisan pooling, yang berfungsi mengekstraksi fitur dari data, serta lapisan terhubung penuh *(fully connected layers)* untuk klasifikasi. CNN mampu memperoleh pengetahuan yang diperlukan untuk mengidentifikasi pola tertentu dalam lalu lintas jaringan yang menjadi indikasi adanya serangan *Distributed Denial of Service (DDoS)*

## HASIL DAN DISKUSI

Model pelatihan dibangun menggunakan arsitektur model MLP dengan seluruh fitur (f = 22), sebagaimana ditunjukkan pada Gambar 3. Dataset yang digunakan untuk melatih pendekatan deteksi yang diusulkan dijelaskan pada Tabel 1. Seperti yang terlihat pada tabel, jumlah total sampel instance adalah 124.688. Dataset tersebut dibagi menjadi 80% untuk pelatihan dan 20% untuk pengujian untuk pengujian. Ini merupakan pendekatan yang sederhana dan teknik yang umum digunakan. Sebagai hasilnya, sebuah confusion matrix dihasilkan untuk merepresentasikan dan mengevaluasi kinerja dari pendekatan deteksi yang diusulkan. *Confusion matrix* biasanya digunakan untuk membandingkan label yang diprediksi dengan label sebenarnya [5]




**Gambar 2.** *DL-based MLP model architecture*

### *Comparison of Proposed Detection*

Selain hasil yang telah disebutkan sebelumnya, bagian ini memberikan evaluasi komprehensif terhadap pendekatan deteksi yang diusulkan dibandingkan dengan pendekatan DLADSC, yang memanfaatkan teknik berbasis RNN untuk mendeteksi serangan DDoS dalam lingkungan pengendali SDN. Kedua pendekatan tersebut bertujuan untuk mengatasi tantangan serupa; namun, perbedaan utama muncul ketika mengevaluasi kinerja mereka menggunakan beberapa metrik, termasuk:(i) *dataset SDN* itu sendiri, (ii) rata-rata akurasi, (iii) presisi, (iv)

*recall*, (v) *FPR (False Positive Rate)*, (vi) *F1-score*, dan (vii) waktu deteksi serangan DdoS (diukur menggunakan fungsi waktu Python mulai dari pemasukan data uji hingga menghasilkan keluaran prediksi akhir) (Ramzan et al., 2023)

***Limitations***

Akurasi yang lebih tinggi dan penurunan FPR menunjukkan bahwa pendekatan deteksi yang diusulkan mampu menangani kompleksitas arsitektur SDN, serta menawarkan deteksi yang andal dan efisien. Selain itu, kemampuan untuk mempertahankan presisi dan recall yang tinggi pada dataset SDN yang realistis menunjukkan skalabilitas dan penerapannya dalam skenario dunia nyata, sehingga menempatkannya sebagai pendekatan deteksi yang lebih tangguh dibandingkan dengan metode lainnya, khususnya pada jaringan berbasis SDN yang praktis. Hasil ini menyoroti kemampuan unggul dari pendekatan deteksi yang diusulkan dalam mengidentifikasi serangan DDoS dengan lebih akurat dan menghasilkan jumlah *False Positive (FP)* yang lebih sedikit, yang sangat penting untuk menjaga efisiensi manajemen jaringan. Meskipun kinerja meningkat, terdapat sedikit kompromi pada waktu deteksi, di mana pendekatan yang diusulkan memiliki waktu deteksi sedikit lebih lama yaitu 1,713 detik dibandingkan dengan 1,627 detik pada pendekatan DLADSC. Walaupun perbedaannya kecil, hal ini mungkin disebabkan oleh jumlah hidden layer yang lebih banyak, yang menambah kompleksitas dan kedalaman pada proses deteksi, sehingga menghasilkan deteksi yang lebih akurat (Bahashwan et al., 2025).

## KESIMPULAN

Dalam penelitian ini, diusulkan penggunaan model *Deep Learning (DL)* untuk mengklasifikasikan serangan DDoS pada jaringan, yang dinilai lebih efektif dibandingkan dengan model Machine Learning. Model LSTM dipilih sebagai model yang layak untuk penelitian ini karena mencakup baik pemilihan fitur maupun ekstraksi fitur dalam modelnya, sehingga lebih unggul dibandingkan metode machine learning dangkal (*shallow machine learning methods*). Dalam penelitian ini, model LSTM telah digunakan untuk klasifikasi antara lalu lintas normal (*benign*) dan lalu lintas berbahaya (*threats*) pada dataset CICDDoS2019. Model LSTM yang digunakan sebagai model *deep learning* mencapai akurasi sekitar 98,6% dalam klasifikasi serangan DDoS, yang jauh lebih tinggi dibandingkan dengan model KNN dan ANN. Selain itu, penggunaan dataset CICDDoS2019 dengan model LSTM untuk mendeteksi serangan DDoS memberikan arah baru bagi penelitian lain dalam deteksi intrusi DDoS. Karena tingkat akurasinya yang tinggi dalam mendeteksi serangan, penerapan model

LSTM ke dalam jaringan berbasis perangkat lunak tampak menjadi pilihan yang baik. Untuk penelitian di masa depan, disarankan dengan menangkap lalu lintas jaringan dan mengintegrasikan incremental learning, sehingga mesin dapat terus memperbarui dirinya terhadap jenis serangan baru.

## REFERENSI


Ahmed *et al.*, "Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron," *Futur. Internet*, vol. 15, no. 2, pp. 1–24, 2023, doi: 10.3390/fi15020076.

Alashjaee, "Deep learning for network security: an Attention-CNN-LSTM model for accurate intrusion detection," *Sci. Rep.*, vol. 15, no. 1, pp. 1–12, 2025, doi: 10.1038/s41598-025-07706-y.

Apostu *et al.*, "Detecting and Mitigating DDoS Attacks with AI: A Survey," 2025, [Online]. Available: http://arxiv.org/abs/2503.17867

Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, and I. H. Hasbullah, "A deep learning approach to detect DDoS flooding attacks on SDN controller," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 38, no. 2, p. 1245, 2025, doi: 10.11591/ijeecs.v38.i2.pp1245-1255.

Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, M. A. Aladaileh, and I. H. Hasbullah, "A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking," *Sensors*, vol. 23, no. 9, 2023, doi: 10.3390/s23094441.

Becerra-Suarez, I. Fernández-Roman, and M. G. Forero, "Improvement of Distributed Denial of Service Attack Detection through Machine Learning and Data Processing," *Mathematics*, vol. 12, no. 9, 2024, doi: 10.3390/math12091294

Hernandez, Y. K. Lai, and H. T. N. Ignatius, "Real-Time DDoS Detection in High-Speed Networks: A Deep Learning Approach with Multivariate Time Series," *Electron.*, vol. 14, no. 13, pp. 1–37, 2025, doi: 10.3390/electronics14132673.

Hekmati, J. Zhang, T. Sarkar, N. Jethwa, E. Grippo, and B. Krishnamachari, "Correlation-Aware Neural Networks for DDoS Attack Detection in IoT Systems," *IEEE/ACM Trans. Netw.*, vol. 32, no. 5, pp. 3929–3944, 2024, doi: 10.1109/TNET.2024.3408675.

Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DdoS Detection using Deep Learning," *Procedia Comput. Sci.*, vol. 218, pp. 2420–2429, 2022, doi: 10.1016/j.procs.2023.01.217.

Made Suartana, "Analisis Penerapan Deep Learning untuk Klasifikasi Serangan Terhadap Keamanan Jaringan," *Klik-Kumpulan J. Ilmu Komput.*, vol. 9, no. 1, pp. 100–109, 2022.

Ramzan *et al.*, "Distributed Denial of Service Attack Detection in Network Traffic Using Deep Learning Algorithm," *Sensors (Basel).*, vol. 23, no. 20, pp. 1–24, 2023, doi: 10.3390/s23208642.

Ramanathan, K. Mahadevan, and S. Dua, "A Novel Supervised Deep Learning Solution to Detect Distributed Denial of Service (DDoS) attacks on Edge Systems using Convolutional Neural Networks (CNN)," 2023, [Online]. Available: http://arxiv.org/abs/2309.05646

Setiawan and C.-W. Lin, "A Deep Learning Framework for Automatic Sleep Apnea Classification Based on Empirical Mode Decomposition Derived from Single-Lead Electrocardiogram," Life, vol. 12, no. 10, p. 1509, Sep. 2022, doi: 10.3390/life12101509.

Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via Convolutional Neural Network (CNN)," in 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS), Cairo, Egypt: IEEE, Dec. 2019, pp. 233–238. doi: 10.1109/ICICIS46948.2019.9014826

Simarmata, N. F. Saragih, I. K. Jaya, and H. Artikel, "Deteksi Serangan DDOS Pada VPS Menggunakan Metode Deep Neural Network," *METHOTIKA J. Ilm. Tek. Inform.*, vol. 3, no. 1, pp. 1–12, 2023, [Online]. Available: https://ejurnal.methodist.ac.id/index.php/methotika/article/view/2107

Widodo, M. K. Delimayanti, and A. Wulandari, "DDoS Attacks Detection With Deep Learning Approach Using Convolutional Neural Network," *J. Appl. Informatics Comput.*, vol. 8, no. 2, pp. 235–240, 2024, doi: 10.30871/jaic.v8i2.8242.