TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 932-939
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8706

Deteksi Serangan DDoS (Distributed Denial of Service) Menggunakan Wavelet Decomposition dan Optimasi Hyperparameter Berbasis Optuna

Andi Khalil Gibran, Mustikasari, Darmatasia, Antamil*

Sains Dan Teknologi, Teknik Informatika, Universitas Islam Negeri Alauddin, Makassar, Indonesia
Email: [1]60200121010@uin-alauddin.ac.id, [2]mustikasari@uin-alauddin.ac.id, [3]darmatasia@uin-alauddin.ac.id,
[4,*]antamil@uin-alauddin.ac.id
Email Penulis Korespondensi: antamil@uin-alauddin.ac.id

Abstrak–Penelitian ini bertujuan untuk merancang dan mengembangkan sistem deteksi serangan *Distributed Denial of Service* (DDoS) berbasis *Wavelet Decomposition* yang mampu mengidentifikasi anomali trafik jaringan secara real-time. Permasalahan yang diangkat adalah tingginya tingkat *false positive* pada metode deteksi konvensional yang sering kali gagal membedakan antara lonjakan trafik sah dengan serangan. Penelitian ini menggunakan dua sumber data utama, yaitu dataset CICIDS2017 dan data *self-generated* yang merepresentasikan pola serangan DDoS terkontrol. Metode yang digunakan melibatkan penerapan *Discrete Wavelet Transform* (DWT) untuk mendekomposisi sinyal trafik menjadi komponen amplitudo dan energi. Selanjutnya, proses deteksi dilakukan menggunakan pendekatan *Median Absolute Deviation* (MAD) dan dioptimasi dengan tiga metode pencarian parameter: *Grid Search*, *Random Search*, dan *Optuna*. Hasil pengujian menunjukkan bahwa metode energi dengan optimasi *Optuna* memberikan kinerja terbaik dengan akurasi mencapai 98,6% pada dataset CICIDS2017 dan 99,4% pada data *self-generated*, serta tingkat kesalahan masing-masing 1,4% dan 0,6%. Penelitian ini memberikan kontribusi pada peningkatan akurasi sistem deteksi DDoS dengan beban komputasi yang ringan dan dapat diimplementasikan pada sistem jaringan skala besar.

Kata Kunci: DDoS; *Wavelet Decomposition*; *Discrete Wavelet Transform*; Anomali Trafik Jaringan; *Median Absolute Deviation*

Abstract–This study aims to design and develop a Distributed Denial of Service (DDoS) attack detection system based on Wavelet Decomposition capable of identifying network traffic anomalies in real-time. The main problem addressed is the high false positive rate in conventional detection methods, which often fail to distinguish between legitimate traffic bursts and actual attacks. Two primary data sources were used: the CICIDS2017 dataset and self-generated data representing controlled DDoS attack patterns. The proposed method applies Discrete Wavelet Transform (DWT) to decompose network traffic signals into amplitude and energy components. Detection is then performed using the Median Absolute Deviation (MAD) approach, optimized with three parameter search methods: Grid Search, Random Search, and Optuna. Experimental results indicate that the energy-based method with Optuna optimization achieves the best performance, with an accuracy of 98.6% on the CICIDS2017 dataset and 99.4% on the self-generated data, and error rates of 1.4% and 0.6%, respectively. This research contributes to enhancing the accuracy of DDoS detection systems with low computational overhead, making it suitable for large-scale network environments.

Keywords: DdoS; Wavelet Decomposition; Discrete Wavelet Transform; Network Traffic Anomaly; Median Absolute Deviation

1. PENDAHULUAN

Transformasi digital pada era revolusi industri 4.0 menuju *society* 5.0 telah membawa kemajuan signifikan dalam berbagai sektor, mulai dari pemerintahan, industri, hingga layanan publik. Pemanfaatan teknologi seperti *Internet of Things* (IoT), *cloud computing*, *big data*, dan kecerdasan buatan telah menjadikan jaringan komputer sebagai infrastruktur kritikal yang menopang aktivitas ekonomi, sosial, hingga pertahanan negara (Faiz dkk., 2022). Seiring meningkatnya ketergantungan terhadap infrastruktur ini, ancaman terhadap keamanan jaringan juga berkembang, dengan salah satu serangan yang paling masif dan merugikan adalah *Distributed Denial of Service* (DDoS).

Serangan DDoS bertujuan mengganggu ketersediaan layanan dengan membanjiri jaringan menggunakan trafik palsu dalam jumlah besar sehingga server tidak dapat memproses permintaan sah pengguna (Purba dkk., 2022). Dampaknya sangat signifikan, meliputi gangguan layanan publik, kerugian finansial, hingga menurunnya kepercayaan masyarakat terhadap sistem digital. Tantangan utama dalam mendeteksi serangan DDoS adalah sifatnya yang sering kali *real-time*, acak, serta menggunakan teknik penyamaran seperti *spoofing* dan *traffic shaping* yang membuat serangan tampak seperti aktivitas normal.

Penelitian terkait mengenai deteksi serangan DDoS telah banyak dilakukan dengan berbagai pendekatan. (Harto & Basuki, 2021) mengusulkan metode Random Forest pada jaringan berbasis *Software Defined Network* (SDN), yang menunjukkan akurasi cukup baik namun masih bergantung pada ekstraksi fitur manual dan pelatihan model yang intensif. (Tantriawan & Suryadi, 2021) memanfaatkan fuzzy logic model Sugeno untuk mendeteksi lalu lintas mencurigakan, tetapi memiliki keterbatasan dalam generalisasi terhadap pola serangan baru. Pendekatan deep learning seperti yang diusulkan (Elsayed dkk., 2020) dengan DDoSNet berbasis *Recurrent Neural Network* (RNN) berhasil mencapai akurasi tinggi, namun membutuhkan data pelatihan besar dan sumber daya komputasi tinggi sehingga kurang optimal untuk lingkungan dengan keterbatasan infrastruktur.

(Maulana ilham & Alamsyah, 2023) melakukan studi komparatif antara *Random Forest*, *Support Vector Machine* (SVM), *K-Nearest Neighbor* (KNN), dan *Multi-Layer Perceptron* (MLP) menggunakan dataset CICIDS2017, namun pendekatan mereka sepenuhnya bergantung pada model klasifikasi tradisional. Di sisi lain, (Munawarah & Arip Winanto, 2024) mengeksplorasi *Deep Neural Network* (DNN) untuk mendeteksi serangan SYN Flood pada *Internet of Things* (IoT), yang meskipun efektif, memiliki risiko *overfitting* dan memerlukan pelatihan intensif.

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 932-939
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8706

Berdasarkan penelitian-penelitian tersebut, terlihat adanya kesenjangan pada kebutuhan sistem deteksi DDoS yang dapat beroperasi secara *real-time*, tidak bergantung pada pelabelan data maupun pelatihan model kompleks, serta hemat sumber daya komputasi. Penelitian ini menawarkan solusi melalui penerapan metode *Wavelet Decomposition*, yang memproses sinyal jaringan pada domain waktu dan frekuensi secara simultan untuk mengekstraksi fitur fluktuasi amplitudo dan energi secara adaptif. Pendekatan ini dilengkapi dengan optimasi parameter berbasis Grid Search, Random Search, dan Optuna untuk meningkatkan kecepatan serta akurasi deteksi.

Kontribusi utama penelitian ini adalah pengembangan sistem deteksi serangan DDoS *real-time* berbasis *Wavelet Decomposition* yang tidak memerlukan data berlabel maupun pembelajaran mesin, namun mampu mengidentifikasi pola serangan termasuk pola serangan periodik dengan amplitudo tinggi secara cepat dan efisien. Dengan demikian, penelitian ini diharapkan dapat menjadi referensi dalam pengembangan solusi keamanan jaringan adaptif yang relevan untuk menghadapi dinamika serangan siber modern.

Selain itu, peningkatan kompleksitas serangan siber saat ini menuntut hadirnya pendekatan yang mampu memahami karakteristik trafik yang bersifat non-stasioner dan berubah secara dinamis. Pendekatan berbasis wavelet telah terbukti efektif dalam analisis sinyal yang memiliki fluktuasi cepat, karena mampu memberikan representasi lokal baik pada domain waktu maupun frekuensi. Berbeda dengan metode statistik konvensional yang hanya melihat sinyal secara global, wavelet memberikan kemampuan deteksi pola mikro yang sering muncul dalam serangan DDoS berbasis *burst*, intensitas tinggi, maupun pola serangan periodik. Hal ini sejalan dengan temuan pada beberapa studi terdahulu yang menunjukkan bahwa transformasi wavelet mampu meningkatkan sensitivitas terhadap perubahan trafik yang abrupt.

Di sisi lain, penggunaan strategi optimasi seperti Grid Search, Random Search, dan Optuna diperlukan untuk memastikan konfigurasi wavelet yang digunakan benar-benar optimal dalam mendeteksi anomali. Mengingat setiap jenis serangan memiliki pola energi dan amplitudo yang berbeda, proses tuning parameter menjadi krusial agar sistem dapat menyesuaikan diri dengan variasi burst, noise jaringan, maupun fluktuasi trafik normal. Optuna, dengan pendekatan Bayesian optimization dan pruning adaptivenya, memberikan keuntungan dalam efisiensi waktu eksekusi sehingga cocok diterapkan pada sistem monitoring jaringan yang membutuhkan keputusan cepat.

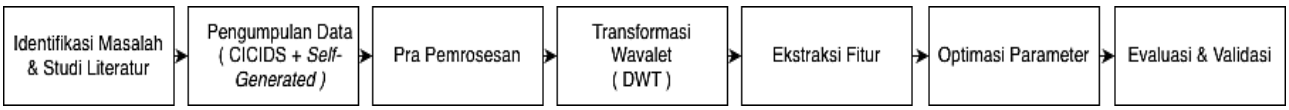
Penelitian ini juga memiliki urgensi praktis, mengingat infrastruktur digital di Indonesia maupun global semakin rentan terhadap serangan DDoS, khususnya pada sektor layanan publik, keuangan, dan pendidikan yang kini sepenuhnya terhubung melalui jaringan. Sistem yang mampu mendeteksi serangan tanpa ketergantungan pada model kompleks maupun dataset besar akan memberikan dampak signifikan bagi institusi yang memiliki keterbatasan sumber daya. Dengan memanfaatkan pemrosesan sinyal wavelet, sistem dapat diimplementasikan pada perangkat berkapasitas rendah sembari tetap mempertahankan performa deteksi yang baik.

Dengan demikian, penelitian ini tidak hanya memberikan kontribusi teoretis dalam pengembangan metode deteksi berbasis analisis sinyal, tetapi juga menawarkan solusi praktis yang dapat diterapkan pada skenario dunia nyata. Pendekatan ini diharapkan dapat menjadi penguat sistem pertahanan siber modern yang lebih adaptif, efisien, dan responsif terhadap ancaman serangan siber yang terus berkembang.

2. METODOLOGI PENELITIAN

2.1 Kerangka Dasar Penelitian

Penelitian ini merupakan penelitian rekayasa perangkat lunak yang bertujuan merancang dan mengembangkan sistem deteksi serangan *Distributed Denial of Service* (DDoS) berbasis *Wavelet Decomposition*. Serangan DDoS menjadi salah satu ancaman utama terhadap infrastruktur jaringan modern karena mampu melumpuhkan layanan daring melalui banjir trafik palsu yang sulit dibedakan dari trafik normal, sehingga mengakibatkan gangguan layanan publik maupun kerugian ekonomi yang signifikan (Purba dkk., 2022). Sumber data terdiri atas dua jenis: dataset CICIDS2017 yang telah menjadi acuan baku dalam penelitian keamanan jaringan (Harto & Basuki, 2021), serta data *self-generated* yang dibuat untuk merepresentasikan pola serangan DDoS terkontrol dengan karakteristik serangan periodik dan amplitudo tinggi.



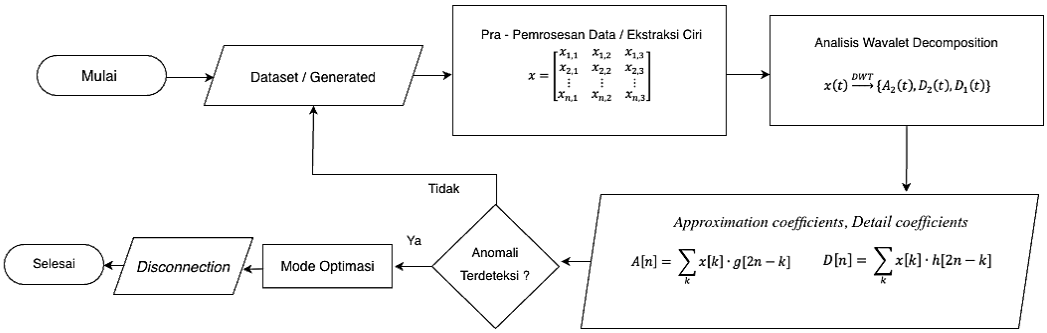
Gambar 1. Kerangka Dasar Penelitian

Variabel utama yang digunakan adalah amplitudo sinyal trafik jaringan dan energi hasil dekomposisi wavelet. Kedua variabel ini dipilih karena dapat memberikan gambaran kuantitatif mengenai perubahan intensitas trafik yang mengindikasikan adanya serangan. Hipotesis yang diajukan adalah bahwa pola serangan DDoS dapat diidentifikasi secara real-time dengan mengukur penyimpangan amplitudo atau energi terhadap karakteristik trafik normal menggunakan metode *Median Absolute Deviation* (MAD) (Chen dkk., 2025). Pemilihan metode wavelet dilakukan karena kemampuannya mendeteksi perubahan mendadak pada domain waktu-frekuensi, sehingga sangat sesuai untuk menganalisis anomali trafik jaringan yang bersifat dinamis.

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 932-939
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8706

2.2 Tahapan Penelitian

Tahapan penelitian ini yang ditunjukan pada gambar 2 terkait *flowchart* sistem dimulai dengan pengumpulan data dari dua sumber yang telah disebutkan sebelumnya. Dataset CICIDS2017 digunakan sebagai *benchmark*, sedangkan data *self-generated* dihasilkan melalui simulasi serangan DDoS terkontrol pada lingkungan jaringan percobaan. Setelah data terkumpul, dilakukan proses *preprocessing* yang meliputi normalisasi data, sinkronisasi *timestamp* antara trafik normal dan serangan, serta pembersihan data dari anomali yang tidak relevan(Yu dkk., 2023) .



Gambar 2. Flowchart Sistem

Tahap selanjutnya adalah penerapan *Discrete Wavelet Transform* (DWT) untuk mendekomposisi sinyal trafik menjadi komponen *approximation* dan *detail*. Dari hasil dekomposisi ini, nilai amplitudo dan energi dianalisis untuk mendeteksi adanya anomali. Deteksi dilakukan dengan metode statistik berbasis median dan *Median Absolute Deviation* (MAD), yang memungkinkan sistem menetapkan ambang batas secara dinamis tanpa memerlukan data berlabel.

Untuk meningkatkan akurasi dan efisiensi deteksi, sistem ini dilengkapi dengan proses optimasi parameter. Tiga pendekatan optimasi yang digunakan adalah *Grid Search*, *Random Search*, dan *Optuna* . Ketiganya berperan dalam mencari konfigurasi ambang batas dan level dekomposisi yang memberikan hasil deteksi terbaik. Evaluasi sistem dilakukan melalui dua skenario, yaitu validasi terhadap *ground truth* pada dataset CICIDS2017 dan pengujian interpretatif pada data *self-generated*. Hasil dari kedua skenario ini digunakan untuk menilai kemampuan sistem dalam mendeteksi pola serangan DDoS baik pada data *benchmark* maupun trafik yang dihasilkan secara mandiri. Alur tahapan penelitian ditunjukkan pada Gambar 1. Persamaan dasar dari analisis trafik menggunakan *Discrete Wavelet Transform* dinyatakan dengan:

$$x(t) \xrightarrow{DWT} \{A_2(t), D_2(t), D_1(t)\} \quad (1)$$

Dimana *x(t)* dapat direpresentasikan sebagai kombinasi komponen aproksimasi $A_2(t)$ dan komponen detil $D_2(t)$ serta $D_1(t)$, dimana komponen detil berperan menyoroti perubahan mendadak akibat anomali atau kemungkinan serangan. Selanjutnya, nilai-nilai detil hasil transformasi tersebut diproses menggunakan *Median Absolute Deviation* (MAD) sebagaimana dirumuskan pada Persamaan (2), yang berfungsi sebagai estimator penyebaran data yang lebih *robust* terhadap *outlier* dibandingkan standar deviasi.

$$MAD = median(|D - M|) \quad (2)$$

Tahap berikutnya yaitu penentuan ambang batas atau *threshold* adaptif seperti pada persamaan (3) dibawah:

$$T = M + 3 \times MAD \quad (3)$$

Dimana nilai rata-rata M ditambahkan 3 kali MAD untuk mengeliminasi variasi alami trafik dan memfokuskan analisis pada anomali signifikan. Deteksi berbasis amplitudo diuraikan dalam persamaan (4), yang menyatakan kondisi keputusan deteksi apabila deviasi sinyal detil $|D(t) - \mu D|$ melebihi ambang θA

$$A(t) = \begin{cases} 1, \\ 0, \end{cases} Jika\ |D(t) - \mu D| > \theta A \quad (4)$$

Formulasi energi sinyal pada persamaan (5) mendefinisikan total energi komponen detil melalui penjumlahan kuadrat amplitudo, sehingga perubahan energi dapat digunakan sebagai indikator kuantitatif terjadinya serangan DDoS.

$$E = \sum_n |D[n]|^2 \quad (5)$$

2.3 Justifikasi Pemilihan Metode Wavelet Decomposition

Pemilihan metode *Wavelet Decomposition* dalam penelitian ini didasarkan pada kemampuan teknik ini dalam menganalisis sinyal trafik jaringan secara simultan pada domain waktu dan skala (Sachenko dkk., 2024). Berbeda dengan transformasi Fourier yang hanya memberikan informasi frekuensi global, *Wavelet Transform* mampu menangkap perubahan lokal yang bersifat dinamis sehingga lebih sesuai untuk mendeteksi serangan DDoS yang sering kali muncul dalam bentuk fluktuasi amplitudo yang mendadak dan tidak beraturan.

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 932-939
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8706

Jenis wavelet yang digunakan adalah Daubechies-4 (db4) dengan level dekomposisi 4 karena memberikan kompromi optimal antara ketajaman deteksi dan beban komputasi. Pemilihan ini juga mempertimbangkan keterbatasan sumber daya pemrosesan dalam implementasi real-time, sehingga metode ini lebih ringan dibanding pendekatan berbasis pembelajaran mesin (*machine learning* maupun *deep learning*) yang memerlukan data berlabel dan proses pelatihan yang kompleks (Elsayed dkk., 2020).

2.4 Lingkungan Penelitian

Seluruh eksperimen dilakukan menggunakan bahasa pemrograman Python dengan integrasi antarmuka Gradio untuk memfasilitasi visualisasi hasil deteksi secara real-time (Wawrowski dkk., 2023). Beberapa pustaka utama yang digunakan meliputi:

a. PyWavelets untuk implementasi *Discrete Wavelet Transform*,
b. NumPy dan pandas untuk pemrosesan dan manajemen data,
c. Optuna untuk optimasi parameter deteksi, serta
d. Matplotlib untuk visualisasi koefisien wavelet dan hasil anomali.

Konfigurasi perangkat lunak ini dipilih untuk mendukung pemrosesan data secara efisien serta memungkinkan integrasi dengan sistem deteksi real-time tanpa memerlukan komputasi tingkat tinggi.

2.5 Konfigurasi Penelitian

Konfigurasi parameter *Discrete Wavelet Transform* (DWT) pada penelitian ini ditentukan berdasarkan karakteristik panjang sinyal dan kebutuhan analisis serangan DDoS secara real-time. Pemilihan level dekomposisi dilakukan dengan mempertimbangkan kompromi antara detail informasi dan kompleksitas komputasi. Pada penelitian ini, level dekomposisi optimal yang digunakan adalah level 4 dengan jenis wavelet Daubechies-4 (db4) karena memberikan keseimbangan yang baik antara akurasi deteksi dan efisiensi pemrosesan yang di tunjukkan pada tabel 1 berikut.

Tabel 1. Konfigurasi Parameter DWT

Parameter	Deskripsi
Level Dekomposisi	4 (ditentukan dari panjang sinyal dan panjang filter db4)
Koefisien Aproksimasi	Diambil dari level tertinggi untuk merepresentasikan pola umum
Koefisien Detail	Digunakan untuk mendeteksi serangan pada perubahan sinyal

Koefisien aproksimasi diambil dari level tertinggi untuk merepresentasikan pola umum trafik jaringan, sedangkan koefisien detail digunakan untuk menangkap perubahan sinyal yang menjadi indikator adanya anomali. Selanjutnya, proses deteksi dilakukan dengan menerapkan nilai ambang (*threshold*) pada masing-masing level dekomposisi. Konfigurasi lengkap parameter yang digunakan dalam penelitian ini ditampilkan pada Tabel 1, sedangkan hasil uji coba tiap level dekomposisi beserta nilai *threshold* dan jumlah serangan yang berhasil dideteksi disajikan pada Tabel 2.

Tabel 2. Konfigurasi Level Dekomposisi

Level Dekomposisi	Jenis Wavelet	Threshold	Jumlah Deteksi Serangan
1	Daubechies-4 (db4)	0.5	3681
2	Daubechies-4 (db4)	1.0	2953
3	Daubechies-4 (db4)	1.5	2720
4	Daubechies-4 (db4)	2.0	2589

3. HASIL DAN PEMBAHASAN

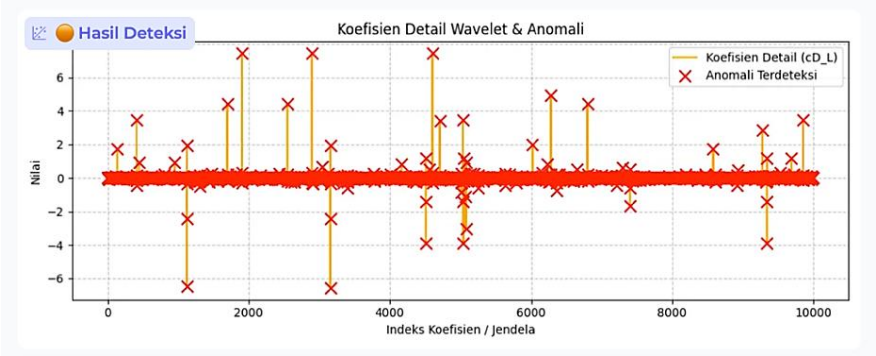
3.1 Hasil Deteksi Berbasis Amplitudo

Metode amplitudo diuji menggunakan level dekomposisi 1 yang terdapat pada Tabel 3, yang pada penelitian ini terbukti paling sensitif dalam mendeteksi pola serangan DDoS. Hasil pengujian pada dataset CICIDS2017 dan *self-generated* menunjukkan performa yang cukup tinggi dalam mendeteksi serangan, namun metode ini rentan terhadap *false positive* akibat lonjakan trafik sah sebagaimana divisualisasikan pada Gambar 3 dan Gambar 4 .

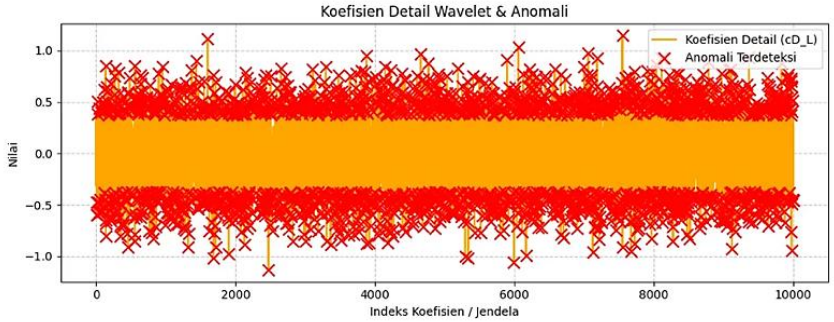
Tabel 3. Hasil Deteksi Amplitudo (Non-Optimasi)

Dataset	Jumlah Deteksi	Akurasi (%)	Kesalahan (%)
CICIDS2017	3.611	98,1	1,9
Self-Generated	2.081	98	2

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 932-939
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8706



Gambar 2. Deteksi *Threshold* 1, Level 1, CICIDS2017 Amplitudo



Gambar 3. Deteksi *Threshold* 1, Level 1, *Self-Generated* Amplitudo

Optimasi parameter dilakukan menggunakan *Grid Search*, *Random Search*, dan *Optuna*. Hasilnya menunjukkan peningkatan akurasi pada data *self-generated*, sedangkan pada dataset CICIDS2017 perubahan akurasi tidak signifikan yang ditunjukan pada Tabel 4 berikut.

Tabel 4. Hasil Optimasi Amplitudo

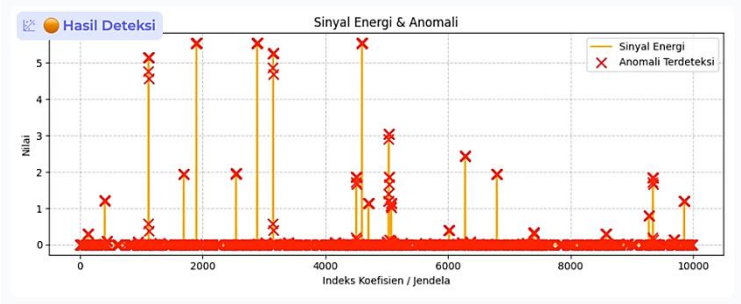
Metode Optimasi	Dataset	Jumlah Deteksi	Akurasi (%)	Kesalahan (%)
Grid Search	CICIDS2017	3.611	98,1	1,9
Random Search	CICIDS2017	3.609	98,1	1,9
Optuna	CICIDS2017	3.600	98,1	1,9
Grid Search	Self-Generated	2.072	99,6	0,4
Random Search	Self-Generated	919	98,1	1,9
Optuna	Self-Generated	2.010	99,2	0,8

3.2 Hasil Deteksi Berbasis Energi

Metode energi diterapkan pada konfigurasi yang sama dengan amplitudo. Kemudian pada Tabel 5 hasil menunjukkan bahwa metode ini lebih stabil terhadap variasi trafik normal dan memberikan performa yang lebih baik dalam menekan *false positive* yang dibuktikan dengan visualisasi Gambar 5 dan Gambar 6.

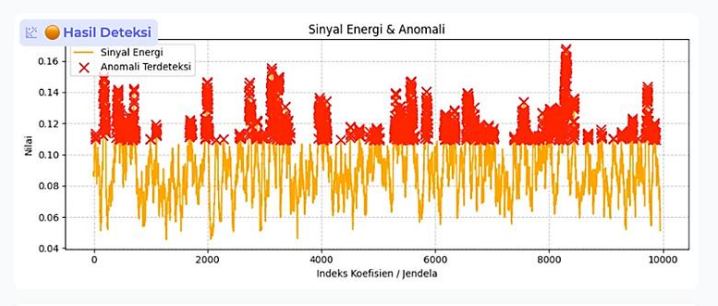
Tabel 5. Hasil Deteksi Energi (Non-Optimasi)

Dataset	Jumlah Deteksi	Akurasi (%)	Kesalahan (%)
CICIDS2017	3.681	98,1	1,9
Self-Generated	1.803	97	3



Gambar 4. Deteksi Threshold 1, Level 1, CICIDS2017 Energi

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 932-939
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8706



Gambar 5. Deteksi *Threshold* 1, Level 1, *Self-Generated* Energi

Setelah optimasi parameter, metode energi menunjukkan peningkatan signifikan, terutama menggunakan *Optuna*, yang memberikan keseimbangan terbaik antara jumlah deteksi dan kesalahan.

Tabel 6. Hasil Optimasi Energi

Metode Optimasi	Dataset	Jumlah Deteksi	Akurasi (%)	Kesalahan (%)
Grid Search	CICIDS2017	3.681	98,1	1,9
Random Search	CICIDS2017	2.325	95,4	4,6
Optuna	CICIDS2017	3.524	98,6	1,4
Grid Search	Self-Generated	1.591	99,5	0,5
Random Search	Self-Generated	19	95,5	4,5
Optuna	Self-Generated	1.955	99,4	0,6

3.3 Pembahasan

Metode berbasis amplitudo pada penelitian ini menunjukkan kemampuan yang cukup baik dalam mendeteksi serangan *Distributed Denial of Service* (DDoS) baik pada dataset CICIDS2017 maupun data *self-generated*. Konfigurasi terbaik diperoleh pada level dekomposisi 1, yang menghasilkan sensitivitas tinggi terhadap lonjakan trafik mencurigakan (Shekhar dkk., 2022). Namun, metode ini rentan terhadap *false positive* yang disebabkan oleh fluktuasi trafik sah, sebagaimana juga ditemukan pada penelitian sejenis yang menggunakan pendekatan berbasis nilai amplitudo untuk analisis anomali trafik jaringan (Purohit dkk., 2025). Temuan ini selaras dengan studi wavelet-based intrusion detection yang menyebutkan bahwa fitur amplitudo sangat sensitif terhadap variasi lokal sinyal dan mudah memicu deteksi berlebih (Natarajan dkk., 2023)

Hasil pengujian non-optimasi amplitudo menunjukkan tingkat akurasi yang relatif baik dengan rata-rata di atas 98%, namun peningkatan yang diperoleh setelah optimasi menggunakan *Grid Search*, *Random Search*, dan *Optuna* tidak signifikan pada dataset CICIDS2017. Pada data *self-generated*, terdapat peningkatan akurasi terutama ketika menggunakan *Optuna*, yang mengoptimalkan ambang batas deteksi secara lebih adaptif (Shekhar dkk., 2022). Sebaliknya, metode berbasis energi memberikan kinerja yang lebih stabil. Pengukuran energi pada sinyal trafik memungkinkan pendeteksian pola serangan yang lebih robust terhadap variasi minor dan *burst traffic*. Pada pengujian awal tanpa optimasi, metode energi mampu mendeteksi serangan dengan tingkat kesalahan yang lebih rendah dibandingkan amplitudo. Setelah dilakukan optimasi parameter, terutama dengan pendekatan *Optuna*, metode energi menunjukkan peningkatan akurasi hingga 98,6% pada dataset CICIDS2017 dan 99,4% pada data *self-generated*, dengan kesalahan deteksi hanya 1,4% dan 0,6% masing-masingnya. Hasil ini mengonfirmasi bahwa pemilihan metode energi yang dioptimasi memberikan keseimbangan yang lebih baik antara sensitivitas dan presisi (Sachenko dkk., 2024)(Purohit dkk., 2025).

Perbandingan kedua metode tersebut mengindikasikan bahwa amplitudo lebih sesuai untuk sistem yang membutuhkan deteksi cepat dan sensitif, meskipun berpotensi menghasilkan *false positive* yang lebih tinggi. Sementara itu, energi lebih direkomendasikan untuk implementasi real-time di mana stabilitas dan keakuratan menjadi prioritas, seperti pada jaringan *Internet of Things* (IoT) atau lingkungan *edge computing* (Munawarah & Arip Winanto, 2024). Proses optimasi berperan penting dalam meningkatkan performa sistem. Pendekatan *Grid Search* memberikan hasil yang konsisten namun terbatas karena ruang pencariannya kaku (Tantriawan & Suryadi, 2021). *Random Search* bersifat lebih variatif tetapi tidak selalu menemukan konfigurasi terbaik (Maulana ilham & Alamsyah, 2023). *Optuna*, yang menggunakan pendekatan pencarian berbasis *Bayesian optimization*, terbukti lebih efektif dalam menemukan parameter optimal untuk metode berbasis energi (Hidayaturrohman & Hanada, 2025) (Yaqin dkk., 2025)

Keterbatasan dari penelitian ini antara lain belum adanya pengujian pada serangan multi-vektor, belum dilakukannya evaluasi terhadap trafik terenkripsi, dan belum diimplementasikannya pendekatan hibrida yang menggabungkan metode wavelet dengan pembelajaran mesin atau *deep learning* (Faiz dkk., 2022) (Tantriawan & Suryadi, 2021) Rencana pengembangan selanjutnya adalah mengintegrasikan metode ini dengan *adaptive threshold* (Yuliswar dkk., 2025), mengujinya dalam arsitektur *cloud-native*, serta mengeksplorasi kombinasi *wavelet transform* dengan model *deep learning* untuk meningkatkan ketahanan deteksi terhadap pola serangan yang lebih kompleks (Wawrowski dkk., 2023)(Chen & Kao, 2025).

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 932-939
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8706

Temuan penelitian ini selaras dengan studi sebelumnya yang menekankan pentingnya optimasi parameter dalam deteksi anomali jaringan. (Saeed & Jameel, 2021) menunjukkan bahwa proses pemilihan parameter berbasis optimasi, seperti PSO, dapat meningkatkan akurasi tanpa menambah beban komputasi, sejalan dengan hasil penelitian ini dimana Optuna memberikan peningkatan paling konsisten. Selain itu, (Said dkk., 2024) mengidentifikasi bahwa pola gangguan sinyal yang bersifat osilatif dan beramplitudo tinggi sering tidak terdeteksi oleh metode konvensional, sehingga mendukung penggunaan pendekatan berbasis wavelet yang mampu menangkap perubahan sinyal non-stasioner.

Temuan dari (Said dkk., 2023)juga memperkuat bahwa analisis multiresolusi seperti wavelet efektif dalam mendeteksi anomali pada sistem real-time dengan variasi trafik yang dinamis. Dengan demikian, tambahan referensi ini mengonfirmasi bahwa metode berbasis energi yang dioptimasi Optuna merupakan pendekatan paling stabil dan presisi untuk mendeteksi serangan DDoS pada lingkungan jaringan modern.

3.4 Analisis Optimasi Parameter

Optimasi parameter merupakan tahap penting dalam meningkatkan kinerja sistem deteksi serangan DDoS berbasis Wavelet Decomposition. Proses ini bertujuan mencari kombinasi nilai parameter yang menghasilkan keseimbangan terbaik antara akurasi dan efisiensi deteksi. Dalam penelitian ini, tiga metode optimasi digunakan, yaitu *Grid Search*, *Random Search*, dan *Optuna*.

Metode *Grid Search* melakukan pencarian menyeluruh terhadap seluruh kombinasi parameter yang mungkin, namun memiliki kelemahan utama pada waktu komputasi yang sangat tinggi (Tantriawan & Suryadi, 2021). Sementara itu, *Random Search* melakukan pencarian acak dalam ruang parameter yang lebih luas dan relatif cepat, tetapi kurang efisien dalam menemukan konfigurasi optimal (Maulana ilham & Alamsyah, 2023).

Optuna menawarkan pendekatan yang lebih adaptif melalui optimasi berbasis *Tree-structured Parzen Estimator* (TPE) yang menggunakan model probabilistik untuk memprediksi kombinasi parameter terbaik pada setiap iterasi. Dengan prinsip *define-by-run* API, Optuna memungkinkan eksplorasi dinamis terhadap ruang parameter serta fitur pruning otomatis untuk menghentikan percobaan yang tidak menjanjikan (Shekhar dkk., 2022). Dalam penelitian ini, ruang parameter yang dioptimasi meliputi level dekomposisi wavelet, nilai ambang batas (*threshold*), dan variabel energi sinyal hasil transformasi. Berdasarkan hasil pengujian pada Tabel 4 dan 6, metode Optuna menghasilkan kinerja terbaik dengan akurasi mencapai 98,6% pada dataset CICIDS2017 dan 99,4% pada data self-generated, serta tingkat kesalahan masing-masing 1,4% dan 0,6%. Hal ini menunjukkan bahwa mekanisme pencarian adaptif *Optuna* mampu menemukan konfigurasi parameter yang lebih optimal dibandingkan dua metode konvensional lainnya.

Keunggulan *Optuna* dibandingkan *Grid Search* dan *Random Search* terletak pada kemampuannya melakukan eksplorasi yang efisien tanpa harus menguji seluruh kombinasi parameter. Dengan memanfaatkan informasi dari hasil percobaan sebelumnya, Optuna dapat mempersempit ruang pencarian ke area yang memiliki probabilitas tinggi menghasilkan performa lebih baik. Hal ini membuat proses optimasi berjalan lebih cepat dengan hasil yang lebih konsisten. Hasil ini sejalan dengan temuan (Hidayaturrohman & Hanada, 2025) yang menunjukkan bahwa optimasi berbasis *Bayesian* memiliki tingkat konvergensi lebih baik dibandingkan metode *brute force*. Dengan demikian, penerapan Optuna dalam sistem deteksi DDoS berbasis Wavelet Decomposition tidak hanya meningkatkan akurasi, tetapi juga efisiensi proses komputasi.

4. KESIMPULAN

Penelitian ini berhasil merancang sistem deteksi DDoS berbasis *Wavelet Decomposition* yang mampu mengidentifikasi anomali trafik secara real-time dengan akurasi tinggi dan beban komputasi rendah. Hasil penelitian menunjukkan bahwa metode berbasis amplitudo mampu mendeteksi pola serangan dengan sensitivitas tinggi, tetapi cenderung menghasilkan tingkat *false positive* lebih besar karena fluktuasi trafik normal. Sebaliknya, metode berbasis energi memberikan stabilitas dan presisi lebih baik, terutama setelah proses optimasi parameter menggunakan *Optuna*, yang memberikan peningkatan signifikan terhadap kinerja sistem. Konfigurasi terbaik yang dicapai menghasilkan akurasi 98,6% pada dataset CICIDS2017 dan 99,4% pada data *self-generated*, menunjukkan kemampuan metode energi dalam menangani pola serangan yang konsisten. Penelitian ini memberikan kontribusi penting dalam pengembangan sistem deteksi intrusi berbasis analisis sinyal dengan pendekatan wavelet, khususnya untuk lingkungan jaringan yang membutuhkan deteksi cepat dan akurat seperti IoT dan *edge computing*. Adapun keterbatasan penelitian ini mencakup belum diuji dengan tipe serangan multi-vektor, belum diterapkan pada trafik terenkripsi, serta belum dieksplorasi integrasi dengan metode *machine learning* atau *deep learning*. Pengembangan lanjutan diarahkan pada implementasi *adaptive threshold*, pengujian pada beban jaringan lebih besar, serta perluasan model deteksi untuk berbagai pola serangan modern.

REFERENCES

Chen, W.-Y., Pao, T.-L. & Kao, Y. (2025). Malware Traffic And Ransomware Anomaly Detection Based On Wavelet Time-Frequency Analysis And Deep Learning. *Advances In Artificial Intelligence And Machine Learning; Research*, *5*(2), 3866–3882. https://doi.org/10.54364/AAIML.2025.52219

Elsayed, M. S., Le-Khac, N.-A., Dev, S. & Jurcut, A. D. (2020). *Ddosnet: A Deep-Learning Model For Detecting Network Attacks*. http://Arxiv.org/Abs/2006.13981

TIN: Terapan Informatika Nusantara
Vol 6, No 7, December 2025, page 932-939
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v6i7.8706

Faiz, M. N., Somantri, O. & Muhammad, A. W. (2022). Rekayasa Fitur Berbasis Machine Learning Untuk Mendeteksi Serangan Ddos. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi*, *11*(3), 176-182. https://doi.org/10.22146/jnteti.v11i3.3423

Harto, M. K. & Basuki, A. (2021). *Deteksi Serangan Ddos Pada Jaringan Berbasis Sdn Dengan Klasifikasi Random Forest*, 5(4), 1329-1333. http://J-Ptiik.Ub.Ac.Id

Hidayaturrohman, Q. A. & Hanada, E. (2025). A Comparative Analysis Of Hyper-Parameter Optimization Methods For Predicting Heart Failure Outcomes. *Applied Sciences (Switzerland)*, *15*(6), 1-17. https://doi.org/10.3390/App15063393

Maulana Ilham & Alamsyah. (2023). Optimalisasi Deteksi Serangan Ddos Menggunakan Algoritma Random Forest, Svm, Knn Dan Mlp Pada Jaringan Komputer. *Indonesian Journal Of Mathematics And Natural Sciences*, *46*(2), 83-92. http://dx.doi.org/10.15294/ijmns.v46i2.48231

Munawarah, S. & Arip Winanto, E. (2024). Deteksi Serangan Ddos Syn Flood Pada Jaringan Internet Of Things (Iot) Menggunakan Metode Deep Neural Network (Dnn). *Jurnal Informatika Dan Rekayasa Komputer (Jakakom)*, *4*(1), 982-990. https://doi.org/10.33998/Jakakom.V4i1

Natarajan, S., Thangamuthu, M., Gnanasekaran, S. & Rakkiyannan, J. (2023). Digital Twin-Driven Tool Condition Monitoring For The Milling Process. *Sensors*, *23*(12), 1-16. https://doi.org/10.3390/S23125431

Purba, R., Lestari, W. S. & Ulina, M. (2022). Deteksi Serangan Ddos Mengunakan Deep Q-Network. *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(1), 684–658. https://doi.org/10.35957/jatisi.v9i1.1473

Purohit, R., Kumar, S., Sayyad, S. & Kotecha, K. (2025). Time-Frequency Analysis And Autoencoder Approach For Network Traffic Anomaly Detection. *MethodsX*, *14*, *1-11*. https://doi.org/10.1016/J.Mex.2025.103228

Sachenko, A., Woloszyn, J. & Rimashevskyi, S. (2024, Mei 25). Enhancing Network Security Through Wavelet Analysis. *Proceedings Of The 8th International Conference On Computational Linguistics And Intelligent Systems. Volume Iii: Intelligent Systems Workshop*. https://doi.org/10.31110/Colins/2024-3/027

Saeed, A. A. & Jameel, N. G. M. (2021). Intelligent Feature Selection Using Particle Swarm Optimization Algorithm With A Decision Tree For Ddos Attack Detection. *International Journal Of Advances In Intelligent Informatics*, *7*(1), 37–48. https://doi.org/10.26555/Ijain.V7i1.553

Said, A., Gotoh, Y. & Matsuo, T. (2023). Assessment Of Replay Attacks Against Power System Stabilizer. *Proceedings of the 10th IIAE International Conference on Intelligent Systems and Image Processing 2023*. 4–10. https://doi.org/10.12792/Icisip2023.004

Said, A., Gotoh, Y. & Matsuo, T. (2024). Assessment Of Cyber Attacks Against Power System Stabilizer And Their Detection Using Phasor Measurement Units. *Journal Of The Institute Of Industrial Applications Engineers*, *12*(3), 48–57. https://doi.org/10.12792/Jiiae.12.48

Shekhar, S., Bansode, A. & Salim, A. (2022). *A Comparative Study Of Hyper-Parameter Optimization Tools*. http://Arxiv.org/Abs/2201.06433

Tantriawan, H. & Suryadi, M. (2021). Deteksi Distributed Denial Of Service (Ddos) Menggunakan Logika Fuzzy Sugeno. *Malcom: Indonesian Journal Of Machine Learning And Computer Science*, *1*(2), 144–154. https://doi.org/10.57152/Malcom.V1i2.95

Wawrowski, Ł., Białas, A., Kajzer, A., Kozłowski, A., Kurianowicz, R., Sikora, M., Szymańska-Kwiecień, A., Uchroński, M., Białczak, M., Olejnik, M. & Michalak, M. (2023). Anomaly Detection Module For Network Traffic Monitoring In Public Institutions. *Sensors*, *23*(6), 1-18. https://doi.org/10.3390/S23062974

Yaqin, A. A., Barata, M. A. & Mahmudah, N. (2025). Implementation Of The Random Forest Algorithm With Optuna Optimization In Lung Cancer Classification. *Sistemasi: Jurnal Sistem Informasi*, *14*(2), 561–569. https://doi.org/10.32520/stmsi.v14i2.4877

Yu, B., Zhang, Y., Xie, W., Zuo, W., Zhao, Y. & Wei, Y. (2023). A Network Traffic Anomaly Detection Method Based On Gaussian Mixture Model. *Electronics (Switzerland)*, *12*(6), 1-9. https://doi.org/10.3390/Electronics12061397

Yuliswar, T., Elfitri, I. & Purbo, O. W. (2025). Optimization Of Intrusion Detection System With Machine Learning For Detecting Distributed Attacks On Server Optimalisasi Sistem Deteksi Intrusi Menggunakan Machine Learning Untuk Deteksi Serangan Terdistribusi Pada Server. *Jurnal Inovtek Polbeng - Seri Informatika*, *10*(1), 367-376. https://doi.org/10.35314/vem9da98