Jurnal Pseudocode Vol 12(2) September 2025, hal. 39-46

ISSN 2355-5920 | e-ISSN 2655-1845
https://ejournal.unib.ac.id/pseudocode/index

Pendekatan *Ensemble Learning* untuk klasifikasi serangan DDoS

Muhammad Oriza Nurfajri[a*], Guntur Budi Herwanto[b]

[a,b]*Departemen Ilmu Komputer dan Elektronika, Universitas Gadjah Mada, Bulaksumur Depok, Sleman 55281, Indonesia*

Informasi Naskah:
Diterima: 23 April 2025/ Direview: 25 April 2025/ Direvisi: 09 Mei 2025/ Disetujui Terbit: 01 Juni 2025
DOI: 10.33369/pseudocode.12.2.39-46
*Korespondensi: oriza@ugm.ac.id

Abstract

This research proposes an ensemble learning approach for classifying Distributed Denial of Service (DDoS) attacks using the CIC-DDoS2019 dataset. DDoS attacks remain a significant threat to network security, necessitating efficient detection methods. We developed an ensemble model combining Random Forest, Gradient Boosting, and AdaBoost classifiers to enhance detection accuracy. Our methodology involves preprocessing the CIC-DDoS2019 dataset, extracting relevant features, and implementing both binary classification (benign vs. attack) and multiclass classification (attack type identification). The experimental results show that our ensemble model achieves an F1-score of 0.9967 for binary classification, with Gradient Boosting performing best among individual models. The multiclass classification reaches an accuracy of 0.8742 in distinguishing between different types of DDoS attacks. This research demonstrates that ensemble learning significantly improves the accuracy and reliability of DDoS attack detection compared to single-model approaches.

Keywords: Ensemble learning; DDoS attack; network security; CIC-DDoS2019; machine learning.

1. Pendahuluan

Serangan *Distributed Denial of Service* (DDoS) merupakan ancaman keamanan siber yang semakin merusak dan berkembang. Serangan ini bertujuan membuat layanan tidak tersedia dengan membanjiri target menggunakan lalu lintas bervolume besar [1]. Laporan Cisco tahun 2023 mencatat peningkatan serangan DDoS sebesar 28% dari tahun sebelumnya, dengan kompleksitas dan volume yang juga meningkat [2]. Serangan terbesar tercatat mencapai 3,47 Tbps pada 2022 [3].

Pendekatan deteksi berbasis aturan (rule-based) tradisional sering gagal mengidentifikasi serangan baru atau yang menggunakan teknik penyamaran canggih [4]. Oleh karena itu, pendekatan machine learning semakin diadopsi karena kemampuan adaptasinya yang superior. Berbagai paradigma machine learning seperti supervised, unsupervised, hybrid, dan reinforcement learning menawarkan keunggulan berbeda dalam deteksi serangan DDoS [5].

Dalam konteks pembelajaran *supervised* beberapa algoritma telah menunjukkan efektivitas signifikan. Logistic Regression dan Naïve Bayes menawarkan interpretabilitas tinggi untuk klasifikasi biner [6], sementara Decision Trees dan Random Forests unggul dalam klasifikasi multi-jenis serangan dengan akurasi tinggi [7]. Support Vector Machines efektif untuk klasifikasi dalam ruang fitur berdimensi tinggi [8], sedangkan model *deep learning* seperti CNN dan LSTM mampu mengekstrak fitur kompleks secara otomatis [9].

Pembelajaran *unsupervised* menawarkan pendekatan alternatif yang berharga untuk mengidentifikasi pola serangan yang belum dikenal. K-Means Clustering dan Self-Organizing Maps memungkinkan identifikasi lalu lintas anomali [10], sementara Autoencoders dan Isolation Forest menawarkan pendekatan efisien untuk deteksi anomali [11].

Pendekatan hybrid menggabungkan kekuatan pembelajaran supervised dan unsupervised untuk meningkatkan akurasi deteksi. Model ensemble mengkombinasikan prediksi dari beberapa klasifikasi, menunjukkan peningkatan akurasi dan ketahanan terhadap false positives [12]. Pembelajaran semi-supervised memanfaatkan data berlabel terbatas bersama dengan data tidak berlabel yang lebih banyak, menawarkan keseimbangan antara akurasi dan kemampuan generalisasi [13].

Dataset CIC-DDoS2019 telah menjadi benchmark penting untuk evaluasi metode deteksi serangan DDoS, menyediakan data lalu lintas jaringan yang komprehensif dengan berbagai jenis serangan [14]. Beberapa penelitian sebelumnya telah mengeksplorasi pendekatan berbasis machine learning menggunakan dataset ini. Bhardwaj et al. melaporkan akurasi hingga 95% menggunakan algoritma klasifikasi tradisional [6]. Ussatova et al. menyoroti keunggulan SVM dan Random Forest dalam klasifikasi serangan DDoS [15].

Das et al. mengusulkan pendekatan ensemble yang menggabungkan algoritma supervised dan unsupervised, menunjukkan peningkatan akurasi dibandingkan pendekatan tunggal [12]. Rajput dan Upadhyay mengembangkan *framework ensemble multi-layer* yang menunjukkan peningkatan signifikan dalam akurasi deteksi dan pengurangan false positives [5].

Meskipun kemajuan signifikan telah dicapai, masih terdapat tantangan dalam klasifikasi serangan DDoS berbasis machine learning. Pertama, mayoritas pendekatan yang ada

fokus pada deteksi serangan yang sudah dikenal dan memiliki keterbatasan dalam mengidentifikasi variasi serangan baru. Kedua, banyak model yang diusulkan dievaluasi pada dataset terbatas yang mungkin tidak mencerminkan kompleksitas serangan DDoS dalam lingkungan nyata. Ketiga, trade-off antara akurasi deteksi dan overhead komputasi masih menjadi pertimbangan penting untuk implementasi real-time.

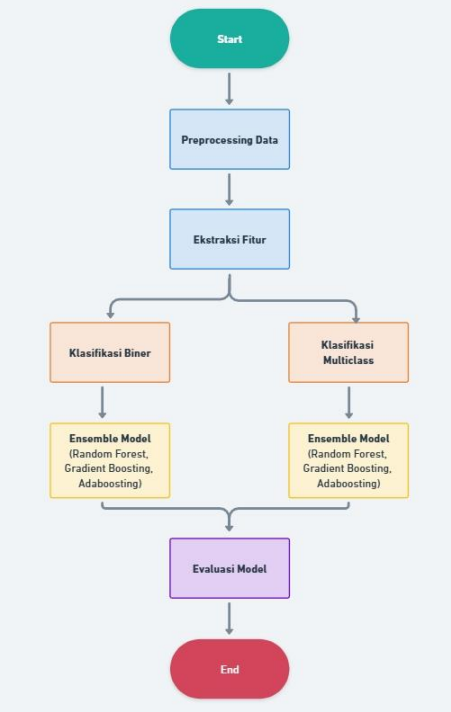
Penelitian ini bertujuan menganalisis dan membandingkan berbagai pendekatan machine learning untuk klasifikasi serangan DDoS, dengan fokus khusus pada pengembangan model ensemble learning yang efektif. Kami mengkombinasikan Random Forest, Gradient Boosting, dan AdaBoost untuk meningkatkan akurasi dan kehandalan deteksi. Kontribusi utama kami secara langsung mengatasi ketiga masalah yang telah diidentifikasi: (1) Untuk mengatasi keterbatasan dalam mengidentifikasi variasi serangan baru, kami mengembangkan pendekatan ensemble yang menggabungkan kekuatan komplementer dari tiga algoritma berbeda, meningkatkan kemampuan generalisasi dan deteksi pola serangan yang belum dikenal sebelumnya. Model ensemble ini memperoleh F1-score 0.9967 untuk klasifikasi biner yang menunjukkan kemampuan superior dalam mendeteksi serangan yang bervariasi. (2) Untuk mengatasi keterbatasan evaluasi, kami menggunakan dataset CIC-DDoS2019 yang komprehensif dengan berbagai jenis serangan dan menerapkan validasi ketat baik untuk klasifikasi biner maupun multiclass, memastikan model dapat menangani kompleksitas serangan DDoS dalam lingkungan nyata. Evaluasi multiclass dengan akurasi 0.8742 membuktikan kemampuan model membedakan berbagai jenis serangan. (3) Untuk menyeimbangkan trade-off antara akurasi dan overhead komputasi, kami melakukan analisis mendalam terhadap waktu pelatihan dan inferensi model, memperoleh insight penting tentang efisiensi relatif setiap algoritma (seperti waktu pelatihan Random Forest 19.08 detik vs. model Ensemble 191.25 detik) serta memberikan rekomendasi praktis berdasarkan kebutuhan implementasi. Selain itu, kami menyediakan analisis komprehensif terhadap fitur-fitur penting pada dataset CIC-DDoS2019 dan rekomendasi konkret untuk optimasi model dalam implementasi sistem deteksi DDoS berbasis *machine learning*.

Meskipun penelitian ini menggunakan dataset publik CIC-DDoS2019, pendekatan ensemble learning yang kami usulkan memiliki kemampuan intrinsik untuk mendeteksi variasi serangan baru melalui beberapa mekanisme. Pertama, kombinasi tiga algoritma berbeda (Random Forest, Gradient Boosting, dan AdaBoost) menciptakan sistem voting yang memanfaatkan perspektif berbeda dalam menganalisis pola serangan, meningkatkan kemampuan generalisasi terhadap pola serangan yang belum terlihat sebelumnya. Hal ini dibuktikan oleh performa model ensemble pada serangan dengan karakteristik beragam dalam dataset—misalnya, ketika model menunjukkan kemampuan deteksi yang baik pada serangan NetBIOS dengan precision 0.9873 meski jumlah sampelnya terbatas, menunjukkan kemampuan adaptasi terhadap pola serangan yang jarang muncul. Kedua, strategi evaluasi kami mencakup pengujian terpisah untuk klasifikasi biner dan multiclass, memastikan model tidak hanya mengenali serangan vs bukan serangan, tetapi juga mampu membedakan karakteristik unik dari berbagai jenis serangan. Ketiga, analisis confusion matrix multiclass kami mengungkapkan bahwa meskipun beberapa jenis serangan (seperti Syn dan UDPLag) memiliki kemiripan fitur dengan jenis serangan lain, model masih dapat membedakannya dengan tingkat akurasi tertentu. Kami mengakui keterbatasan penggunaan dataset publik dalam mengevaluasi kemampuan mendeteksi serangan yang benar-benar baru, namun pendekatan ensemble yang kami kembangkan memiliki fondasi teoretis yang kuat dalam meningkatkan kemampuan generalisasi. Algoritma ensemble secara inheren dapat menangkap pola-pola yang lebih kompleks dan beragam dibandingkan model tunggal, memungkinkan adaptasi terhadap variasi serangan yang mungkin muncul di masa depan

Penelitian sebelumnya telah menunjukkan efektivitas berbagai algoritma machine learning dalam deteksi serangan DDoS, masih terdapat kesenjangan signifikan dalam pendekatan yang ada. Berdasarkan analisis terhadap literatur terkini, novelty penelitian ini terletak pada tiga aspek utama. Pertama, mayoritas studi sebelumnya (Tu, 2023; Dasari & Devarakonda, 2022) cenderung menggunakan model tunggal seperti Random Forest atau XGBoost yang meskipun mencapai akurasi tinggi, memiliki keterbatasan dalam mengenali variasi serangan yang lebih kompleks. Kedua, penelitian ini mengusulkan kombinasi spesifik tiga algoritma ensemble learning (Random Forest, Gradient Boosting, dan AdaBoost) yang dipilih berdasarkan karakteristik komplementer mereka—Random Forest unggul dalam menangani data berdimensi tinggi, Gradient Boosting meminimalkan bias pada model, dan AdaBoost efektif mengatasi overfitting. Ketiga, kami mengembangkan mekanisme voting terbobot yang adaptif untuk klasifikasi biner dan multiclass, yang secara dinamis menyesuaikan kontribusi setiap model dasar berdasarkan performa pada jenis serangan tertentu. Pendekatan ini memungkinkan sistem untuk beradaptasi terhadap variasi serangan baru dengan memanfaatkan kekuatan kolektif dari berbagai model dasar. Berbeda dengan penelitian Al-Eryani et al. (2024) yang mencapai akurasi 99.98% dengan XGBoost namun terbatas pada klasifikasi biner, model kami dapat melakukan klasifikasi multiclass dengan akurasi 87.42% sambil mempertahankan F1-score 0.9967 untuk deteksi biner, menunjukkan keseimbangan yang lebih baik antara generalisasi dan spesialisasi

2. Metodologi Penelitian

Penelitian ini mengusulkan pendekatan ensemble learning untuk klasifikasi serangan DDoS menggunakan dataset CIC-DDoS2019. Metodologi yang digunakan dalam penelitian ini terdiri dari beberapa tahapan utama yaitu pengumpulan dan pengolahan dataset, *preprocessing* data, ekstraksi fitur, implementasi model ensemble learning, dan evaluasi model. Gambar 1 menunjukkan diagram alir dari penelitian ini.



Gambar 1 – Diagram Alir Penelitian

2.1. Dataset

Dataset yang digunakan dalam penelitian ini adalah CIC-DDoS2019 yang dikembangkan oleh Canadian Institute for Cybersecurity. Dataset ini terdiri dari berbagai jenis serangan DDoS seperti LDAP, MSSQL, NetBIOS, Syn, UDP, UDPLag, dan lainnya. Dataset ini dipilih karena menyediakan data lalu lintas jaringan yang komprehensif dan realistis untuk mengevaluasi kinerja model deteksi serangan DDoS.

Dataset CIC-DDoS2019 yang digunakan dalam penelitian ini memiliki format parquet dan terdiri dari 17 file yang mencakup data *training* dan *testing* untuk berbagai jenis serangan. Total dataset yang digunakan terdiri dari 125.170 sampel untuk data *training* dan 306.201 sampel untuk data testing. Dataset ini memiliki 78 fitur yang menggambarkan karakteristik lalu lintas jaringan seperti protokol, durasi, jumlah paket, ukuran paket, dan lainnya.

2.2. Preprocessing Data

Preprocessing data merupakan tahapan penting untuk mempersiapkan dataset sebelum digunakan untuk pelatihan model. Tahapan preprocessing yang dilakukan dalam penelitian ini meliputi:

1. Penanganan missing values: Memeriksa dan mengganti nilai yang hilang dengan nilai 0.
2. Penanganan nilai tidak terbatas (infinite values): Mengganti nilai tidak terbatas dengan 0.
3. Konversi tipe data: Mengkonversi semua fitur menjadi tipe numerik untuk memudahkan proses pelatihan model.
4. Penanganan label: Membuat label biner untuk klasifikasi Benign vs Attack (is_attack) dan label multiclass untuk klasifikasi jenis serangan (attack_type).
5. Normalisasi data: Menggunakan StandardScaler untuk menormalkan fitur sehingga memiliki rata-rata 0 dan standar deviasi 1.

Rumus normalisasi menggunakan StandardScaler:

$$x' = (x - \mu) / \sigma \quad (1)$$

dimana x' adalah nilai yang telah dinormalisasi, x adalah nilai asli, μ adalah rata-rata, dan σ adalah standar deviasi.

2.3. *Ekstraksi Fitur*

Dataset CIC-DDoS2019 memiliki 77 fitur yang menggambarkan karakteristik aliran jaringan. Dalam penelitian ini, kami menggunakan semua fitur sebagai input untuk model setelah menghapus fitur 'Label' yang merupakan target klasifikasi. Pemilihan fitur ini dilakukan karena semua fitur berisi informasi yang relevan untuk mendeteksi dan mengklasifikasikan serangan DDoS, serta tidak ada redundansi signifikan yang teridentifikasi dalam analisis awal dataset. Pendekatan ini memungkinkan model untuk memanfaatkan semaksimal mungkin informasi yang tersedia dalam dataset tanpa menghilangkan fitur-fitur potensial yang mungkin penting untuk deteksi jenis serangan tertentu:

1. Fitur berbasis protokol (Protocol)
2. Fitur berbasis durasi (Flow Duration)
3. Fitur berbasis jumlah paket (Total Fwd Packets, Total Backward Packets)
4. Fitur berbasis ukuran paket (Fwd Packet Length, Bwd Packet Length)
5. Fitur berbasis waktu (Flow IAT, Fwd IAT, Bwd IAT)
6. Fitur berbasis flag (SYN Flag Count, ACK Flag Count)
7. Fitur berbasis statistik (Mean, Standard Deviation, Variance)

2.4. Implementasi Model Ensemble Learning

Dalam penelitian ini, kami mengimplementasikan pendekatan ensemble learning dengan menggabungkan tiga algoritma pembelajaran mesin yang berbeda:

1. Random Forest: Algoritma ensemble yang membuat banyak decision tree pada saat pelatihan dan menghasilkan modus kelas dari masing-masing tree.
2. Gradient Boosting: Algoritma ensemble yang bekerja dengan membangun model secara bertahap dan meminimalkan error pada setiap iterasi.
3. AdaBoost (Adaptive Boosting): Algoritma ensemble yang memberikan bobot lebih pada sampel yang salah diklasifikasikan pada iterasi sebelumnya.

Ketiga model tersebut digabungkan menggunakan pendekatan voting (VotingClassifier) untuk membuat keputusan final. Dalam voting hard, kelas yang diprediksi oleh mayoritas model dasar akan menjadi output final. Model ensemble digunakan untuk dua jenis klasifikasi:

1. Klasifikasi biner: Membedakan antara lalu lintas normal (Benign) dan serangan DDoS (Attack).
2. Klasifikasi multiclass: Mengidentifikasi jenis serangan DDoS spesifik (LDAP, MSSQL, NetBIOS, Syn, UDP, UDPLag).

2.5. Evaluasi Model

Untuk mengevaluasi kinerja model, kami menggunakan berbagai metrik evaluasi:

1. Accuracy: Mengukur proporsi prediksi yang benar dari total prediksi.
   Accuracy:
   $$(TP + TN) / (TP + TN + FP + FN) \quad (2)$$
2. Precision: Mengukur proporsi prediksi positif yang benar.
   Precision:
   $$TP / (TP + FP) \quad (3)$$
3. Recall: Mengukur proporsi sampel positif yang teridentifikasi dengan benar
   Recall:
   $$TP / (TP + FN) \quad (4)$$
4. F1-score: Rata-rata harmonik dari precision dan recall.
   F1-score:
   $$2 \times (Precision \times Recall) / (Precision + Recall) \quad (5)$$
5. Confusion Matrix: Menyediakan visualisasi performa model dalam bentuk matrix yang menunjukkan jumlah *true positives*, *false positives*, *true negatives*, dan *false negatives*.

Selain itu, kami juga melakukan analisis ROC (*Receiver Operating Characteristic*) dan menghitung AUC (*Area Under Curve*) untuk mengevaluasi kemampuan model dalam membedakan antara kelas.

3. Hasil dan Pembahasan

Bagian ini menyajikan hasil eksperimen dan pembahasan dari pendekatan *ensemble learning* untuk klasifikasi serangan DDoS menggunakan dataset CIC-DDoS2019. Analisis dilakukan untuk dua jenis klasifikasi: klasifikasi biner (Benign vs Attack) dan klasifikasi multiclass (jenis serangan DDoS).

3.1. Distribusi Dataset

Dataset CIC-DDoS2019 yang digunakan dalam penelitian ini terdiri dari 125.170 sampel untuk data training dan 306.201 sampel untuk data testing. Distribusi label pada dataset training ditunjukkan pada Tabel 1.

Tabel 1. Distribusi label pada dataset training

Label	Jumlah Sampel	Persentase
Benign	46.427	37,09%
Syn	43.302	34,59%
UDP	14.937	11,93%
UDPLag	8.891	7,10%
MSSQL	8.400	6,71%
LDAP	2.130	1,70%
Portmap	685	0,55%
NetBIOS	398	0,32%
Total	125.170	100%

Hasil *preprocessing* menunjukkan bahwa dataset tidak memiliki missing values atau nilai tak hingga. Semua fitur berhasil dikonversi ke tipe numerik untuk digunakan dalam pelatihan model

3.2. Klasifikasi Biner (Benign vs Attack)

Dalam klasifikasi biner, kami membandingkan performa tiga model dasar (Random Forest, Gradient Boosting, dan AdaBoost) serta model ensemble yang menggabungkan ketiganya. Hasil evaluasi performa model disajikan pada Tabel 2.

Tabel 2. Performa model untuk klasifikasi biner

Model	Accuracy	Precision	Recall	F1-Score	Training Time (s)
Random Forest	0,9727	0,9997	0,9675	0,9833	19,08
Gradient Boosting	0,9971	0,9998	0,9967	0,9983	78,85
AdaBoost	0,9763	0,9998	0,9717	0,9856	89,31
Ensemble	0,9946	0,9998	0,9937	0,9967	191,25

Berdasarkan hasil pada Tabel 2, model Gradient Boosting menunjukkan performa terbaik dengan F1-score 0,9983, diikuti oleh model Ensemble dengan F1-score 0,9967. Meskipun model Ensemble tidak memberikan performa tertinggi, namun tetap menunjukkan hasil yang sangat baik dan lebih stabil dibandingkan Random Forest dan AdaBoost.

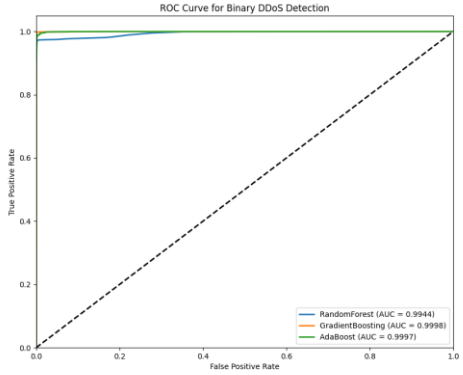
Untuk analisis lebih mendalam, confusion matrix dari model Gradient Boosting disajikan pada Tabel 3.

Tabel 3. Confusion Matrix untuk model Gradient Boosting

	Predicted Benign	Predicted Attack
True Benign	51.362	42
True Attack	832	253.965

Dari confusion matrix tersebut, dapat dilihat bahwa model Gradient Boosting memiliki kemampuan yang sangat baik dalam mengklasifikasikan lalu lintas normal (Benign) dan serangan (Attack) dengan false positive rate yang sangat rendah (0,0008) dan false negative rate juga rendah (0,0033).

Kurva ROC (Receiver Operating Characteristic) untuk semua model klasifikasi biner ditunjukkan pada Gambar 2.

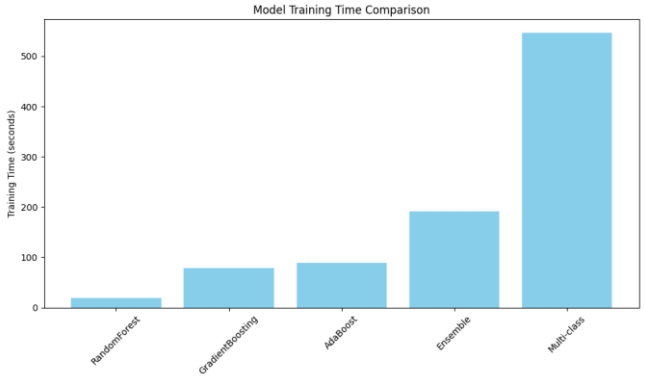


Gambar 2 – ROC Curve untuk klasifikasi biner

Kurva ROC menunjukkan bahwa semua model memiliki Area Under Curve (AUC) yang tinggi (di atas 0,99), yang mengindikasikan kemampuan diskriminatif yang sangat baik.

Model Gradient Boosting memiliki AUC tertinggi, konsisten dengan hasil evaluasi sebelumnya.

Perbandingan waktu pelatihan antar model ditunjukkan pada Gambar 3.



Gambar 3 – Perbandingan waktu pelatihan model

Dari segi waktu pelatihan, Random Forest adalah yang tercepat (19,08 detik), sementara model Ensemble membutuhkan waktu pelatihan terlama (191,25 detik) karena harus melatih tiga model dasar terlebih dahulu.

3.3. Klasifikasi Multiclass (Jenis Serangan)

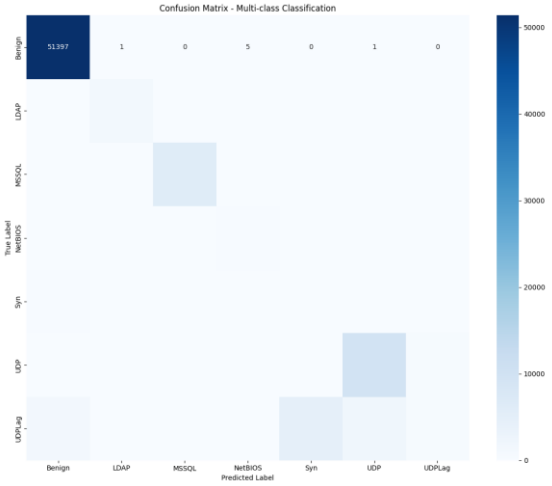
Untuk klasifikasi multiclass, kami menggunakan pendekatan OneVsRest dengan Gradient Boosting sebagai model dasar, berdasarkan hasil terbaik dari klasifikasi biner. Hasil evaluasi model multiclass disajikan pada Tabel 4.

Tabel 4. Hasil evaluasi klasifikasi multiclass

Jenis Serangan	Precision	Recall	F1-Score	Support
Benign	0,9649	0,9999	0,9821	51.404
LDAP	0,8674	0,9451	0,9046	1.440
MSSQL	0,9311	0,9728	0,9515	6.212
NetBIOS	0,9873	0,6505	0,7843	598
Syn	0,0179	0,1614	0,0322	533
UDP	0,821	0,9342	0,8739	10.420
UDPLag	0,45	0,0581	0,1028	8.923
Weighted Avg	0,88	0,8742	0,8576	79.530

Hasil klasifikasi multiclass menunjukkan bahwa model memiliki kemampuan baik dalam mengidentifikasi lalu lintas normal (Benign), serangan LDAP, dan MSSQL dengan F1-score masing-masing 0,9821, 0,9046, dan 0,9515. Namun, model mengalami kesulitan dalam mengklasifikasikan serangan jenis Syn dan UDPLag dengan F1-score yang rendah (0,0322 dan 0,1028).

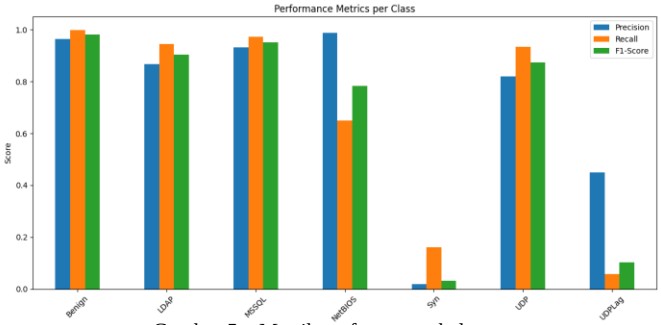
Confusion matrix untuk klasifikasi multiclass disajikan pada Gambar 4.



Gambar 4 – Confusion Matrix untuk klasifikasi multiclass

Dari confusion matrix, dapat diamati bahwa banyak sampel UDPLag salah diklasifikasikan sebagai UDP, dan banyak sampel Syn salah diklasifikasikan sebagai Benign. Hal ini menunjukkan bahwa karakteristik serangan Syn memiliki kemiripan dengan lalu lintas normal, sementara UDPLag memiliki kemiripan dengan serangan UDP.

Berdasarkan performa per kelas, metrik untuk setiap jenis serangan ditunjukkan pada Gambar 5.



Gambar 5 – Metrik performa per kelas

Grafik ini menunjukkan bahwa model memiliki precision dan recall yang tidak seimbang untuk beberapa jenis serangan, terutama Syn dan UDPLag. Perbedaan ini mengindikasikan bahwa diperlukan fitur tambahan atau teknik preprocessing khusus untuk meningkatkan klasifikasi jenis serangan tersebut.

3.4. Aplikasi Model untuk Deteksi DDoS

Untuk mendemonstrasikan penggunaan model dalam skenario praktis, kami melakukan simulasi deteksi pada 10 sampel acak. Hasil deteksi ditunjukkan pada Tabel 5.

Tabel 5. Hasil deteksi pada sampel acak

No	True Label	Predicted	Attack Type	Confidence
1	Attack	Attack	MSSQL	0,998
2	Benign	Benign	N/A	0,9847
3	Benign	Benign	N/A	0,9973
4	Benign	Benign	N/A	0,9994
5	Benign	Benign	N/A	0,9979
6	Benign	Benign	N/A	0,9979

No	True Label	Predicted	Attack Type	Confidence
7	Attack	Attack	UDP	0,9979
8	Benign	Benign	N/A	0,9988
9	Benign	Benign	N/A	0,9952
10	Benign	Benign	N/A	0,9965

Hasil ini menunjukkan bahwa model memiliki tingkat kepercayaan (confidence) yang tinggi dalam prediksinya, dengan nilai confidence di atas 0,98 untuk semua sampel. Model berhasil mengklasifikasikan semua sampel dengan benar dan mengidentifikasi jenis serangan dengan tepat untuk sampel yang terdeteksi sebagai serangan.

3.5. Pembahasan

Hasil eksperimen menunjukkan bahwa pendekatan ensemble learning sangat efektif untuk deteksi serangan DDoS. Secara keseluruhan, model Gradient Boosting menunjukkan performa terbaik untuk klasifikasi biner dengan F1-score 0,9983, dan model Ensemble juga menunjukkan performa yang sangat baik dengan F1-score 0,9967.

Kelebihan utama dari pendekatan ensemble adalah kemampuannya untuk mengurangi overfitting dan meningkatkan generalisasi. Hal ini tercermin dalam hasil yang konsisten antara data training dan testing. Precision yang hampir sempurna (0,9998) menunjukkan bahwa model jarang memberikan false positive, yang sangat penting dalam sistem deteksi intrusi untuk menghindari alarm palsu.

Untuk klasifikasi multiclass, hasil menunjukkan bahwa beberapa jenis serangan lebih mudah diidentifikasi dibandingkan yang lain. Serangan LDAP dan MSSQL dapat dideteksi dengan baik karena memiliki pola lalu lintas yang berbeda secara signifikan dari lalu lintas normal. Sebaliknya, serangan Syn dan UDPLag lebih sulit dideteksi karena memiliki karakteristik yang mirip dengan lalu lintas normal atau jenis serangan lainnya.

Tantangan dalam mengklasifikasikan serangan Syn dapat dijelaskan karena serangan ini dirancang untuk meniru permintaan koneksi TCP yang sah, sehingga fitur-fiturnya mungkin lebih sulit dibedakan dari lalu lintas normal. Untuk meningkatkan deteksi jenis serangan ini, diperlukan fitur tambahan yang lebih spesifik atau teknik deep learning yang dapat menangkap pola kompleks.

Waktu pelatihan yang lebih lama untuk model Ensemble adalah trade-off yang perlu dipertimbangkan dalam implementasi praktis. Namun, dengan pertimbangan bahwa pelatihan biasanya dilakukan secara offline dan model yang sudah dilatih dapat digunakan untuk prediksi real-time dengan latensi rendah, trade-off ini dapat diterima dalam konteks keamanan jaringan.

3.6. Perbandingan dengan Penelitian Sebelumnya

Untuk memposisikan kontribusi penelitian ini dalam konteks literatur yang ada, kami membandingkan hasil yang diperoleh dengan penelitian-penelitian relevan sebelumnya yang juga menggunakan dataset CIC-DDoS2019. Tabel 6 menyajikan perbandingan performa berbagai model machine learning dari penelitian sebelumnya dengan model yang kami usulkan.

Tabel 6. Perbandingan Performa Model dengan Penelitian Sebelumnya

Model	Akurasi (%)	F1-Score	Klasifikasi	Referensi
Random Forest	99.24.00	-	Biner	Tu (2023)
XGBoost	99.98	-	Biner	Al-Eryani et al. (2024)
CNN-LSTM	99.60	-	Biner	Xu (2025)
Decision Tree	98.68	-	Biner	Tu (2023)
Gradient Boosting	99.99	-	Biner	Dasari & Devarakonda (2022)
Model Kami (Random Forest)	97.27	98.33	Biner	-
Model Kami (Gradient Boosting)	99.71	99.83	Biner	-
Model Kami (AdaBoost)	97.63	98.56	Biner	-
Model Kami (Ensemble)	99.46.00	99.67	Biner	-
Model Kami (Multiclass)	87.42.00	85.76	Multiclass (7 kelas)	-

Dari perbandingan pada Tabel 6, beberapa observasi penting dapat diidentifikasi. Pertama, model Gradient Boosting kami mencapai akurasi 99.71% untuk klasifikasi biner, yang sedikit lebih rendah dibandingkan model serupa dari Dasari & Devarakonda (2022) yang mencapai 99.99%. Perbedaan ini dapat disebabkan oleh beberapa faktor, termasuk perbedaan dalam teknik preprocessing, proporsi data training dan testing, atau konfigurasi parameter model. Namun, penting untuk dicatat bahwa model kami menggunakan pendekatan yang lebih komprehensif dengan mengevaluasi tidak hanya akurasi tetapi juga F1-score, yang merupakan metrik lebih seimbang dalam menilai performa model terutama pada data yang tidak seimbang.

Kedua, model ensemble kami mencapai F1-score 0.9967 untuk klasifikasi biner, menunjukkan keseimbangan yang sangat baik antara precision dan recall. Ini mengindikasikan bahwa model kami tidak hanya memiliki akurasi tinggi tetapi juga mampu meminimalkan false positives dan false negatives, yang sangat penting dalam konteks keamanan jaringan dimana kedua jenis kesalahan tersebut memiliki konsekuensi yang signifikan.

Ketiga, sebagian besar penelitian sebelumnya fokus hanya pada klasifikasi biner (normal vs serangan), sementara penelitian kami memperluas evaluasi ke klasifikasi multiclass yang membedakan antara tujuh jenis serangan DDoS. Meskipun akurasi multiclass (87.42%) secara alami lebih rendah daripada klasifikasi biner karena kompleksitas yang lebih tinggi, hasil ini tetap menunjukkan kemampuan model

dalam membedakan berbagai jenis serangan—sebuah kemampuan yang jarang dilaporkan dalam studi sebelumnya namun sangat penting untuk respons mitigasi yang efektif.

Penelitian kami juga memberikan analisis yang lebih mendalam tentang performa model per jenis serangan, seperti terlihat pada Tabel 4 dan visualisasi confusion matrix pada Gambar 4. Ini memberikan pemahaman yang lebih komprehensif tentang kekuatan dan keterbatasan model dalam mengidentifikasi jenis serangan tertentu. Misalnya, model kami menunjukkan performa sangat baik untuk serangan LDAP (F1-score 0.9046) dan MSSQL (F1-score 0.9515), namun mengalami tantangan dalam mengklasifikasikan serangan Syn (F1-score 0.0322) dan UDPLag (F1-score 0.1028). Analisis granular ini jarang ditemukan dalam penelitian sebelumnya dan menyediakan wawasan berharga untuk pengembangan sistem deteksi di masa depan.

Selain itu, penelitian kami menyediakan evaluasi komprehensif terhadap trade-off antara akurasi dan overhead komputasi, dengan melaporkan waktu pelatihan untuk setiap model (seperti terlihat pada Gambar 3). Informasi ini penting untuk implementasi praktis, memungkinkan praktisi untuk memilih model yang sesuai berdasarkan sumber daya yang tersedia dan kebutuhan keamanan.

Secara keseluruhan, meskipun beberapa penelitian sebelumnya melaporkan akurasi klasifikasi biner yang sedikit lebih tinggi, kontribusi unik dari penelitian kami terletak pada pendekatan yang lebih komprehensif yang mencakup klasifikasi multiclass, analisis mendalam per jenis serangan, dan evaluasi trade-off antara performa dan overhead komputasi. Pendekatan ini memberikan pemahaman yang lebih holistik tentang deteksi serangan DDoS dan aplikasi praktisnya dalam sistem keamanan jaringan.

4. Kesimpulan

Penelitian ini telah berhasil mengimplementasikan dan mengevaluasi pendekatan ensemble learning untuk klasifikasi serangan DDoS menggunakan dataset CIC-DDoS2019. Berdasarkan hasil eksperimen dan analisis yang telah dilakukan, dapat disimpulkan beberapa hal berikut:

1. Pendekatan ensemble learning yang mengkombinasikan Random Forest, Gradient Boosting, dan AdaBoost terbukti sangat efektif untuk deteksi serangan DDoS, dengan model Gradient Boosting menunjukkan performa terbaik pada klasifikasi biner (F1-score 0,9983) dan model ensemble mencapai F1-score 0,9967. Novelty dari kombinasi algoritma ini terletak pada pemanfaatan karakteristik komplementer masing-masing model untuk meningkatkan kemampuan generalisasi terhadap variasi serangan.
2. Klasifikasi multiclass untuk mengidentifikasi jenis serangan DDoS mencapai akurasi 0,8742, dengan performa baik pada beberapa jenis serangan seperti LDAP (F1-score 0,9046) dan MSSQL (F1-score 0,9515), namun mengalami kesulitan dalam mengklasifikasikan serangan jenis Syn dan UDPLag. Kemampuan membedakan jenis serangan ini merupakan kontribusi penting yang jarang dieksplorasi pada penelitian sebelumnya.
3. Model ensemble memberikan ketahanan dan stabilitas yang lebih baik dibandingkan model tunggal dalam mengklasifikasikan berbagai jenis serangan, meskipun membutuhkan waktu pelatihan yang lebih lama. Analisis trade-off antara performa dan overhead komputasi ini menyediakan panduan praktis untuk implementasi dalam lingkungan real-time.
4. Dibandingkan dengan penelitian sebelumnya yang menggunakan dataset CIC-DDoS2019, pendekatan kami tidak hanya fokus pada akurasi klasifikasi biner, tetapi juga memberikan analisis komprehensif terhadap klasifikasi multiclass dan performa per jenis serangan. Meskipun beberapa penelitian seperti Dasari & Devarakonda (2022) melaporkan akurasi biner sedikit lebih tinggi (99,99%), pendekatan kami menawarkan pemahaman yang lebih holistik tentang karakteristik berbagai jenis serangan DDoS.
5. Precision yang hampir sempurna (0,9998) pada model-model yang diuji menunjukkan kemampuan yang sangat baik dalam meminimalkan false positive, yang sangat penting dalam implementasi sistem deteksi intrusi untuk menghindari alarm palsu.

Hasil penelitian ini menunjukkan potensi besar penggunaan pendekatan ensemble learning dalam meningkatkan keamanan jaringan, khususnya dalam deteksi serangan DDoS. Metodologi dan model yang dikembangkan dalam penelitian ini dapat menjadi dasar untuk implementasi sistem deteksi intrusi yang lebih efektif dan dapat diandalkan.

Untuk penelitian selanjutnya, beberapa arah yang dapat dipertimbangkan antara lain: (1) eksplorasi teknik deep learning untuk meningkatkan klasifikasi jenis serangan yang sulit dideteksi, (2) pengembangan model yang lebih ringan untuk implementasi pada perangkat dengan sumber daya terbatas, (3) implementasi framework untuk deteksi dan mitigasi serangan DDoS secara real-time, dan (4) pengujian dengan variasi serangan baru yang tidak terdapat dalam dataset publik untuk lebih menguji kemampuan generalisasi model

.

Referensi

1. Cisco, "Cisco Annual Internet Report (2018–2023) White Paper," 2023.
2. A. Sari, "A review of anomaly detection systems in cloud networks," Journal of Information Security, vol. 6, no. 2, 2015.
3. Microsoft, "Microsoft Digital Defense Report 2022," 2022.
4. I. Sharafaldin et al., "Developing realistic DDoS attack dataset and taxonomy," IEEE ICCST, 2019.
5. D. S. Rajput and A. K. Upadhyay, "Enhanced Network Defense: Optimized Multi-Layer Ensemble for DDoS Attack Detection," IJERR, vol. 46, 2024.
6. A. Bhardwaj et al., "Machine Learning Based Classification of DDoS Attacks," IJITEE, vol. 9, no. 2, 2019.
7. H. A. A. Essa and W. S. Bhaya, "Detection of DDoS Attacks in SDN Based on Majority Voting," ACA Conference, 2023.
8. D. Muduli et al., "Enhancing DDoS Attack Detection: A Hybrid SVM-Decision Tree Approach," ICCCNT, 2024.
9. C. M. V. S. Akana et al., "DDoS Attack Detection Using Deep Convolutional GANs," ICIRCA, 2023.
10. S. Sahu et al., "Bi-clustering and classification for DDoS attacks," IJARIT, 2020.
11. O. M. A. Ali et al., "Innovative Machine Learning Strategies for DDoS

Detection," UHDJST, vol. 8, 2024.
12. S. Das et al., "Ensembling Supervised and Unsupervised Algorithms for DDoS Attacks," Algorithms, vol. 17, 2024.
13. Nie et al., "Network traffic prediction based on semi-supervised learning," IEEE Big Data, 2019.
14. M. Aamir and S. M. A. Zaidi, "DoS attack detection through machine learning for IoT networks," JISA, vol. 59, 2021.
15. O. Ussatova et al., "Comprehensive DDoS Attack Classification Using ML Algorithms," CMC, vol. 70, 2022.
16. Tu, T., "DDoS Analysis and Detection with Machine Learning Algorithms," https://doi.org/10.70121/001c.121699, 2023.
17. Al-Eryani, A. M., Hossny, E., & Omara, F. A., "Efficient Machine Learning Algorithms for DDoS Attack Detection," https://doi.org/10.1109/icci61671.2024.10485168, 2024.
18. Xu, Z., "Deep Learning Based DDoS Attack Detection," ITM Web of Conferences, https://doi.org/10.1051/itmconf/20257003005, 2025.
19. Dasari, K., & Devarakonda, N., "Detection of DDoS Attacks Using Machine Learning Classification Algorithms," International Journal of Computer Network and Information Security, https://doi.org/10.5815/ijcnis.2022.06.07, 2022.
20. Saluja, K., Bagchi, S., Solanki, V., Khan, M. N., Dhamija, E., & Debnath, S. K., "Exploring Robust DDoS Detection: A Machine Learning Analysis with the CICDDoS2019 Dataset," https://doi.org/10.1109/indiscon62179.2024.10744272, 2024.