MASE Media Applied Science and Engineering

Media Journal of General Computer Science, 2025, Vol 2, Issue 1,18-27
Published Online January 2025 in MASE (http://www.mase.or.id)
DOI: 10.62205/mjgcs.v2i1.90

Enhancing IoT Security: Detecting DoS and SPOOFING Attacks with DNN-based IDS using CICIoT 2024

Budi Setiawan
Department of Computer Engineering, Dinamika Bangsa University, Jambi, Indonesia
E-mail: budisetiawan.tebo@gmail.com

Raka Jumersyah Pratama
Department of Computer Engineering, Dinamika Bangsa University, Jambi, Indonesia
E-mail: rakajumersyahpratama74222@gmail.com

Hengkky Restu Putra
Department of Computer Engineering, Dinamika Bangsa University, Jambi, Indonesia
E-mail: henkkyx16@gmail.com
*Correspondent Author

FA Bambang Sukoco
Department of Information System, Dinamika Bangsa University, Jambi, Indonesia
E-mail: bengsgkt@gmail.com

Received: 14 January, 2025; Accepted: 25 January, 2025; Published: 30 January, 2025

Abstract: With the rapid expansion of IoT (Internet of Things) devices, ensuring network security has become a critical challenge. Distributed Denial of Service (DoS) and spoofing attacks are among the most common and damaging threats in IoT ecosystems. Traditional Intrusion Detection Systems (IDS) often face difficulties in detecting these attacks due to the high volume and complexity of IoT network traffic. This study introduces a novel Deep Neural Network (DNN)-based IDS designed to effectively detect DoS and spoofing attacks using the CICIoT 2024 dataset. The CICIoT 2024 dataset provides a comprehensive benchmark with realistic IoT network traffic patterns, including benign and malicious activities. The results highlight the potential of DDN-based IDS to enhance IoT network security, paving the way for more resilient and intelligent defense mechanisms against evolving cyber threats. The detection results are promising, significantly improving attack detection performance, reaching up to 100%.

Keywords: IoT, IDS, DoS, Spoofing, DDN, Deep Learning, CICIoV2024, Dataset

I. Introduction

Keamanan pada Internet of Things (IoT) telah menjadi perhatian utama seiring dengan meningkatnya adopsi perangkat IoT dalam berbagai sektor. Berbagai penelitian telah dilakukan untuk meningkatkan keamanan IoT dengan memanfaatkan teknik machine learning. Sebagai contoh, sebuah studi terbaru memperkenalkan model baru untuk meningkatkan keamanan sistem IoT menggunakan classifier machine learning [1]. Selain itu, penelitian lain menganalisis dan mengevaluasi model machine learning dan deep learning untuk mendeteksi aktivitas berbahaya dalam jaringan IoT [2]. Lebih lanjut, sebuah survei komprehensif membahas solusi berbasis machine learning untuk keamanan IoT, menyoroti tantangan dan arah penelitian di masa depan [3].

Beberapa Tahun terakhir, *Internet of Things* (IoT) menjadi popular dalam melayani masyarakat dengan berbagai cara [4] [5], IoT telah merevolusi cara manusia berinteraksi dengan lingkungan sekitar dan memiliki potensi untuk memberikan dampak yang signifikan di berbagai sektor. [6] [7] IoT merupakan sebuah revolusi teknologi yang menggambarkan masa depan dalam bidang komputasi dan komunikasi. Perkembangannya sangat bergantung pada inovasi teknis yang terus-menerus di berbagai bidang penting, mulai dari sensor tanpa kabel hingga nanoteknologi. Setiap objek akan diberi label untuk tujuan identifikasi, otomatisasi, pemantauan, dan pengendalian. [8] Pada penelitian ini akan berfokus pada penerapan *intrusion detection systems* (IDS) berbasis *Deep Neural Network* (DNN) untuk mendeteksi *Denial of Service* (DoS) dan SPOOFING attack.

Masalah yang ada pada keamanan perangkat IoT adalah meningkatnya serangan dunia maya yang memanfaatkan

celah keamanan pada perangkat yang saling terhubung. Perangkat IoT yang semakin banyak digunakan dalam berbagai sektor seperti layanan kesehatan, perbankan, energi, dan pemerintahan, menjadi target serangan yang berpotensi merugikan infrastruktur penting. [9] Berbagai penelitian telah dilakukan untuk meningkatkan keamanan perangkat IoT dengan memanfaatkan algoritma deep learning dan teknologi big data.

Penelitian sebelumnya [10] telah menunjukkan bahwa algoritma *Deep Neural Network* (DNN) memberikan hasil yang lebih baik dibandingkan metode pembelajaran mesin tradisional dalam mendeteksi ancaman pada jaringan. Salah satu pendekatan yang diusulkan adalah dengan menggunakan DNN yang didistribusikan di platform big data seperti Apache Spark, yang memungkinkan pemrosesan data dalam skala besar dengan waktu yang lebih efisien. Model DNN seperti *Multi-Layer Perceptron* (MLP) dan *Feed Forward Neural Network* (FFNN) telah diuji dalam berbagai skenario deteksi intrusi, termasuk pada sistem IoT, dan menunjukkan kinerja yang unggul dalam mendeteksi serangan siber. Namun, tantangan utama yang dihadapi dalam penerapan DNN adalah waktu prediksi yang relatif tinggi dan kebutuhan akan sumber daya komputasi yang besar. Oleh karena itu, penelitian ini mengusulkan kerangka kerja yang menggabungkan DNN dengan teknologi big data untuk meningkatkan efisiensi deteksi intrusi pada perangkat IoT. Dengan memanfaatkan kemampuan DNN untuk mempelajari pola data yang kompleks dan kemampuan big data dalam memproses volume data yang besar, sistem yang diusulkan diharapkan dapat meningkatkan akurasi deteksi dan mengurangi risiko serangan pada jaringan IoT.

DNN merupakan jenis jaringan saraf tiruan yang terdiri dari beberapa lapisan tersembunyi antara lapisan input dan output. Setiap lapisan terdiri dari neuron yang melakukan komputasi pada data input, memungkinkan DNN untuk mempelajari pola dan representasi yang kompleks dari data. DNN telah diterapkan dalam berbagai tugas pembelajaran mesin, termasuk pengenalan gambar, pemrosesan bahasa alami, dan deteksi intrusi jaringan. [11] Sehingga memiliki potensi untuk digunakan sebagai metode deteksi serangan, DNN mampu menemukan manipulasi matematis yang tepat untuk mengubah input menjadi output. [12]

2. Research Method

2.1 Experiment Setup

Dalam penelitian ini, kami menggunakan dataset *CICIoT 2024* untuk melatih dan menguji model Deep Neural Network (DNN) yang dirancang untuk mendeteksi serangan DoS dan spoofing. Dataset ini dipilih karena kelengkapannya dalam mencakup berbagai jenis serangan yang umum terjadi pada lingkungan IoT. Proses pelatihan melibatkan beberapa tahap, termasuk pra-pemrosesan data, pemilihan fitur, dan penyesuaian hyperparameter untuk mengoptimalkan kinerja model. Pendekatan ini sejalan dengan metode yang digunakan dalam penelitian sebelumnya yang berhasil mengimplementasikan model machine learning untuk deteksi serangan pada jaringan IoT [13].

Penelitian ini bertujuan untuk mendeteksi serangan jaringan, khususnya serangan *DoS* dan *Spoofing***,** menggunakan *Deep Neural Network* (DNN) dengan dataset *CICIoT 2024*. Dataset ini terdiri dari 8 fitur utama, yaitu DATA_0 hingga DATA_7**,** dan tiga kategori target: Benign**,** *DoS*, dan *Spoofing*. Sejumlah tahap penelitian yang perlu dilakukan akan diuraikan secara lebih rinci dalam alur penelitian dalam Fig.1.

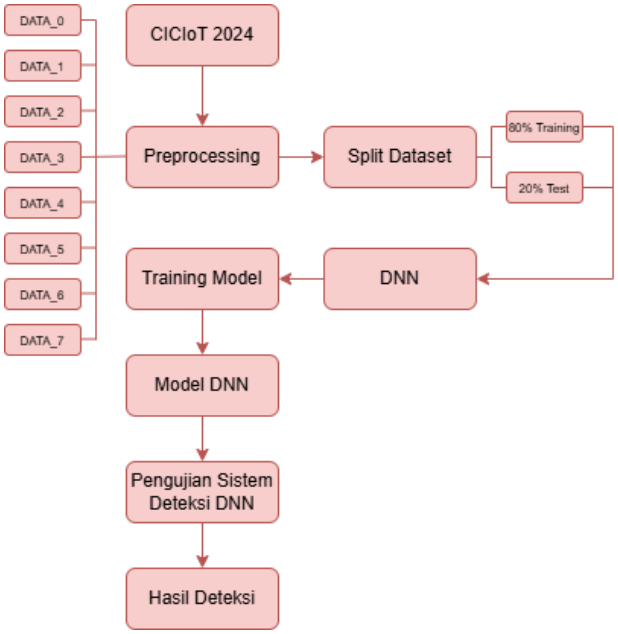


Fig.1. Experiment setup

Fig.1 adalah diagram eksperimen yang dirancang khusus untuk penelitian ini. Oleh karena itu, proses penelitian dibagi menjadi tuas tahap terpisah:

- Sebagai Langkah awal, dilakukan ekstraksi fitur dari kumpulan data menggunakan delapan fitur utama (DATA_0 hingga DATA_7) yang sudah tersedia dalam dataset *CICIoT 2024*. Selanjutnya, dilakukan normalisasi fitur numerik menggunakan metode StandardScaler untuk mendapatkan distribusi yang seragam. Label kategori (*category*) dikodekan menjadi bentuk numerik dan diubah menjadi one-hot encoding agar sesuai dengan kebutuhan klasifikasi multi-kelas. Dataset kemudian dibagi menjadi dua bagian: 80% data latih dan 20% data uji, untuk memastikan model dapat diuji secara adil pada data yang belum pernah dilihat sebelumnya.
- Pada tahap kedua, dilakukan pelatihan model menggunakan kumpulan data latih. Model *Deep Neural Network* (DNN) yang dibangun terdiri dari tiga lapisan utama: lapisan masukan dengan 8 neuron (mengacu pada jumlah fitur), dua lapisan tersembunyi dengan masing-masing 64 dan 32 neuron menggunakan fungsi aktivasi ReLU, serta lapisan keluaran dengan 3 neuron menggunakan fungsi aktivasi Softmax. Pelatihan dilakukan selama 10 epoch dengan batch size 32 menggunakan Adam optimizer dan fungsi kerugian categorical crossentropy. Model ini dilatuh untuk mengenali pola yang ada dalam dataset, sehingga mampu mendeteksi kategori serangan dengan baik.
- Pada Langkah terakhir, dilakukan pengujian menggunakan dataset uji pada model yang telah dilatih sebelumnya. Pengujian ini bertujuan untuk menghitung tingkat keberhasilan model, termasuk metrik utama seperti Accuracy, Precision, Recall, dan F1-Score. Selain itu, digunakan Confusion Matrix untuk menganalisis distribusi prediksi model pada setiap kelas (Benign, DoS, dan Spoofing). Hasil pengujian divisualisasikan dalam bentuk grafik batang, yang menunjukan performa model berdasarkan metrik-metrik tersebut.

2.2 Dataset

Penelitian ini akan memanfaatkan dataset *CICIoT 2024* sebagai sumber data. Dataset tersebut mengklasifikasikan serangan menjadi 2 kategori yang berbeda, yakni *DoS* dan *Spoofing*. Dataset yang digunakan dalam penelitian ini memiliki total 1.048.575 data yang terdiri dari beberapa kategori utama, yaitu Benign**,** DoS, dan berbagai jenis serangan Spoofing. Data kategori Benign mencakup 864.093 data, sementara kategori DoS memiliki 74.663 data. Untuk kategori Spoofing, dataset ini terbagi menjadi beberapa jenis serangan spesifik, yaitu GAS sebanyak 9.991 data, RPM sebanyak 54.900 data, SPEED sebanyak 24.951 data, dan STEERING_WHEEL sebanyak 19.977 data, yang tercatat dalam dataset ini dilakukan oleh perangkat IoT berbahaya yang memiliki tujuan menyerang perangkat IoT lainnya. [14]

2.3 Features and Description

Ekstraksi fitur dari Dataset *CICIoT 2024* mempermudah proses deteksi ancaman. Fitur pertama (ID) mengacu pada bidang arbitrasi. Selanjutnya, fitur data (yaitu, DATA_0 hingga DATA_7) merepresentasikan byte dari data yang ditransmisikan. Kemudian, label, category, dan specific_class digunakan untuk acuan dalam mendeteksi serangan cyber. Fig.2. Menunjukkan fitur-fitur yang tersedia pada dataset decimal.

#	Column	Non-Null Count	Dtype
0	ID	1048575 non-null	int64
1	DATA_0	1048575 non-null	int64
2	DATA_1	1048575 non-null	int64
3	DATA_2	1048575 non-null	int64
4	DATA_3	1048575 non-null	int64
5	DATA_4	1048575 non-null	int64
6	DATA_5	1048575 non-null	int64
7	DATA_6	1048575 non-null	int64
8	DATA_7	1048575 non-null	int64
9	label	1048575 non-null	object
10	category	1048575 non-null	object
11	specific_class	1048575 non-null	object

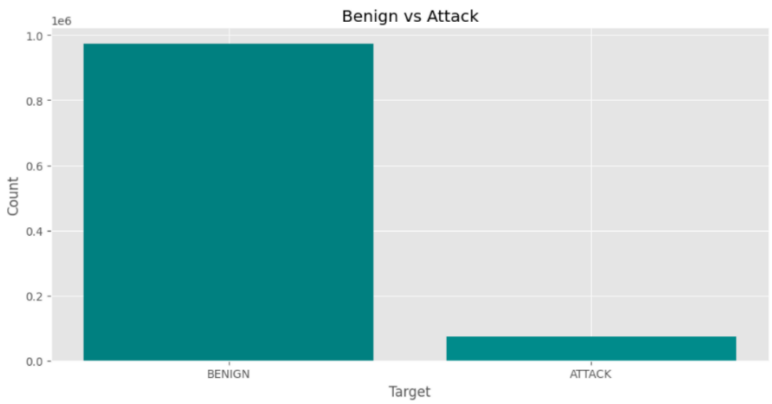
Fig.2. Fittur data

Pada penelitian ini menggunakan Dataset decimal, Fig.3 memberikan deskripsi statistic dataset *CICIoT 2024* untuk representasi decimal. Tabel ini mencantumkan nilai hitung (count), rata-rata (mean), deviasi standar (std), nilai minimun (min), persentil 25% (25%), persentil 50% (50%), persentil 75% (75%), dan nilai maksimum (max) untuk setiap fitur (DATA_0 hingga DATA_7).

	ID	DATA_0	DATA_1	DATA_2	DATA_3	DATA_4	DATA_5	DATA_6	DATA_7
count	1.048575e+06	1.048575e+06	1.048575e+06	1.048575e+06	1.048575e+06	1.048575e+06	1.048575e+06	1.048575e+06	1.048575e+06
mean	5.278453e+02	6.908744e+01	6.711774e+01	5.353152e+01	5.618947e+01	4.393630e+01	5.164533e+01	6.968507e+01	5.826741e+01
std	3.177823e+02	8.809091e+01	9.395721e+01	7.237711e+01	8.887989e+01	6.366508e+01	9.242341e+01	1.001666e+02	9.800205e+01
min	6.500000e+01	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00
25%	3.440000e+02	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00
50%	5.140000e+02	1.600000e+01	1.200000e+01	1.000000e+01	2.000000e+00	6.000000e+00	0.000000e+00	1.000000e+00	0.000000e+00
75%	5.780000e+02	1.270000e+02	1.280000e+02	1.250000e+02	8.000000e+01	8.600000e+01	6.300000e+01	1.380000e+02	8.000000e+01
max	1.438000e+03	2.550000e+02	2.550000e+02	2.550000e+02	2.550000e+02	2.550000e+02	2.550000e+02	2.550000e+02	2.550000e+02

Fig.3. Deskripsi statistic decimal

Setelah dekripsi statistic decimal di tampilkan, Fig.4 menampilkan analisis distribusi class data dengan visualisasi subplot berupa diagram perbandingan. Pada Diagram pertama membandingkan jumlah instance antara Benign dan Attack (DoS dan Spoofing), kemudian diagram kedua membandingkan jumlah instance antara serangan *Spoofing* dan *DoS*, dan yang terakhir membandingkan distribusi kelas spesifik dari kategori serangan *Spoofing* (RPM, SPEED, STEERING_WHEEL, GAS).



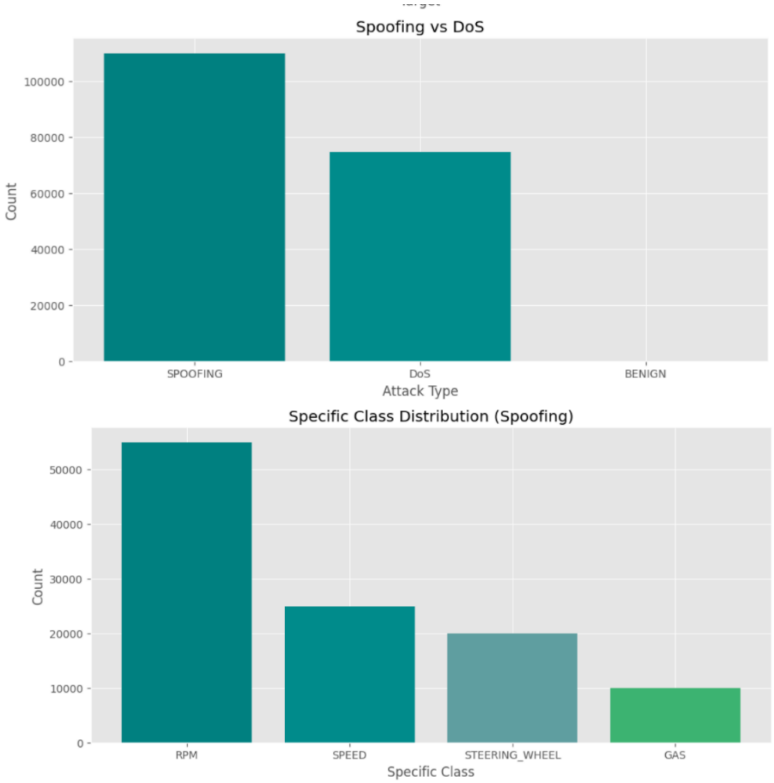


Fig.4. Analisis distribusi class

Selanjutnya, Fig.4 menunjukkan distribusi data berdasarkan kategori serangan dan aktivitas normal (Benign) yang terdapat dalam dataset CICIoT 2024. Kategori Benign memiliki jumlah data tertinggi dengan 864.093 instance, yang merepresentasikan lalu lintas jaringan normal. Sebaliknya, kategori serangan terbagi menjadi DoS (74.663 instance) dan berbagai jenis serangan Spoofing, seperti GAS (9.991 instance)**,** RPM (54.900 instance), SPEED (24.951 instance), dan STEERING_WHEEL (19.977 instance).

Distribusi ini dirancang untuk memberikan proporsi realistis terhadap skenario nyata pada lingkungan IoT, di mana lalu lintas normal umumnya mendominasi, tetapi tetap mengandung potensi serangan yang signifikan. Tujuan utama dari representasi ini adalah untuk memastikan bahwa model machine learning yang dikembangkan dapat mendeteksi serangan meskipun data serangan memiliki jumlah yang jauh lebih sedikit dibandingkan dengan data normal. Dengan demikian, gambar ini menjadi dasar dalam memahami tantangan utama yang dihadapi dalam mendeteksi serangan IoT, khususnya dalam hal ketidakseimbangan data.Terakhir, Fig.5 menggambarkan jumlah instance yang tersedia dalam dataset untuk setiap kelas.

Tabel Distribusi Kategori:

	category	specific_class	count
0	BENIGN	BENIGN	864093
1	DoS	DoS	74663
2	SPOOFING	GAS	9991
3	SPOOFING	RPM	54900
4	SPOOFING	SPEED	24951
5	SPOOFING	STEERING_WHEEL	19977

Fig.5. Distribusi kategori

2.3 Environment Setup

Eksperimen dalam penelitian ini dilaksanakan menggunakan sebuah laptop dengan spesifikasi berikut: menggunakan system operasi Windows 11 Pro 64-bit (versi 21H2, OS build 22000.2538), dilengkapi dengan prosesor AMD Ryzen 5 PRO 2500U yang memiliki Radeon Vega Mobile Gfx dan kecepatan sekitar 2.0 GHz, serta RAM berkapasitas 16 GB. Selain itu, alat-alat yang diperlukan dalam penelitin meliputi Python, Seikit-Learn, TensorFlow, dan Keras.

3. Result and Discusion

Bagian ini mencakup hasil eksperimen yang telah dilakukan menggunakan *Deep Neural Network* (DNN) untuk mendeteksi serangan jaringan pada dataset *CICIoT 2024*, termasuk laporan dari Langkah-langkah reduksi fitur dan uji kinerja algoritma DNN. Dalam pembahasan ini, akan di eveluasi efektivitas proses reduksi fitur serta analisis kinerja algoritma DNN. Model DNN yang dikembangkan menunjukkan akurasi yang tinggi dalam mendeteksi serangan DoS dan spoofing pada dataset CICIoT 2024. Hasil ini konsisten dengan temuan dari penelitian lain yang menggunakan teknik machine learning untuk meningkatkan keamanan IoT. Sebagai contoh, sebuah studi menemukan bahwa integrasi machine learning dalam sistem IoT dapat secara signifikan meningkatkan kemampuan deteksi ancaman [15].

3.1 Machine Learning (ML) Evaluation

Eksperimen yang dilakukan dalam penelitian ini menilai kinerja algoritma *Deep Neural Network* (DNN). Masalah klasifikasi dipertimbangkan menggunakan representasi decimal. Dalam kasus decimal, model diharapkan dapat mengklasifikasikan instance menjadi Benign, DoS, Spoofing Steering_Wheel, spoofing gas, spoofing RPM, dan spoofing speed. Fig.6 menggambarkan hasil yang diperoleh untuk semua scenario (5 fitur, 8 fitur , all fitur) untuk repsentasi decimal terkait akurasi, recall, presisi, dan F1-score.

Sebagian besar model menunjukkan kinerja yang baik untuk tugas klasifikasi yang melibatkan kelas decimal, menampilkan hasil bahwa DNN mampu berkinerja baik dalam pengkodean kelas decimal. Hasil menunjukkan bahwa klasifikasi decimal, hampir mencapai skor sempurna (1.0) ini menunjukkan bahwa lalu lintas serangan menunjukkan pola yang berbeda dibandingkan dengan benign. Fig.7 Menunjukkan hasil numerik dari setiap class (DATA_0 hingga DATA_7) terkait akurasi, recall, presisi, dan F1-score.

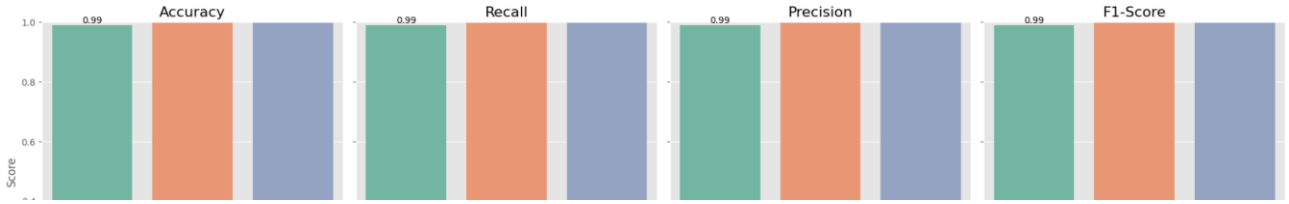


Fig.6. Hasil yang didapat dari machine learning evalution

Pengujian	Jumlah Fitur	Akurasi	Presisi	Recall
DATA_0	1	0.882474	0.900309	0.882474
DATA_1	1	0.871740	0.900953	0.871740
DATA_2	1	0.894271	0.888608	0.894271
DATA_3	1	0.926753	0.921934	0.926753
DATA_4	1	0.866395	0.885624	0.866395
DATA_5	1	0.878135	0.873707	0.878135
DATA_6	1	0.901790	0.889024	0.901791
DATA_7	1	0.929771	0.929109	0.929771

Fig.7. Hasil yang didapat setiap kelas dari machine learning evalution

3.2 Hasil Deteksi Deep Neural Network (DNN)

Setelah melalui proses *machine learning evaluation*, data dibagi menjadi dua bagian yaitu 80% data latih dan 20% data uji. Langkah pertama adalah melatih model DNN untuk mendeteksi serangan jaringan IoT dengan mempelajari pola-pola dari data latih. Model DNN dirancang dengan arsitektur hierarkis, yang terdiri dari lapisan masukan, dua lapisan tersembunyi, dan lapisan keluaran. Selama proses pelatihan, model mempelajari bobot dan bias yang dioptimalkan menggunakan algoritma Adam untuk memaksimalkan performa deteksi serangan. Fig.8 menunjukkan hasil percobaan yang mampu mendeteksi serangan dengan tingkat keberhasilan yang relating tinggi.

	precision	recall	f1-score	support
DoS	1.00	1.00	1.00	172842
SPOOFING	1.00	1.00	1.00	14857
BENIGN	1.00	1.00	1.00	22016
accuracy			1.00	209715
macro avg	1.00	1.00	1.00	209715
weighted avg	1.00	1.00	1.00	209715

Fig.8. Hasil deteksi DNN

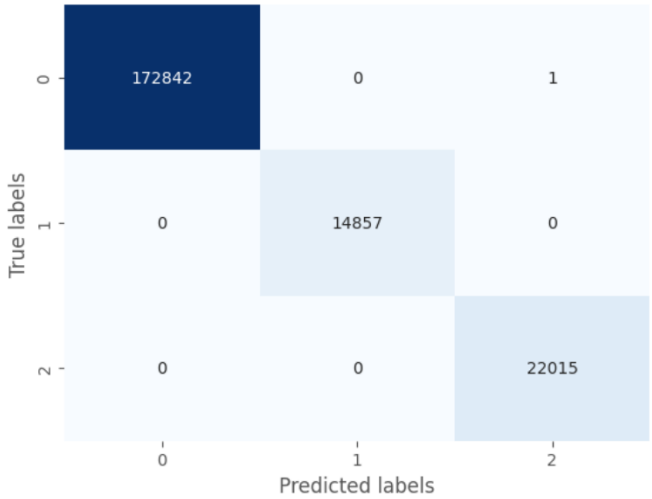


Fig.9. Confusion mastrix

Fig.9 adalah hasil pengujian menggunakan algoritma DNN pada dataset CICIoT 2024. Yang menunjukkan hasil yang sangat memuaskan berdasarkan tigas parameter evaluasi utama: akurasi, presisi, dan recall. Pengujian dilakukan dengan memvariasikan jumlah fitur yang digunakan, yaitu satu hingga delapan fitur. Hasil akurasi tertinggi diperoleh saat menggunakan seluruh delapan fitur (DATA_0 hingga DATA_7), dengan nilai mendekati 100%.

4. Conclusion

Perkembangan teknologi saat ini turut memengaruhi tingkat kerentanan keamanan pada jaringan IoT. Penelitian ini mengusulkan system deteksi intrusi menggunakan *Deep Neural Network* (DNN) untuk menganalisis dataset CICIoT 2024. Dataset ini mencakup 8 fitur utama (DATA_0 hingga DATA_7) yang mewakili data lalu lintas jaringan IoT. Penelitian ini mengevaluasi performa model DNN pada 8 fitur utama, untuk mengidentifikasi lalu lintas normal (Benign) dan serangan (DoS dan Spoofing).

Proses pelatihan dan pengujian dilakukan menggunakan data yang telah dinormalisasikan untuk memastikan konsistensi hasil. Hasil penelitian menunujukkan bahwa model DNN pada *Machine Learning* (ML) mencapai tingkat akurasi rata-rata sebesar 99.8% pada jaringan IoT kompleks. Akurasi tertinggi diperoleh saat menggunakan DNN pada seluruh 8 fitur, mencapai tingkat akurasi 100%. Hasil ini membuktikan bahwa metode *Deep Neural Network* (DNN) dapat menjadi solusi yang andal dan efektif untuk mendeteksi serangan pada jaringan IoT, sehinggan dapat meningkatkan keamanan jaringan secara signifikan.

Acknowledgment

Penelitian ini didukung oleh Universitas Dinamika Bangsa, Jambi, Indonesia

References

[1] S. E. O. H. K. B. B. Hosam El-Sofany, "Using machine learning algorithms to enhance IoT systemsecurity," 2024.

[2] A. A. A. Amer Dawood Saleem, "ATTACKS DETECTION IN INTERNET OF THINGS USING MACHINE LEARNING TECHNIQUES: A REVIEW," vol. 6, pp. 684-703, 2024.

[3] H. K. P. S. Syeda Manjia Tahsien, "Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey," 2020.

[4] A. I. G. M. Luigi Atzori, "The Internet of Things: A survey," vol. 54, no. 15, pp. 2787-2805, 2010.

[5] N. W. Lu Tan, "Future internet: The Internet of Things," vol. 5, 20 September 2010.

[6] e. a. Erwin, PENGANTAR & PENERAPAN INTERNET OF THINGS : Konsep Dasar & Penerapan IoT Di Berbagai Sektor, Sonpedia Publishing Indonesia, 2023.

[7] I. B. Mustafa Kocakulak, "An overview of Wireless Sensor Networks towards internet of things," pp. 1-6, 02 March 2017.

[8] R. R. S. T. Somayya Madakam, "Internet of Things (IoT): A Literature Review," vol. 3, 2015.

[9] F. G. D. V. A. S. Ahmadiki Firman Dwi Suryawan, "pjiseKeamanan IoTdan Sistem Terdistribusi," vol. 1, 2024.

[10] N. I. P. Zen Munawar, "KEAMANAN IOT DENGAN DEEP LEARNING DAN TEKNOLOGI BIG DATA," vol. 7, 2 Desember 2020.

[11] e. a. Wojciech, "Explaining Deep Neural," vol. 109, March 2021.

[12] K. E. A. W. Syifa Munawarah, "Deteksi Serangan DDoS SYN Flood Pada Jaringan Internet of Things (IoT) Menggunakan Metode Deep Neural Network (DNN)," vol. 4, pp. 982-990, April 2024.

[13] R. A. B. A. Satish Pokhrel, "IoT Security: Botnet detection in IoT using Machine learning," 2021.

[14] e. a. E. C. P. Neto, "University of New Brunswick," Canadian Institute for Cybersecurity, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/iov-dataset-2024.html. [Accessed 7 January 2024].

[15] G. T. Ayodele, "Machine Learning in IoT Security: Current Issues and Future Prospects," 2024.

Authors' Profiles

Budi Setiawan lahir di Jambi, Indonesia. Saat ini dia tengah menempuh Program Sarjana Ilmu Komputer di Universitas Dinamika Bangsa, Indonesia.

Raka Jumersyah Pratama lahir di Palembang, Indonesia. Saat ini dia tengah menempuh Program Sarjana Ilmu Komputer di Universitas Dinamika Bangsa, Indonesia.

Hengkky Restu Putra lahir di Jambi, Indonesia. Saat ini dia tengah menempuh Program Sarjana Ilmu Komputer di Universitas Dinamika Bangsa, Indonesia.

FA Bambang Sukoco FA Bambang Sukoco meraih gelar Sarjana di bidang Ilmu Komputer dari Universitas Sanata Dharma Jogjakarta, dan gelar M.S.I bidang Sistem Informasi dari Universitas Dinamika Bangsa, Jambi. Saat ini sedang aktif sebagai praktisi di bidang Jaringan Komputer dan dosen di Fakultas Ilmu Komputer, Universitas Dinamika Bangsa, Indonesia. Minat penelitiannya meliputi Rekasaya Perangkat Lunak, blockchain, dan keamanan jaringan.