UPGRADE: Jurnal Pendidikan Teknologi Informasi
Volume 3, No. 2, Februari, 2026, (63-76)
E-ISSN: 3021-7076
DOI: https://doi.org/10.30812/upgrade.v3i2.6174

Deteksi Anomali Lalu Lintas Jaringan berbasis Machine Learning Menggunakan Dataset CIC-IDS2017

Nadhir Fachrul Rozam*, Tika Novita Sari, Muhammad Resa Arif Yudianto, Dzul Fadli Rahman
Universitas Negeri Yogyakarta, Yogyakarta, Indonesia
Email Korespondensi: nadhirfachrulrozam@uny.ac.id

Genesis Artikel: **Diterima**: 18 Februari 2026 **Diterbitkan**: 28 Februari 2026

ABSTRACT: *The increasing volume and diversity of traffic in modern networks demand more adaptive intrusion detection approaches than traditional signature-based methods. This study aims to evaluate and compare the performance of several machine learning algorithms in detecting multi-class network traffic anomalies using the CIC-IDS2017 dataset. The research process includes data cleaning and transformation, class imbalance handling through random undersampling, and the implementation of five classification models: Logistic Regression, Gaussian Naïve Bayes, Random Forest, K-Nearest Neighbors, and Support Vector Machine. Model performance is assessed using accuracy, precision, recall, and F1-score, supported by confusion matrix analysis and feature contribution evaluation. The results indicate that Random Forest achieves the best performance with an accuracy of 99.44% and consistently high evaluation metrics, while Gaussian Naïve Bayes shows the lowest performance. Furthermore, flow-based features are found to play a dominant role in improving classification accuracy, while misclassifications mainly occur among classes with similar traffic patterns. The findings highlight that selecting appropriate algorithms and applying effective preprocessing strategies are critical for developing more accurate and adaptive intrusion detection systems capable of addressing evolving cyber threats.*

Keyword: *CIC-IDS2017; Intrusion Detection System; Machine Learning; Network Security; Network Traffic Anomaly.*

ABSTRAK: Peningkatan trafik dan keragaman aktivitas pada jaringan modern menuntut pendekatan deteksi intrusi yang lebih adaptif dibandingkan metode berbasis *signature*. Penelitian ini bertujuan menilai serta membandingkan kinerja sejumlah algoritma *machine learning* dalam mengidentifikasi anomali trafik jaringan secara multi-kelas dengan memanfaatkan dataset CIC-IDS2017. Metode penelitian meliputi pembersihan dan transformasi data, penyeimbangan kelas menggunakan teknik *random undersampling*, serta penerapan lima model klasifikasi, yaitu Logistic Regression, Gaussian Naïve Bayes, Random Forest, K-Nearest Neighbors, dan Support Vector Machine. Evaluasi dilakukan melalui metrik akurasi, presisi, *recall*, dan *F1-score*, dilengkapi dengan analisis *confusion matrix* serta kontribusi fitur terhadap model. Hasil penelitian menunjukkan bahwa Random Forest mencapai performa paling optimal dengan tingkat akurasi 99,44% dan konsistensi nilai evaluasi yang tinggi, sedangkan Gaussian Naïve Bayes menghasilkan performa paling rendah. Selain itu, fitur berbasis aliran terbukti memiliki peran dominan dalam meningkatkan ketepatan klasifikasi, sementara kesalahan umumnya muncul pada kelas dengan pola trafik yang serupa. Implikasi penelitian ini menegaskan bahwa kombinasi pemilihan algoritma yang tepat dan strategi prapemrosesan yang efektif sangat penting dalam mengembangkan sistem deteksi intrusi yang lebih akurat dan adaptif terhadap ancaman siber yang terus berkembang.

Kata Kunci: CIC-IDS2017; Keamanan Jaringan; Machine Learning; Network Traffic Anomali; Sistem Deteksi Intrusi.

Cara Sitasi:
Rozam, N.F., Sari, T.N., Yudianto, M. R. A., Rahman, D.F. (2026). Deteksi Anomali Lalu Lintas Jaringan berbasis Machine Learning Menggunakan Dataset CIC-IDS2017. *UPGRADE: Jurnal Pendidikan Teknologi Informasi, 3*(2), 63-76. https://doi.org/10.30812/upgrade.v3i2.6174

PENDAHULUAN

Perkembangan teknologi jaringan komputer yang semakin pesat telah mendorong peningkatan volume dan kompleksitas lalu lintas jaringan, yang berimplikasi pada kebutuhan keamanan jaringan yang lebih adaptif dan andal (Buczak and Guven, 2016). Transformasi digital di berbagai sektor, termasuk pendidikan, pemerintahan, dan industri, menyebabkan infrastruktur jaringan menjadi semakin terbuka dan rentan terhadap berbagai ancaman keamanan siber (Rios et al., 2022). Salah satu permasalahan utama yang sering muncul adalah anomali lalu lintas jaringan, baik yang disebabkan oleh kesalahan konfigurasi maupun aktivitas serangan seperti Distributed Denial of Service (DDoS) (Nisa et al., 2024; Rios et al., 2022; Rozam and Riasetiawan, 2023). Anomali jaringan yang tidak terdeteksi secara dini dapat berdampak serius terhadap ketersediaan layanan, integritas sistem, dan keamanan data (Isarianto et al., 2025).

Pendekatan konvensional dalam mendeteksi anomali jaringan umumnya menggunakan metode berbasis aturan (*rule-based*) atau *signature-based*, yang efektif untuk serangan yang telah dikenal namun memiliki keterbatasan dalam menghadapi pola serangan baru dan lalu lintas yang dinamis (Aldweesh et al., 2020). Ketergantungan terhadap pembaruan manual dari aturan atau *signature* membuat sistem deteksi menjadi kurang responsif terhadap ancaman baru (Alanazi et al., 2022; Raza et al., 2024). Oleh karena itu, pendekatan berbasis *machine learning* (ML) yang dapat mempelajari pola dari data historis dan mengidentifikasi perilaku yang menyimpang secara otomatis menjadi semakin populer dalam penelitian sistem deteksi intrusi (*intrusion detection systems*) (Bamou et al., 2023). Banyak tinjauan menyatakan bahwa ML memberikan potensi signifikan dalam meningkatkan kemampuan deteksi sambil menurunkan tingkat alarm palsu jika dibandingkan dengan IDS konvensional (Chennoufi et al., 2024; Setitra et al., 2024).

Berbagai penelitian telah mengeksplorasi penggunaan algoritma ML, termasuk Random Forest, Support Vector Machine (SVM), dan K-Nearest Neighbor (KNN) dalam deteksi anomali jaringan (Budiati et al., 2023; Gadze et al., 2021; Nisa et al., 2024), serta pendekatan berbasis *deep learning* yang menunjukkan peningkatan performa dalam mengenali pola serangan kompleks (Liu et al., 2023; Mujiono et al., 2025; Najar and Manohar Naik, 2024). Sebagai contoh, penelitian oleh (Putra et al., 2025). yang menggunakan dataset CIC-IDS2017 menunjukkan bahwa algoritma Random Forest mampu mencapai tingkat akurasi yang lebih tinggi dibandingkan metode klasik lainnya dalam mendeteksi serangan DDoS. Selain itu, (Rosay et al., 2022) mengungkapkan bahwa kombinasi fitur berbasis aliran (*flow-based features*) dan algoritma ML dapat meningkatkan kemampuan klasifikasi multi-kelas pada berbagai jenis serangan jaringan. Temuan-temuan tersebut menunjukkan bahwa pemilihan algoritma dan representasi fitur memiliki peran penting dalam meningkatkan performa sistem deteksi intrusi. Selain itu, pendekatan *feature selection* dan teknik *oversampling* untuk menangani ketidakseimbangan data telah terbukti membantu dalam meningkatkan sensitivitas model serta memaksimalkan metrik evaluasi seperti *recall* dan *F1-score* (Setitra and Fan, 2024).

Dataset publik seperti CIC-IDS2017 telah banyak digunakan sebagai standar benchmark dalam studi ML berbasis deteksi anomali karena menyediakan data lalu lintas realistis yang mencakup berbagai jenis serangan dan karakteristik jaringan modern (Rosay et al., 2022; Sharafaldin et al., 2018). Dataset ini dihasilkan dengan menggunakan *flow-based feature extraction* yang memberikan representasi atribut yang relevan bagi pembelajaran mesin dan evaluasi model. Meskipun dataset tersebut telah dipakai luas, beberapa penelitian sebelumnya cenderung fokus pada penggunaan satu model tertentu atau belum mendalami perbandingan performa beberapa algoritma ML secara sistematis, termasuk interpretasi model dan analisis kesalahan klasifikasi yang relevan untuk implementasi nyata (Rosay et al., 2022; Wang et al., 2024).

Selain tantangan dalam mendeteksi pola serangan yang semakin kompleks, sistem deteksi anomali lalu lintas jaringan juga dihadapkan pada permasalahan ketidakseimbangan data (*imbalanced data*), di mana jumlah trafik normal jauh lebih dominan dibandingkan trafik serangan tertentu. Kondisi ini dapat menyebabkan bias pada proses pembelajaran model dan menurunkan kemampuan sistem dalam mendeteksi serangan dengan frekuensi rendah namun berdampak tinggi. Beberapa penelitian menunjukkan bahwa tanpa penanganan khusus terhadap ketidakseimbangan data, model ML cenderung memiliki nilai

akurasi yang tinggi namun performa yang rendah pada metrik *recall* dan *F1-score* untuk kelas minoritas (Neethu and Ravish Aradhya, 2024). Oleh karena itu, penerapan teknik prapemrosesan data seperti *resampling* dan pemilihan fitur yang relevan menjadi aspek penting dalam meningkatkan kinerja dan reliabilitas sistem deteksi anomali berbasis ML (Putra et al., 2025).

Dengan memanfaatkan dataset CIC-IDS2017 sebagai basis data, penelitian ini bertujuan untuk mengembangkan dan menganalisis model deteksi anomali lalu lintas jaringan berbasis ML secara komparatif. Fokus utama penelitian ini adalah mengevaluasi kinerja beberapa algoritma ML dalam mengklasifikasikan trafik normal dan anomali menggunakan metrik akurasi, presisi, *recall*, dan *F1-score*, serta melakukan analisis korelasi fitur untuk mengetahui karakteristik fitur yang berkontribusi signifikan dalam deteksi. Diharapkan hasil penelitian ini dapat memberikan kontribusi praktis dalam pengembangan sistem deteksi anomali yang lebih efektif dan adaptif serta menjadi referensi bagi penelitian lanjutan di bidang keamanan jaringan komputer.

METODE

Penelitian ini menggunakan pendekatan eksperimen komputasional berbasis ML untuk mendeteksi anomali lalu lintas jaringan. Metode yang diterapkan bertujuan untuk mengevaluasi kinerja beberapa algoritma klasifikasi dalam membedakan trafik normal dan anomali pada skenario multi-kelas secara sistematis. Penelitian diawali dengan pengumpulan data menggunakan dataset CIC-IDS2017 yang berisi lalu lintas jaringan dengan berbagai jenis serangan, yang diklasifikasikan ke dalam beberapa kategori, yaitu *Normal Traffic, DoS, DDoS, Port Scanning, Brute Force, Web Attacks, dan Bots*.

Tahap pra-pemrosesan data dilakukan untuk meningkatkan kualitas data serta memastikan kesesuaiannya dengan algoritma ML sebelum proses pelatihan dan analisis. Proses ini meliputi pembersihan data dengan menghapus *missing values*, data duplikat, serta nilai yang tidak valid untuk mengurangi *noise* dan potensi bias. Selanjutnya, *outlier* pada fitur numerik diidentifikasi berdasarkan distribusi data dan dihapus guna mencegah distorsi nilai ekstrem yang dapat memengaruhi stabilitas model. Transformasi dan penyesuaian label juga dilakukan dengan mengelompokkan data ke dalam kategori *Normal Traffic, DoS, DDoS, Port Scanning, Brute Force, Web Attacks, dan Bots*, sehingga permasalahan diformulasikan sebagai klasifikasi multi-kelas. Untuk mengatasi ketidakseimbangan distribusi kelas, dilakukan penanganan pada data latih guna mengurangi bias terhadap kelas mayoritas dan meningkatkan kemampuan model dalam mengenali kelas minoritas. Selain itu, normalisasi diterapkan pada fitur numerik untuk menyamakan skala antar fitur, khususnya pada algoritma berbasis jarak dan margin. Tahap akhir adalah pembagian dataset menjadi data latih dan data uji menggunakan skema *train-test split* guna memastikan evaluasi model dilakukan secara objektif dan tidak bias.

Tahap selanjutnya adalah penerapan model dengan menggunakan beberapa algoritma ML untuk melakukan klasifikasi multi-kelas pada lalu lintas jaringan. Pemilihan algoritma didasarkan pada perbedaan karakteristik pendekatan, sehingga memungkinkan perbandingan kinerja yang objektif. Algoritma yang digunakan meliputi:

1. Logistic Regression
   Logistic Regression merupakan algoritma klasifikasi linier yang memodelkan hubungan antara fitur input dan probabilitas suatu kelas menggunakan fungsi logistik. Pada klasifikasi multi-kelas, Logistic Regression diimplementasikan menggunakan pendekatan *multinomial logistic regression*, di mana probabilitas setiap kelas dihitung secara simultan.Fungsi probabilitas Logistic Regression dinyatakan seperti pada Persamaan 1; dengan x merupakan vektor fitur, w_k dan b_k adalah parameter model untuk kelas ke-k, serta K adalah jumlah kelas. Algoritma ini digunakan sebagai *baseline model* untuk mengevaluasi kemampuan model linier dalam mengklasifikasikan pola lalu lintas jaringan.

$$P(y = k|x) = \frac{e^{w}k^{Tx} + b_k}{\sum_{j=1}^{K} e^{w}j^{Tx} + b_j} \tag{1}$$

2. Naive Bayes
Naive Bayes merupakan algoritma klasifikasi probabilistik yang didasarkan pada Teorema Bayes dengan asumsi independensi antar fitur. Probabilitas suatu kelas dihitung berdasarkan probabilitas bersyarat setiap fitur terhadap kelas tersebut. Teorema Bayes dinyatakan seperti pada Persamaan 2; dengan C_k merupakan kelas ke-k. Asumsi independensi fitur menyebabkan probabilitas bersyarat $P(x|C_k)$ dapat dihitung sebagai hasil perkalian probabilitas masing-masing fitur. Naive Bayes dipilih karena memiliki kompleksitas komputasi yang rendah dan mampu memberikan hasil yang cukup baik pada dataset berdimensi tinggi.

$$P(C_k|x) = \frac{P(x|C_k)P(C_k)}{P(x)} \tag{2}$$

3. Random Forest
Random Forest merupakan algoritma *ensemble learning* yang membangun sejumlah pohon keputusan (*decision trees*) secara acak dan menggabungkan hasil prediksi masing-masing pohon melalui mekanisme pemungutan suara (*majority voting*). Setiap pohon dibangun menggunakan subset data dan subset fitur yang dipilih secara acak. Prediksi akhir Random Forest dinyatakan seperti pada Persamaan 3; dengan h_t (x) merupakan prediksi pohon ke-t dan Tadalah jumlah pohon. Pendekatan ini mampu meningkatkan akurasi dan mengurangi risiko *overfitting*, sehingga cocok untuk menangani data lalu lintas jaringan yang kompleks dan berdimensi tinggi.

$$\hat{y} = modeh_1(x), h_2(x), \ldots, h_T(x) \tag{3}$$

4. k-Nearest Neighbor (k-NN)
k-NN digunakan sebagai algoritma k-Nearest Neighbor merupakan algoritma klasifikasi berbasis jarak yang mengklasifikasikan data uji berdasarkan mayoritas kelas dari kdata latih terdekat. Kedekatan antar data dihitung menggunakan fungsi jarak tertentu, umumnya jarak Euclidean. Rumus jarak Euclidean dinyatakan seperti pada Persamaan 4; dengan x merupakan data uji dan x_i merupakan data latih. Algoritma k-NN digunakan untuk menganalisis kemiripan pola lalu lintas jaringan berdasarkan kedekatan fitur dalam ruang multidimensi.

$$d(x, x_i) = \sqrt{\sum_{j=1}^{n}(x_j - xij^2)} \tag{4}$$

5. Support Vector Machine (SVM) SVM merupakan algoritma klasifikasi berbasis margin yang bertujuan untuk menemukan *hyperplane* optimal guna memaksimalkan jarak antar kelas. Pada skenario multi-kelas, SVM diimplementasikan menggunakan pendekatan *one-vs-rest* atau *one-vs-one*. Proses pelatihan dilakukan dengan mengoptimalkan fungsi objektif untuk memaksimalkan margin sekaligus meminimalkan kesalahan klasifikasi. Dalam penelitian ini, digunakan kernel linear karena sesuai untuk data yang relatif dapat dipisahkan secara linear serta memiliki efisiensi komputasi yang lebih baik seperti pada persamaan 5. Seluruh algoritma dilatih menggunakan data latih yang sama dan dievaluasi pada data uji yang identik untuk memastikan perbandingan kinerja yang objektif dan adil.

$$f(x) = w^{Tx} + b \tag{5}$$

Tahap terakhir dalam penelitian ini adalah evaluasi kinerja model untuk menilai kemampuan masing-masing algoritma ML dalam melakukan klasifikasi multi-kelas terhadap lalu lintas jaringan berdasarkan hasil prediksi pada data uji. Evaluasi dilakukan menggunakan metrik *accuracy*, *precision*, *recall*, dan F1-score. *Accuracy* digunakan untuk mengukur proporsi prediksi yang benar secara keseluruhan sebagaimana ditunjukkan pada persamaan 6. *Precision* menunjukkan tingkat

ketepatan model dalam mengklasifikasikan suatu kelas ditunjukan pada persamaan 7, sedangkan *recall* mengukur kemampuan model dalam mengenali seluruh data pada kelas tertentu ditunjukkan pada persamaan 8. Sementara itu, *F1-score* digunakan sebagai ukuran keseimbangan antara *precision* dan *recall* ditunjukan pada persamaan 9. Penggunaan keempat metrik ini bertujuan untuk memberikan evaluasi yang komprehensif terhadap performa model dalam klasifikasi multi-kelas.

$$Accuracy = \frac{\sum_{i=1}^{K} TP_i}{N} \tag{6}$$

$$Precision_i = \frac{TP_i}{TP_i + FP_i} \tag{7}$$

$$Recall_i = \frac{TP_i}{TP_i + FN_i} \tag{8}$$

$$F1_i = 2 \times \frac{Precision_i \times Recall_i}{Precision_i + Recall_i} \tag{9}$$

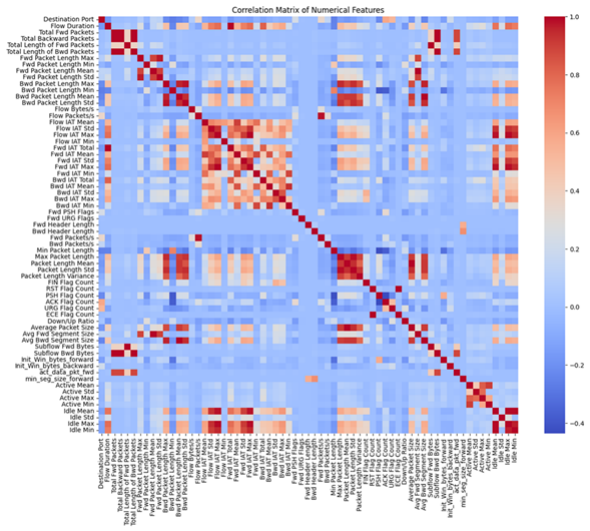
HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil eksperimen dari proses analisis dan pemodelan data lalu lintas jaringan menggunakan algoritma ML. Hasil yang diperoleh meliputi karakteristik dataset, distribusi kelas sebelum dan sesudah pra-pemrosesan, serta evaluasi kinerja model klasifikasi multi-kelas. Hasil tersebut kemudian dianalisis untuk mengidentifikasi pengaruh pra-pemrosesan data dan karakteristik algoritma terhadap performa deteksi anomali.

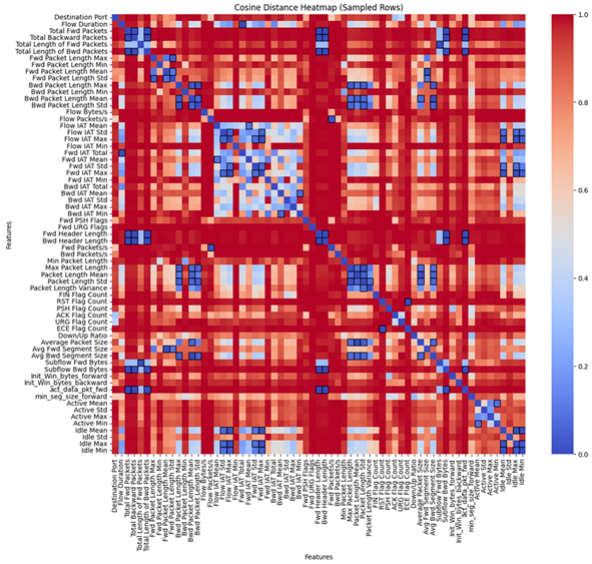
Dataset CIC-IDS2017 yang digunakan terdiri dari 78 fitur numerik dan satu kolom label yang merepresentasikan karakteristik lalu lintas jaringan berbasis flow. Fitur-fitur tersebut mencakup informasi statistik terkait paket, waktu, ukuran, serta *flag* protokol, yang digunakan sebagai variabel independen dalam proses klasifikasi, sedangkan label digunakan sebagai variabel dependen. Secara umum, fitur dalam dataset dapat dikelompokkan ke dalam beberapa kategori utama, yaitu fitur berbasis paket, waktu (*inter-arrival time*), laju (*rate-based*), flag TCP, serta aktivitas dan *idle*. Pengelompokan ini menunjukkan bahwa dataset memiliki representasi yang komprehensif terhadap pola lalu lintas jaringan, sehingga mendukung proses deteksi anomali secara lebih efektif.

Visualisasi korelasi antarfitur pada Gambar 1 menunjukkan adanya hubungan linier antar variabel numerik dalam dataset. Beberapa fitur memiliki tingkat korelasi yang tinggi, terutama pada kelompok fitur sejenis seperti *flow-based features* (Flow IAT, Fwd IAT, dan Bwd IAT) serta fitur panjang paket. Hal ini mengindikasikan adanya redundansi informasi yang berpotensi memengaruhi kinerja model, khususnya pada algoritma yang sensitif terhadap multikolinearitas seperti Logistic Regression. Namun, sebagian besar fitur lainnya menunjukkan korelasi yang rendah, yang mencerminkan keragaman informasi dalam dataset. Dengan demikian, analisis ini memberikan gambaran awal mengenai struktur data dan hubungan antar fitur sebelum proses pemodelan dilakukan.

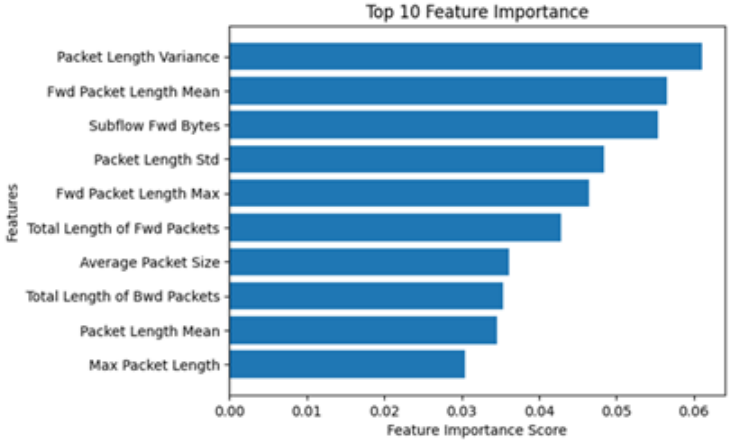
Gambar 2 menampilkan *cosine distance heatmap* yang digunakan untuk mengukur tingkat kemiripan antar fitur dalam ruang vektor. Hasil visualisasi menunjukkan bahwa sebagian besar fitur memiliki tingkat kemiripan yang tinggi, ditandai dengan dominasi warna merah, yang mengindikasikan adanya kesamaan karakteristik dalam merepresentasikan pola lalu lintas jaringan. Namun, terdapat beberapa fitur dengan tingkat kemiripan yang lebih rendah, yang menunjukkan adanya informasi unik yang berpotensi meningkatkan kemampuan model dalam membedakan kelas. Analisis ini memberikan gambaran mengenai struktur dan kedekatan antar fitur serta mendukung pemahaman terhadap kompleksitas data dalam proses klasifikasi.



Gambar 1. Visualisasi korelasi antar fitur



Gambar 2. Tingkat kemiripan antar fitur

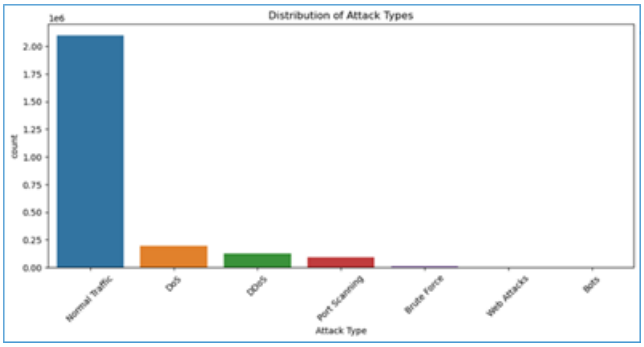


Gambar 3. Analisis feature importance

Analisis *feature importance* dilakukan untuk mengidentifikasi fitur yang paling berkontribusi dalam proses klasifikasi menggunakan model Random Forest. Berdasarkan Gambar 3, fitur Packet Length Variance memiliki nilai kepentingan tertinggi, diikuti oleh Fwd Packet Length Mean dan Subflow Fwd Bytes, yang menunjukkan bahwa karakteristik terkait variasi dan ukuran paket berperan dominan dalam membedakan lalu lintas normal dan serangan. Selain itu, fitur seperti Packet Length Std, Fwd Packet Length Max, dan Total Length of Fwd Packets juga memberikan kontribusi yang signifikan. Dominasi fitur berbasis ukuran paket dan aliran (*flow-based features*) mengindikasikan bahwa pola distribusi dan volume data dalam koneksi jaringan menjadi indikator penting dalam deteksi anomali. Secara keseluruhan, hasil ini menunjukkan bahwa kontribusi fitur tidak merata, sehingga pemilihan fitur yang relevan berpotensi meningkatkan efisiensi dan kinerja model.

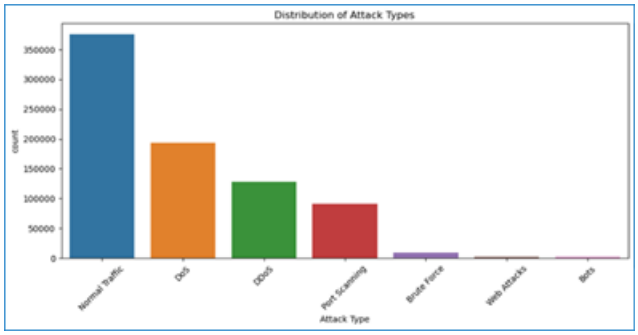
Pada tahap awal, dataset memiliki berbagai label serangan dengan tingkat granularitas yang tinggi. Untuk menyederhanakan skema klasifikasi dan mendukung pendekatan multi-kelas, dilakukan pemetaan label serangan ke dalam beberapa kategori utama sebagaimana ditunjukkan pada proses *group mapping*. Melalui proses pemetaan tersebut, lalu lintas jaringan dikelompokkan ke dalam tujuh kelas utama, yaitu *Normal Traffic, DoS, DDoS, Port Scanning, Brute Force, Web Attacks, dan Bots*. Beberapa kelas seperti *Infiltration* dihapus dari dataset karena jumlah data yang sangat kecil sehingga tidak signifikan secara statistik dan berpotensi menimbulkan bias pada proses pelatihan model.

Setelah dilakukan proses penyaringan kelas, distribusi data yang digunakan dalam penelitian ini menunjukkan ketidakseimbangan yang cukup signifikan antar kelas. Kelas *Normal Traffic* memiliki jumlah data paling besar, yaitu sebanyak 2.095.057 data, diikuti oleh kelas DoS sebanyak 193.745 data dan DDoS sebanyak 128.014 data. Selanjutnya, kelas *Port Scanning* terdiri dari 90.694 data, sementara kelas Brute Force berjumlah 9.150 data. Adapun kelas dengan jumlah data paling sedikit adalah *Web Attacks* dan *Bots*, masing-masing sebanyak 2.143 dan 1.948 data. Distribusi tersebut menunjukkan adanya ketidakseimbangan kelas yang sangat signifikan, dengan dominasi kelas *Normal Traffic* dibandingkan kelas serangan lainnya. Sebagai gambaran distribusi data dapat dilihat pada Gambar 4.



Gambar 4. Distribusi jumlah data pada setiap kelas dataset

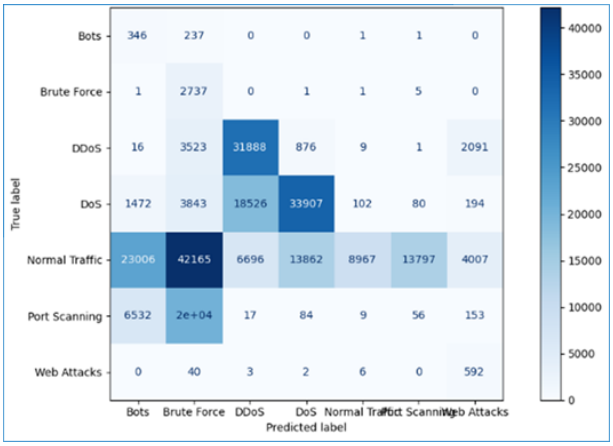
Selain itu, dilakukan pembersihan data dengan menghapus baris yang mengandung nilai negatif pada fitur numerik guna memastikan validitas data, di mana dari total 2.520.751 baris, sebanyak 2.910 baris dihapus sehingga tersisa 2.517.841 baris, tanpa memengaruhi distribusi data secara signifikan. Selanjutnya, untuk mengatasi ketidakseimbangan kelas, diterapkan teknik *random undersampling* pada kelas mayoritas, yaitu dengan mengurangi jumlah data *Normal Traffic* menjadi 375.000 data, sementara seluruh data pada kelas serangan tetap dipertahankan. Data hasil undersampling kemudian digabungkan dan diacak kembali untuk memperoleh distribusi yang lebih representatif. Setelah proses penyeimbangan, dataset akhir berjumlah 800.694 data dengan distribusi sebagai berikut: *Normal Traffic* sebanyak 375.000 data, DoS sebanyak 193.745 data, DDoS sebanyak 128.014 data, *Port Scanning* sebanyak 90.694 data, Brute Force sebanyak 9.150 data, *Web Attacks* sebanyak 2.143 data, dan Bots sebanyak 1.948 data, sehingga distribusi antar kelas menjadi lebih proporsional untuk mendukung proses pelatihan model klasifikasi.



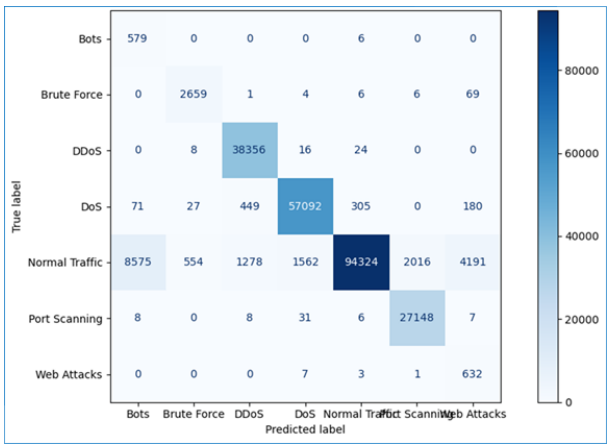
Gambar 5. Distribusi kelas setelah pra-pemrosesan

Visualisasi distribusi kelas setelah pra-pemrosesan pada Gambar5 menunjukkan bahwa dominasi kelas *Normal Traffic* telah berkurang secara signifikan. Kondisi ini menyebabkan distribusi data menjadi lebih seimbang antar kelas, sehingga tidak terjadi dominasi yang berlebihan dari kelas mayoritas. Dengan demikian, model klasifikasi memiliki peluang yang lebih baik untuk mempelajari pola dari setiap kelas serangan secara lebih optimal.

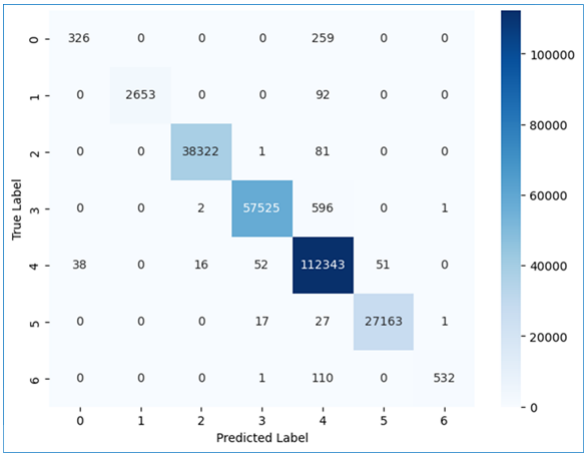
Tahap selanjutnya adalah pengujian model menggunakan beberapa algoritma ML, yaitu Logistic Regression, Gaussian Naïve Bayes, Random Forest, KNN, dan SVM. Pengujian dilakukan menggunakan data uji yang telah dipisahkan pada tahap pra-pemrosesan untuk mengevaluasi kemampuan masing-masing model dalam melakukan klasifikasi multi-kelas terhadap lalu lintas jaringan yang ditunjukkan pada Gambar 6, 7, 8, 9, 10.



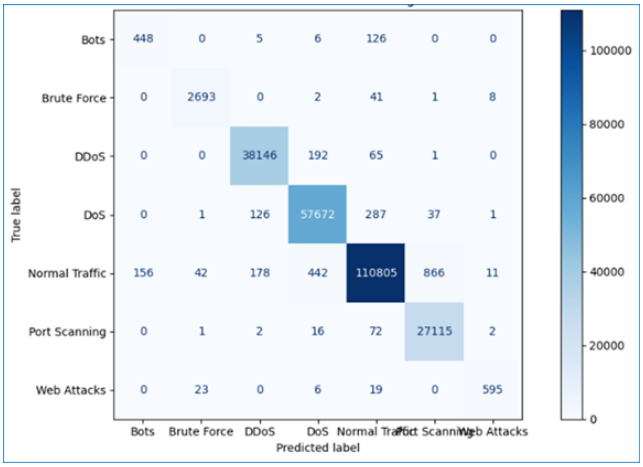
Gambar 6. Confusion matrix naive bayes



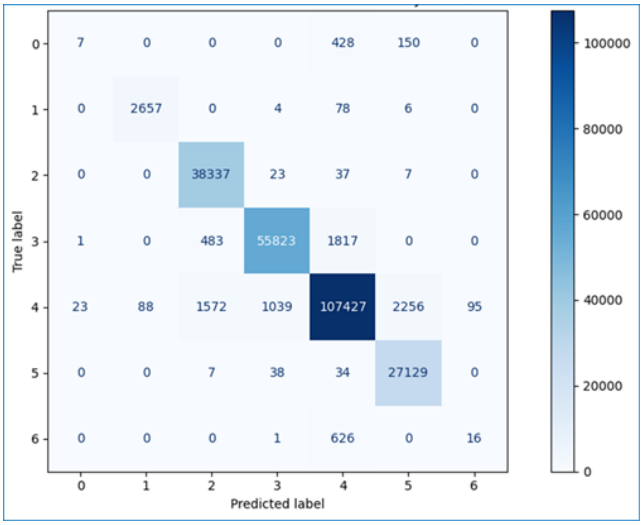
Gambar 7. Confusion matrix logistic regression



Gambar 8. Confusion matrix random forests



Gambar 9. Confusion matrix KNN



Gambar 10. Confusion matrix SVM

Gambar 6 menampilkan *confusion matrix* hasil pengujian model Gaussian Naïve Bayes yang mampu mengklasifikasikan kelas seperti DDoS dan DoS dengan baik, namun masih memiliki kesalahan pada kelas *Normal Traffic* serta performa rendah pada kelas minoritas seperti *Web Attacks* dan *Bots*;

Gambar 7 menunjukkan hasil Logistic Regression yang memiliki performa cukup stabil pada kelas utama seperti DDoS, DoS, dan *Port Scanning*, meskipun masih terdapat kesalahan pada kelas dengan pola yang saling tumpang tindih; Gambar 8 memperlihatkan hasil Random Forest yang memberikan performa terbaik dengan dominasi nilai diagonal di hampir seluruh kelas, menandakan akurasi dan stabilitas yang tinggi; Gambar 9 menampilkan hasil KNN yang mampu mengenali pola utama data dengan cukup baik, namun masih mengalami kesalahan pada kelas dengan karakteristik mirip dan kelas minoritas; sedangkan Gambar 10 menunjukkan hasil SVM yang memiliki performa cukup baik, tetapi masih mengalami kesalahan klasifikasi yang cukup signifikan, terutama pada kelas *Normal Traffic*. Secara keseluruhan, Random Forest menjadi model dengan performa paling optimal dalam klasifikasi multi-kelas lalu lintas jaringan.

Tahap selanjutnya adalah evaluasi kinerja masing-masing algoritma menggunakan metrik *accuracy*, *precision*, *recall*, dan *F1-score*. Evaluasi ini bertujuan untuk mengukur kemampuan model dalam mengklasifikasikan lalu lintas jaringan ke dalam beberapa kelas secara akurat dan konsisten. Hasil pengujian dari setiap model kemudian dirangkum dalam bentuk tabel untuk memudahkan perbandingan performa antar algoritma yang digunakan dalam penelitian ini yang ditunjukan pada Tabel 1.

Tabel 1. Ringkasan Kinerja Model Klasifikasi

Model	***Accuracy***
Logistic Regression	0.9192
Gaussian Naive Bayes	0.3300
Random Forest	**0.9944**
KNN	0.9887
SVM	0.9569

Hasil pengujian model menunjukkan bahwa Random Forest memberikan performa terbaik dengan nilai *accuracy* sebesar 0,9944 serta *precision*, *recall*, dan *F1-score* masing-masing sebesar 0,99. Kinerja ini menunjukkan kemampuan model yang sangat tinggi dalam mengklasifikasikan seluruh kelas secara akurat dan konsisten. Model KNN juga menunjukkan performa yang sangat baik dengan *accuracy* 0,9887 dan nilai *precision*, *recall*, serta *F1-score* yang sama-sama mencapai 0,99. Selanjutnya, SVM memperoleh hasil yang cukup baik dengan *accuracy* 0,9569 serta keseimbangan metrik evaluasi yang relatif tinggi. Logistic Regression menunjukkan performa yang cukup stabil dengan *accuracy* 0,9192 dan *F1-score* sebesar 0,94, meskipun masih berada di bawah model berbasis *ensemble* dan jarak. Sementara itu, Gaussian Naïve Bayes memiliki performa paling rendah dengan *accuracy* sebesar 0,3300 dan nilai *recall* serta *F1-score* yang juga rendah, yang mengindikasikan keterbatasan model dalam menangkap kompleksitas pola data. Secara keseluruhan, model berbasis *ensemble* seperti Random Forest terbukti lebih unggul dibandingkan algoritma lainnya dalam klasifikasi multi-kelas pada lalu lintas jaringan. Hasil penelitian ini sejalan dengan temuan penelitian sebelumnya yang melaporkan bahwa Random Forest merupakan salah satu algoritma yang paling efektif untuk klasifikasi serangan jaringan pada dataset CIC-IDS2017. (Mujiono et al., 2025) menunjukkan bahwa Random Forest mampu mencapai tingkat akurasi yang lebih tinggi dibandingkan KKN pada skenario deteksi intrusi jaringan. Selain itu, penelitian oleh (Putra et al., 2025) melaporkan bahwa kombinasi Random Forest dengan strategi penyeimbangan data dapat meningkatkan performa deteksi serangan, khususnya pada kelas minoritas.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa penerapan teknik ML mampu digunakan secara efektif untuk mendeteksi anomali lalu lintas jaringan dalam skenario klasifikasi multi-kelas. Tahap pra-pemrosesan data, yang meliputi pembersihan data, transformasi label, serta penanganan ketidakseimbangan kelas, berperan penting dalam meningkatkan kualitas data dan kinerja model. Hasil pengujian menunjukkan bahwa algoritma Random Forest memberikan performa terbaik dengan nilai *accuracy* sebesar 0,9944 serta *precision*, *recall*, dan *F1-score* masing-masing sebesar 0,99, yang menunjukkan kemampuan model dalam mengklasifikasikan data secara sangat akurat dan

Dipublikasi oleh Universitas Bumigora

konsisten. Model KNN dan SVM juga menunjukkan kinerja yang baik, sementara Logistic Regression memiliki performa yang cukup stabil namun masih terbatas dalam menangani pola yang kompleks. Di sisi lain, Gaussian Naïve Bayes menunjukkan performa terendah akibat keterbatasan dalam menangkap hubungan antar fitur. Dengan demikian, dapat disimpulkan bahwa model berbasis *ensemble* seperti Random Forest lebih unggul dalam menangani kompleksitas data lalu lintas jaringan dibandingkan algoritma lainnya. Hasil penelitian ini mengindikasikan bahwa ketepatan dalam pemilihan algoritma, yang didukung oleh strategi prapemrosesan data yang optimal, memiliki pengaruh signifikan terhadap performa sistem deteksi intrusi berbasis ML. Dengan demikian, temuan ini memberikan kontribusi penting sebagai dasar pengembangan sistem keamanan jaringan yang lebih *robust*, adaptif, dan responsif terhadap dinamika ancaman siber. Adapun untuk penelitian selanjutnya disarankan untuk dilakukan penanganan data tidak seimbang dengan berbagai metode untuk meningkatkan kinerja model ML.

DEKLARASI

Taksonomi Peran Kontributor

Semua penulis berkontribusi sama sebagai kontributor utama dari makalah ini. Semua penulis membaca dan menyetujui makalah akhir

Pernyataan Pendanaan

Penelitian ini tidak menerima hibah khusus dari lembaga pendanaan di sektor publik, komersial, atau nirlaba

Kepentingan Bersaing

Penulis menyatakan bahwa tidak terdapat konflik kepentingan, baik keuangan maupun non-keuangan, yang dapat mempengaruhi atau dianggap mempengaruhi hasil penelitian dan penulisan artikel ini.

Informasi Tambahan

Tuliskan informasi tambahan jika diperlukan.

DAFTAR PUSTAKA

Alanazi, F., Jambi, K., Eassa, F., Khemakhem, M., Basuhail, A., and Alsubhi, K. (2022). Ensemble Deep Learning Models for Mitigating DDoS Attack in Software-Defined Network. *Intelligent Automation and Soft Computing*, 33(2):923–938. https://doi.org/10.32604/iasc.2022.024668.

Aldweesh, A., Derhab, A., and Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189:105124. https://doi.org/10.1016/j.knosys.2019.105124.

Bamou, A., Driss, M., Ouadghiri, E., Aghoutane, B., and Maada, L. (2023). IDS Based on Machine Learning in Reaction to IoT Attacks: Review and Empirical Evaluation. 13(2).

Buczak, A. L. and Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys and Tutorials*, 18(2):1153–1176. https://doi.org/10.1109/COMST.2015.2494502.

Budiati, H., Himamunanto, A. R., and Bolo, N. T. (2023). Identifikasi Pola Obyek Kain Tenun Sumba dengan Menggunakan Metode K-Nearest Neighbor (KNN). *UPGRADE : Jurnal Pendidikan Teknologi Informasi*, 1(1):1–8. https://doi.org/10.30812/upgrade.v1i1.3149.

Chennoufi, S., Blanc, G., Jmila, H., and Kiennert, C. (2024). SoK: Federated Learning based Network Intrusion Detection in 5G: Context, State of the Art and Challenges. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3664476.3664500.

Gadze, J. D., Bamfo-Asante, A. A., Agyemang, J. O., Nunoo-Mensah, H., and Opare, K. A. B. (2021). An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers. *Technologies*, 9(1). https://doi.org/10.3390/technologies9010014.

Isarianto, I., Turmudi Zy, A., Maulana, D., and Susilo, A. (2025). Analisis Efektivitas Sistem Deteksi Intrusi Terhadap Serangan Ddos: Investigasi Berbasis Simulasi. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 9(4):6983–6987. https://doi.org/10.36040/jati.v9i4.14359.

Liu, Z., Wang, Y., Feng, F., Liu, Y., Li, Z., and Shan, Y. (2023). A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks. *Sensors*, 23(13). https://doi.org/10.3390/s23136176.

Mujiono, M., Larasati, D. A., Hemansyah, M., and Fatimatuzzahra, F. (2025). Deteksi Anomali dalam Sistem Keamanan Jaringan Menggunakan Teknik Supervised Machine Learning. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi dan Sistem Komputer*, 9(1):65–69. https://doi.org/10.55886/infokom.v9i1.971.

Najar, A. A. and Manohar Naik, S. (2024). Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS attacks. *Computers & Security*, 139:103716. https://doi.org/10.1016/J.COSE.2024.103716.

Neethu, S. and Ravish Aradhya, H. V. (2024). Evaluation of distributed denial of service attacks detection in software defined networks. *IAES International Journal of Artificial Intelligence*, 13(4):4488–4498. https://doi.org/10.11591/ijai.v13.i4.pp4488-4498.

Nisa, N., Khan, A. S., Ahmad, Z., and Abdullah, J. (2024). TPAAD: Two-phase authentication system for denial of service attack detection and mitigation using machine learning in software-defined network. *International Journal of Network Management*, 34(3). https://doi.org/10.1002/nem.2258.

Putra, D. K., Pradana, C. A., Gilardin, M. H., and Riyandi, A. (2025). Comparative Analysis of Machine Learning Algorithms in Detecting DDoS Attacks on CICIDS2017 Dataset. *Journal of Intelligent Systems and Information Technology*, 2(2). https://doi.org/10.61971/jisit.v2i2.182.

Raza, M. S., Sheikh, M. N. A., Hwang, I. S., and Ab-Rahman, M. S. (2024). Feature-Selection-Based DDoS Attack Detection Using AI Algorithms. *Telecom*, 5(2):333–346. https://doi.org/10.3390/telecom5020017.

Rios, V. D. M., Inacio, P. R. M., Magoni, D., and Freire, M. M. (2022). Detection and Mitigation of Low-Rate Denial-of-Service Attacks: A Survey. *IEEE Access*, 10(July):76648–76668. https://doi.org/10.1109/ACCESS.2022.3191430.

Rosay, A., Cheval, E., Carlier, F., and Leroux, P. (2022). Network Intrusion Detection: A Comprehensive Analysis of CIC-IDS2017. In *Proceedings of the 8th International Conference on Information Systems Security and Privacy*, volume 9, pages 25–36. SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0010774000003120.

Rozam, N. F. and Riasetiawan, M. (2023). XGBoost Classifier for DDOS Attack Detection in Software Defined Network Using sFlow Protocol. *International Journal on Advanced Science, Engineering and Information Technology*, 13(2):718–725. https://doi.org/10.18517/ijaseit.13.2.17810.

Setitra, M. A. and Fan, M. (2024). Detection of DDoS attacks in SDN-based VANET using optimized TabNet. *Computer Standards and Interfaces*, 90. https://doi.org/10.1016/j.csi.2024.103845.

Setitra, M. A., Fan, M., Benkhaddra, I., and Bensalem, Z. E. A. (2024). DoS/DDoS attacks in Software Defined Networks: Current situation, challenges and future directions. *Computer Communications*, 222:77–96. https://doi.org/10.1016/J.COMCOM.2024.04.035.

Sharafaldin, I., Lashkari, A. H., and Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. https://doi.org/10.5220/0006639801080116.

Wang, Z., Li, J., Yang, S., Luo, X., Li, D., and Mahmoodi, S. (2024). A lightweight IoT intrusion detection model based on improved BERT-of-Theseus. *Expert Systems with Applications*, 238:122045. https://doi.org/10.1016/J.ESWA.2023.122045.

[This page is intentionally left blank.]