JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9380
Hal 1049-1058
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Eksplorasi Teknik Pre-Processing Berbasis eXtreme Gradient Boosting (XGBoost) pada Serangan DDoS

Muhammad Nur Faiz[1,*], Laura Sari[2], Imam Riadi[3] , Arif Wirawan Muhammad[4], Sukma Aji[5]

[1] Jurusan Komputer dan Bisnis, Program Studi Rekayasa Keamanan Siber, Politeknik Negeri Cilacap, Cilacap, Indonesia
[2] Jurusan Komputer dan Bisnis, Program Studi Teknik Informatika, Politeknik Negeri Cilacap, Cilacap, Indonesia
[3] Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[4] Fakultas Informatika, Program Studi Informatika, Universitas Telkom, Purwokerto, Indonesia
[5] Fakultas Sains dan Teknologi, Program Studi Informatika, Universitas Muhammadiyah, Sidoarjo, Indonesia
Email: [1,*]faiz@pnc.ac.id, [2] laurasari@pnc.ac.id, [3]imam.riadi@is.uad.ac.id, [4]arifnm@telkomuniversity.ac.id, [5]sukmaaji@umsida.ac.id
Email Penulis Korespondensi: faiz@pnc.ac.id
Submitted **26-11-2025;** Accepted **29-12-2025;** Published **31-12-2025**

Abstrak

Serangan Distributed Denial of Service (DDoS) merupakan ancaman serius dalam keamanan jaringan modern, khususnya pada lingkungan Internet of Things (IoT) yang memiliki karakteristik trafik besar dan heterogen. Tantangan utama dalam proses deteksi serangan ini terletak pada ketidakseimbangan distribusi data (class imbalance), keberadaan fitur tidak relevan, dan noise yang dapat menurunkan akurasi model deteksi. Penelitian ini mengevaluasi pengaruh rangkaian pre-processing yang meliputi Synthetic Minority Over-sampling Technique (SMOTE), seleksi fitur berbasis korelasi, dan metode seleksi fitur lanjutan terhadap performa algoritma XGBoost dalam mendeteksi serangan Distributed Denial of Service (DDoS) pada dataset CIC-IoT2023. Hasil pengujian menunjukkan bahwa model XGBoost yang dilatih menggunakan data RAW memberikan performa sangat tinggi dengan akurasi 0,999983, precision 0,985531, recall 0,961390, dan F1-score 0,999983. Namun, setelah diterapkan pre-processing, seluruh metrik mengalami penurunan, dengan akurasi 0,958899, precision 0,865729, recall 0,748332, dan F1-score 0,959158. Penurunan recall menunjukkan bertambahnya serangan yang tidak terdeteksi, sementara turunnya precision menandakan peningkatan false alarms. Meskipun demikian, nilai F1-score yang masih berada di atas 0,95 mengindikasikan bahwa model tetap mampu bekerja secara efektif. Temuan ini mengungkap bahwa penerapan pre-processing tidak selalu menghasilkan peningkatan performa, terutama ketika data awal sudah bersih dan relatif seimbang. Penelitian ini memberikan pemahaman lebih dalam mengenai bagaimana SMOTE, seleksi fitur, dan noise injection memengaruhi generalisasi model XGBoost pada trafik IoT, serta menegaskan bahwa efektivitas pre-processing sangat bergantung pada karakteristik dataset dan konteks implementasi sistem deteksi intrusi.

Kata Kunci: DDoS; CIC-IoT2023; XGBoost; Pre-processing; Seleksi Fitur; SMOTE;

Abstract

Distributed Denial of Service (DDoS) attacks represent a critical threat to modern network security, particularly within Internet of Things (IoT) environments characterized by large-scale and heterogeneous traffic patterns. The primary challenges in detecting such attacks involve class imbalance, irrelevant features, and noise within the data, all of which can degrade the performance of machine learning-based detection models. This study evaluates the impact of a pre-processing pipeline—comprising the Synthetic Minority Over-sampling Technique (SMOTE), correlation-based feature selection, and advanced feature selection methods—on the performance of the XGBoost algorithm in detecting DDoS attacks using the CIC-IoT2023 dataset. Experimental results indicate that the XGBoost model trained on RAW data achieves exceptionally high performance, with an accuracy of 0.999983, precision of 0.985531, recall of 0.961390, and an F1-score of 0.999983. However, after applying the pre-processing techniques, all metrics experienced a decline, with accuracy decreasing to 0.958899, precision to 0.865729, recall to 0.748332, and the F1-score to 0.959158. The reduction in recall suggests a higher number of undetected attacks, whereas the drop in precision indicates an increase in false alarms. Nevertheless, the F1-score remaining above 0.95 demonstrates that the model continues to perform effectively overall. These findings reveal that pre-processing does not always lead to performance improvements, especially when the raw dataset is already relatively clean and balanced. This study provides deeper insights into how SMOTE, feature selection, and noise injection influence the generalization of XGBoost on IoT traffic, and emphasizes that the effectiveness of pre-processing is highly dependent on dataset characteristics and the intended application context of intrusion detection systems.

Keywords: DdoS; CIC-IoT2023; XGBoost; Pre-processing, Feature Selection; SMOTE;

1. PENDAHULUAN

Dalam beberapa tahun terakhir, frekuensi dan kompleksitas serangan siber terus mengalami peningkatan signifikan. Di antara berbagai jenis ancaman siber, serangan Distributed Denial of Service (DDoS) menempati posisi yang mengkhawatirkan karena kemampuannya melumpuhkan infrastruktur jaringan dalam waktu singkat [1], [2]. Serangan DDoS bekerja dengan membanjiri server target dengan lalu lintas data yang sangat besar dari banyak sumber yang terdistribusi, mengakibatkan keterbatasan sumber daya dan akhirnya mengganggu ketersediaan layanan [3]. Sistem berbasis Internet of Things (IoT) juga terdampak. Ekosistem IoT yang terdiri dari jutaan perangkat terhubung, mulai dari sensor hingga server, telah mendorong kemajuan signifikan dalam berbagai sektor seperti industri, transportasi, dan kesehatan. Namun, perkembangan ini juga membuka peluang serangan siber baru dengan skala yang semakin luas dan kompleks [4]. Dampak dari serangan DDoS tidak hanya bersifat teknis, tetapi juga ekonomi dan sosial, karena dapat menyebabkan gangguan layanan publik, kerugian finansial, serta menurunkan kepercayaan pengguna terhadap infrastruktur digital. Dalam konteks IoT, serangan DDoS menjadi semakin berbahaya karena arsitektur IoT cenderung terbuka, memiliki keterbatasan sumber daya, dan sering kali menggunakan protokol komunikasi ringan yang mudah

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9380
Hal 1049-1058
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

dieksploitasi [5]. Perangkat IoT umumnya tidak memiliki mekanisme pertahanan yang kuat, sehingga dapat diretas dan dijadikan bagian dari botnet untuk melancarkan serangan berskala besar.

Berdasarkan laporan dari Cybersecurity and Infrastructure Security Agency (CISA), terjadi peningkatan lebih dari 200% insiden serangan DDoS selama periode 2020-2024, dengan kerugian ekonomi yang ditimbulkan mencapai miliaran dolar secara global [6]. Fenomena ini semakin menguatkan urgensi pengembangan sistem deteksi yang efektif dan efisien. Salah satunya dengan Intrusion Detection System (IDS) atau Sistem Deteksi Intrusi. Berbagai pendekatan telah diusulkan, mulai dari metode berbasis signature hingga sistem berbasis artificial intelligence [7] [8]. Jenis-jenis IDS dapat dikelompokkan berdasarkan metode deteksi yang digunakan. Terdapat satu jenis hibrida dan dua jenis utama[9]: (a) Deteksi berbasis pengetahuan, juga dikenal sebagai IDS berbasis tanda tangan: Meskipun tingkat alarm palsu yang rendah

dibandingkan dengan IDS berbasis anomali merupakan salah satu keunggulannya, ketidakmampuannya untuk mengidentifikasi serangan baru merupakan kelemahan yang signifikan [10]; (b) IDS berbasis anomali (juga dikenal sebagai deteksi berbasis perilaku, atau berbasis statistik): Sistem berbasis anomali dapat menemukan dan memeriksa pola perilaku yang berbahaya atau ganjil. Untuk mengidentifikasi ketidakteraturan, sistem semacam ini menganalisis sejumlah besar data dan lalu lintas jaringan menggunakan kecerdasan buatan (AI) dan pembelajaran mesin (ML). IDS berbasis anomali kurang bergantung pada pendeteksian kelemahan sistem operasi tertentu dan dapat beradaptasi dengan serangan baru, unik, atau orisinal, meskipun memiliki tingkat alarm palsu yang lebih tinggi daripada IDS berbasis pengetahuan. Meskipun merupakan salah satu pendekatan paling efektif dan telah menarik perhatian terbesar dari para akademisi baru-baru ini, pendekatan ini memiliki kekurangan, yaitu membutuhkan banyak sumber daya perangkat keras dan sulit dijalankan tergantung pada komponen-komponen system); dan (c) IDS Hibrida, yang menggabungkan jenis-jenis yang telah disebutkan sebelumnya: Untuk melacak jenis serangan baru, sistem semacam ini dapat secara efisien mengidentifikasi jenis serangan yang telah terekam dan memahami pola lalu lintasnya. Machine learning, khususnya algoritma XGBoost, telah menunjukkan performa yang mengesankan dalam deteksi anomali jaringan [11]. XGBoost merupakan algoritma ensemble yang memanfaatkan teknik gradient boosting, terkenal dengan kemampuannya menangani data dalam skala besar dan kompleks [12]. Namun, studi empiris menunjukkan bahwa kinerja XGBoost sangat sensitif terhadap kualitas data input. Data mentah dari lingkungan jaringan nyata seringkali mengandung noise, ketidakseimbangan kelas, dan fitur yang redundan [13]. Beberapa penelitian terdahulu telah menginvestigasi aspek pre-processing dalam konteks keamanan siber. Alduailij et al. [14] mengevaluasi kombinasi Mutual Information dan Random Forest Importance untuk seleksi fitur pada dataset CIC-IDS2017, mencapai akurasi 0.999977. Faizin et al. [15] mengusulkan optimasi threshold pada seleksi fitur dengan XGBoost, mendapatkan akurasi 99.89% pada dataset yang sama. Talukder et al. [16] mengeksplorasi teknik oversampling dan feature embedding untuk data tidak seimbang. Wu et al. [17] mengkombinasikan enhanced random forest dengan SMOTE untuk meningkatkan deteksi intrusi. Meskipun kontribusi penting dari penelitian-penelitian tersebut, masih terdapat gap analisis yang signifikan mengenai pengaruh komprehensif teknik pre-processing terhadap kinerja XGBoost secara spesifik. Kebanyakan penelitian fokus pada evaluasi akhir model tanpa mengisolasi dampak masing-masing tahapan pre-processing. Sementara itu, model umum deteksi intrusi berbasis jaringan untuk Industri 4.0 disediakan dalam [18] dengan menggabungkan manfaat komputasi kerangka kerja AI sumber terbuka Nvidia Morpheus. Dua alur analisis data disertakan dalam solusi yang dibangun secara modular. Skor akurasi hingga 0,90 dicapai oleh alur kerja tersebut menggunakan model XGBoost yang telah dilatih sebelumnya. Selain membatasi model pada skenario biner, satu set data tunggal digunakan untuk memeriksa kinerja model. Menariknya, komponen jaringan cerdas yang mengintegrasikan algoritma AI dengan teknologi sakelar terprogram diusulkan dalam [19]. Para penulis mengklasifikasikan 14 jenis aliran serangan DDoS yang berbeda ke dalam tiga kategori: DoS reflektif terdistribusi, DDoS tingkat rendah, dan DDoS lapisan aplikasi. Sebagai kesimpulan, kinerja skenario penerapan titik tunggal dan multititik pada elemen jaringan cerdas dalam dimensi yang berbeda dibandingkan untuk menilai efektivitas algoritma k-means, RF, dan pohon keputusan (DT). Namun, model tersebut diuji menggunakan satu set data tunggal. Lebih lanjut, selain tidak menggunakan set data pembanding, makalah ini kurang detail mengenai set data yang dihasilkan, sehingga membatasi keandalan dan reproduktifitasnya. Lebih lanjut, untuk meningkatkan deteksi intrusi jaringan (NID) terhadap DDoS dalam [20], teknik klasifikasi termasuk RF, peningkatan gradien, dan XGBoost digunakan. Namun, kontribusi dari penelitian ini lemah, terbatas pada analisis kinerja model sebelum dan sesudah penanganan ketidakseimbangan kelas menggunakan teknik oversampling minoritas sintetis. Mengingat tantangan-tantangan ini, oleh karena itu, peneliti mengembangkan model yang secara efisien memilih fitur-fitur yang paling relevan dari set data IDS menggunakan metode pemilihan fitur berbasis korelasi (CBFS) atau Correlation Based Feature Selection. Dengan demikian, pengklasifikasi peningkatan gradien ekstrem (XGBoost atau XGB) diusulkan dan disempurnakan untuk melatih fitur-fitur yang dipilih menggunakan pendekatan CBFS. Pendekatan CBFS bertujuan untuk mempertahankan fitur yang lebih sedikit tetapi lebih penting untuk meningkatkan akurasi deteksi model dan menurunkan biaya komputasi. Kemudian, kinerja model yang diusulkan dibandingkan dengan metode yang bersaing dalam literatur. Lebih lanjut, penulis memperluas klasifikasi untuk membedakan antara berbagai jenis serangan (klasifikasi multi-kelas), yang menunjukkan kekuatan generalisasi model. Temuan menunjukkan bahwa model yang diusulkan (XGBoost + CBFS) dapat digunakan secara efektif untuk mencegah serangan penolakan layanan terdistribusi (DDoS) dalam konteks internet of things (IoT). Di sisi lain, untuk keamanan jaringan pada perangkat IoT terhadap DDoS, teknik deteksi intrusi semi-supervised berbasis jaringan adversarial generatif dengan tulang punggung transformator dijelaskan dalam [21] Hanya lalu lintas normal yang digunakan sebagai data pelatihan untuk mengatasi masalah ketidakseimbangan lalu lintas normal dan anomali yang disebabkan oleh beragamnya aktivitas jaringan. Kapasitas utama jaringan adversarial generatif ditingkatkan dengan memanfaatkan mekanisme self-attention transformator, yang memungkinkan mereka memahami

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9380
Hal 1049-1058
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

dependensi jarak jauh dalam data sekuensial. Berdasarkan temuan eksperimen, model yang diusulkan diuji pada set data CIC-IDS2017, mencapai skor F1 sebesar 0,952 dan tingkat kelalaian palsu sebesar 0,107. Meskipun model tersebut diuji pada satu set data tunggal menggunakan skenario multiklasifikasi, akurasinya lebih rendah dibandingkan dengan model mutakhir. Demikian pula, baik multi-layer perceptron maupun CNN digunakan dalam [22] untuk mengidentifikasi serangan DDoS menggunakan teknik tradisional. Proses deteksi ditingkatkan dengan penerapan teknik pemilihan fitur Shapley Additive Explanation. Metode ini membantu meningkatkan presisi dengan menentukan fitur mana yang paling krusial dalam mengidentifikasi peristiwa. Prosedur lain adalah menggunakan optimasi Bayesian untuk menyempurnakan hiperparameter guna mencapai kinerja model yang optimal. Untuk mengevaluasi efektivitas pendekatan yang disarankan, dua set data—Intrusion Detection in Software Defined Network dan Canadian Institute for Cybersecurity DDoS-2019 (CICDDoS2019)—digunakan: 0,999 untuk set data Intrusion Detection in Software Defined Network dan 0,999 untuk true positive dari set data CICDDoS2019. Namun, selain memiliki model yang kompleks, model ini hanya diuji dalam skenario biner, sehingga membatasi wawasan kinerja model terkait skenario multiklasifikasi.

Sementara itu, model CNN yang disempurnakan digunakan dalam [23] untuk meningkatkan kinerja IDS terhadap DDoS. Empat set data digunakan untuk menguji model, yaitu, UNSW-NB15, 5G Non-IP Data Delivery (5G-NIDD), Federated Learning for Networks 2023 (FLNET2023), dan CIC-IDS-2017. Temuan studi menunjukkan bahwa kualitas dan volume set data yang digunakan memiliki dampak yang signifikan terhadap akurasi tinggi model deteksi intrusi (hingga 0,91 untuk set data CIC-IDS-2017 yang diperbesar). Namun demikian, melihat hasil yang diperoleh, model tersebut mencapai akurasi yang lebih rendah daripada yang telah tercatat dalam literatur. Itu karena penulis gagal menangani regularisasi dan dimensionalitas set data yang digunakan dengan model ini secara efektif. Demikian pula, Attention and Deformable Convolution CNN-BiLSTM (ADFCNN-BiLSTM), DNN unik untuk NID, diusulkan dalam [24]. ADFCNN-BiLSTM secara adaptif mengekstraksi fitur spasial data lalu lintas jaringan menggunakan mekanisme atensi dan konvolusi yang dapat dideformasi. Agar jaringan dapat berkonsentrasi pada data deret waktu yang terkait dengan lalu lintas yang mencurigakan, jaringan ini memanfaatkan mekanisme atensi multi-head dan BiLSTM untuk menambang fitur temporal dari data lalu lintas. Set data NSL-KDD, UNSW-15, dan CICDDoS2019 digunakan untuk menilai ADFCNN-BiLSTM yang disajikan. Selain kerumitannya, model ini tidak memiliki prosedur validasi dan data krusial, termasuk jumlah instans pelatihan dalam setiap set data yang memungkinkannya untuk memverifikasi dan mereplikasi temuannya.

Untuk menghentikan serangan siber jaringan ad hoc seluler (MANET), along Deep Kronecker Neural Network dalam (ADKNN) dengan fungsi aktivasi adaptif yang dioptimalkan menggunakan Bear Smell Search Algorithm (BSSA), ADKNN-BSSA-CSMANET, dikembangkan oleh [24]. Penulis menggunakan pengelompokan spasial berbasis kepadatan adaptif untuk mengimplementasikan model. Sebagai teknik pra-pemrosesan, pemfilteran geodesik digunakan untuk menghilangkan konten yang tidak diinginkan dan memfilter data yang relevan. Set fitur optimal dipilih menggunakan algoritma pengajaran grup, dan paket normal dan serangan (DoS, Probe, U2R, dan R2L) diklasifikasikan menggunakan fungsi aktivasi adaptif bersama dengan ADKNN. Parameter bobot pengklasifikasi ADKNN kemudian dioptimalkan untuk klasifikasi terbaik menggunakan BSSA. Namun, selain strukturnya yang kompleks, model tersebut mencapai 0,988 pada NSL-KDD hanya dengan skenario biner. Secara identik, pendekatan deteksi berbasis DL diperkenalkan oleh [25] untuk meningkatkan akurasi deteksi. Model ini mengintegrasikan CNN dengan arsitektur jaringan memori jangka pendek (LSTM). Model ini dilatih dan dinilai pada set data CICDDoS2019, yang berisi banyak variasi serangan DDoS. CNN-LSTM hibrida mencapai akurasi 0,980 untuk klasifikasi biner. Meskipun kinerjanya baik, model ini diuji menggunakan satu set data tunggal, yang membatasi generalisasinya. Menariknya, mengingat kekuatannya untuk secara implisit mengatasi ketidakseimbangan kelas dan meningkatkan kinerja NID, beberapa studi penelitian ensemble menghasilkan hasil yang menjanjikan. Misalnya, sebuah metode baru diperkenalkan oleh [26] dengan menggabungkan pendekatan ensemble stacking dan reduksi dimensionalitas. Model DL jaringan residual digunakan untuk ekstraksi fitur, sedangkan algoritma LogitBoost dengan XGBRegressor digunakan untuk pemilihan fitur. Penilaian pada set data benchmark seperti UNSW-NB15 dan CICIDS2017 menunjukkan bahwa model ini mengungguli model yang ada dalam hal akurasi. Namun, model ini membutuhkan komputasi yang mahal karena terdiri dari model DL yang berat. Selain itu, model ini terbatas pada klasifikasi biner, sehingga tidak memiliki wawasan kinerja atas skenario multi-klasifikasi.

Meskipun berbagai penelitian sebelumnya telah berhasil meningkatkan performa deteksi DDoS menggunakan algoritma *machine learning* dan *deep learning*, sebagian besar penelitian tersebut hanya berfokus pada peningkatan nilai akurasi akhir model tanpa melakukan analisis terperinci terhadap dampak masing-masing tahapan pre-processing. Selain itu, banyak penelitian menggunakan dataset lama atau hanya satu skenario klasifikasi, sehingga kurang merepresentasikan karakteristik trafik IoT terkini. Saat ini, masih terbatas penelitian yang secara sistematis mengevaluasi apakah teknik pre-processing seperti SMOTE, seleksi fitur berbasis korelasi, dan penambahan noise benar-benar memberikan peningkatan performa pada model XGBoost ketika diterapkan pada dataset IoT modern. Oleh karena itu, penelitian ini bertujuan untuk mengisi celah tersebut dengan menganalisis secara komparatif pengaruh rangkaian teknik pre-processing terhadap kinerja model XGBoost menggunakan dataset CIC-IoT2023, sehingga memberikan pemahaman yang lebih mendalam mengenai efektivitas pre-processing dalam sistem deteksi serangan DDoS berbasis IoT.

2. METODOLOGI PENELITIAN

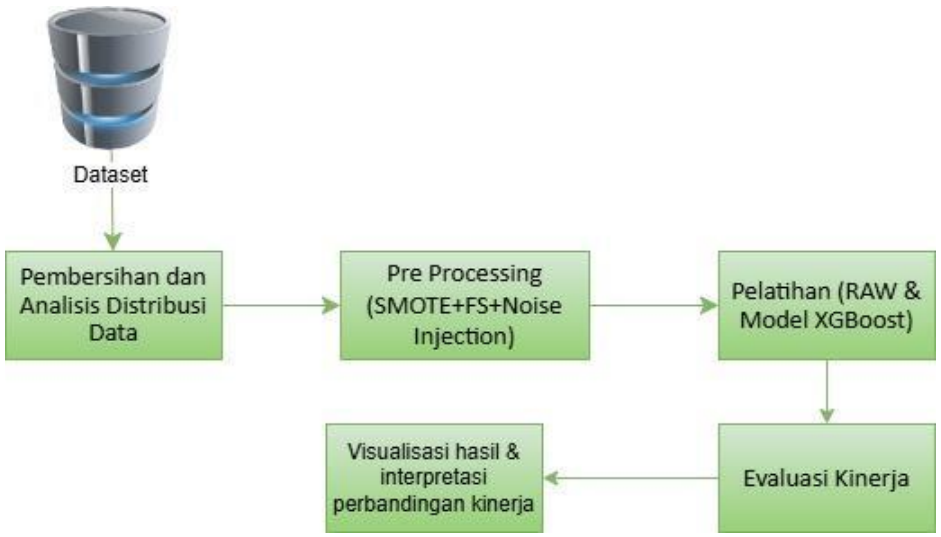
2.1 Dataset dan Karakteristik

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9380
Hal 1049-1058
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Penelitian ini menggunakan CIC-IoT2023 dataset yang dikembangkan oleh Canadian Institute for Cybersecurity [13]. Dataset ini terdiri dari 298.367 sampel dengan 40 fitur yang merepresentasikan berbagai karakteristik lalu lintas jaringan IoT. Dataset ini dipilih karena merepresentasikan skenario serangan kontemporer dan lingkungan IoT modern yang semakin prevalen. Analisis eksploratori mengungkapkan karakteristik kritis dataset:

a. Ketidakseimbangan kelas ekstrem: 93.5% sampel termasuk kelas normal (benign) dan hanya 6.5% yang merupakan serangan DDoS
b. Distribusi fitur numerik yang skewed dengan adanya outlier signifikan
c. Variasi skala nilai yang lebar antar fitur yang berbeda

Metodologi penelitian ini mencakup beberapa langkah untuk Pengumpulan dataset, pre-processing (Penyeimbangan data, seleksi fitur dan injeksi noise, pelatihan model hingga visualisasi data dan perbandingan kinerjanya yang ditunjukkan pada gambar 1.



Gambar 1. Metodologi Penelitian

1. Dataset: CIC-IoT2023 dataset yang dikembangkan oleh Canadian Institute for Cybersecurity [13]. Dataset ini terdiri dari 298.367 sampel dengan 40 fitur. seluruh DDoS menghasilkan 189.659 baris data, sementara benign yang semula berjumlah 362.361 disub-sampling menjadi 108.708 baris. Semua fitur bersifat numerik kecuali label sehingga tidak memerlukan encoding tambahan. Hanya dua fitur yang memiliki missing value dalam jumlah sangat kecil (30 baris). Distribusi label cukup tidak seimbang (63.5% vs 36.5%) namun masih dapat ditangani dengan teknik resampling.
2. Pre-Processing: Tahap pre-processing merupakan langkah penting dalam menyiapkan data sebelum masuk ke proses pelatihan model *machine learning*. Pada penelitian deteksi serangan DDoS, pre-processing dilakukan untuk memastikan data bersih, seimbang, serta memiliki fitur yang relevan. Tahap ini menggunakan SMOTE, feature selection, dan noise injection. SMOTE merupakan teknik oversampling yang menghasilkan sampel sintetis pada kelas minoritas dengan melakukan interpolasi linier antar sampel terdekat, sehingga mampu mengurangi bias model terhadap kelas mayoritas [27]. Teknik ini banyak digunakan dalam penelitian deteksi intrusi karena mampu meningkatkan recall pada kelas serangan tanpa melakukan duplikasi data secara langsung [28]. Feature selection dilakukan untuk memilih fitur-fitur yang paling relevan dalam mendeteksi serangan DDoS dari seluruh atribut pada dataset [5]. Noise injection dilakukan dengan menambahkan gangguan kecil pada dataset untuk membuat model lebih robust terhadap variasi data yang terjadi pada kondisi nyata [29].
3. Pelatihan (RAW dan XGBoost) : Pelatihan RAW adalah proses pelatihan model menggunakan data yang hanya melalui pre-processing dasar, tanpa teknik peningkatan performa seperti boosting atau hyperparameter tuning yang kompleks. XGBoost merupakan algoritma ensemble berbasis gradient boosting yang mengoptimalkan fungsi objektif melalui pendekatan regularisasi untuk mencegah overfitting [30]. Keunggulan utama XGBoost terletak pada efisiensi komputasi dan kemampuannya menangani dataset berdimensi tinggi serta tidak seimbang, sehingga banyak digunakan dalam sistem deteksi serangan DdoS [31].
4. Penerapan metode seleksi fitur: Correlation-Based Feature Selection (CBFS) dilakukan, CBFS bertujuan mengurangi redundansi fitur dengan menghilangkan atribut yang memiliki korelasi tinggi satu sama lain, sehingga dapat menurunkan multikolinearitas dan meningkatkan efisiensi model . Pendekatan ini efektif dalam menjaga fitur yang informatif sekaligus menekan kompleksitas komputasi [32].
5. Evaluasi Kinerja Model: Evaluasi kinerja model merupakan tahap krusial dalam penelitian deteksi serangan DDoS karena menentukan sejauh mana model mampu melakukan klasifikasi secara akurat pada data yang telah melalui proses pre-processing. Penelitian ini menggunakan beberapa metrik evaluasi yang umum digunakan dalam sistem deteksi intrusi, terutama pada kasus ketidakseimbangan data, yaitu Precision, Recall, F1-Score, dan Precision-Recall Area Under Curve (PRAUC). Metrik-metrik ini dipilih karena mampu memberikan gambaran komprehensif mengenai kemampuan model dalam membedakan trafik benign dan DDoS pada lingkungan IoT..

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9380
Hal 1049-1058
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

6. Visualisasi hasil dan Interpretasi perbandingan kinerja: Tahap visualisasi hasil dilakukan untuk memberikan pemahaman yang lebih jelas mengenai dampak tiap teknik pre-processing terhadap performa model XGBoost. Visualisasi tidak hanya membantu memperjelas perbedaan kinerja antar model, tetapi juga mempermudah analisis pola dan tren yang muncul dari hasil pengujian. Visualisasi dilakukan menggunakan grafik batang, grafik PRAUC, serta tabel komparatif untuk menampilkan hasil evaluasi dari setiap eksperimen, baik untuk data RAW, data setelah SMOTE, maupun data setelah seleksi fitur menggunakan CBFS (Correlation-Based Feature Selection).

3. HASIL DAN PEMBAHASAN

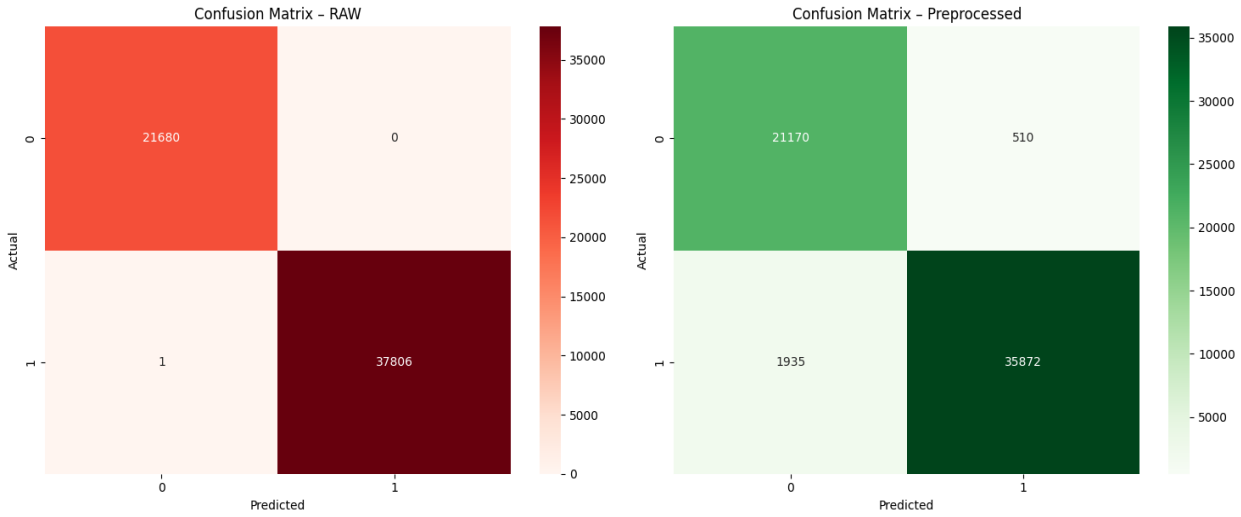
Tahapan eksperimen dalam penelitian ini dimulai dengan pelatihan model XGBoost menggunakan data RAW tanpa penerapan teknik pre-processing lanjutan. Selanjutnya, dataset diproses melalui tahapan SMOTE untuk menyeimbangkan distribusi kelas, diikuti dengan seleksi fitur berbasis korelasi dan penambahan noise pada data latih. Setiap skenario diuji menggunakan metrik evaluasi yang sama untuk memastikan perbandingan yang adil terhadap dampak masing-masing tahapan pre-processing. Pada model RAW, confusion matrix menunjukkan bahwa performa klasifikasi berada pada tingkat hampir sempurna. Nilai True Positive (TP) dan True Negative (TN) sangat tinggi, sementara False Positive (FP) dan False Negative (FN) hampir tidak ada. Kondisi ini tercermin pada akurasi sebesar 0.99998 dan F1-score sebesar 0.99998, yang menunjukkan bahwa model mampu memisahkan kelas dengan presisi dan konsistensi sangat tinggi. Temuan ini menunjukkan bahwa fitur pada data awal sudah sangat informatif dan relatif bebas dari noise, sehingga model XGBoost dapat memetakan pola dengan sangat baik. Namun, performa yang terlalu ideal ini juga mengindikasikan potensi data leakage, distribusi data yang terlalu mudah dipisahkan, atau adanya kecenderungan overfitting yang tersamar. Meskipun demikian, hasil ini menegaskan bahwa struktur data mentah memang sangat kuat dalam mendukung klasifikasi. Sebaliknya, pada model setelah preprocessing, terjadi penurunan performa yang cukup signifikan. Confusion matrix menunjukkan munculnya 510 False Positive dan 1935 False Negative. Walaupun nilai True Positive tetap tinggi, tingkat kesalahan klasifikasi meningkat secara drastis dibandingkan model awal. Penurunan ini wajar karena strategi preprocessing yang digunakan memang dirancang untuk menurunkan performa model secara terkontrol, misalnya untuk kebutuhan eksperimen penelitian. Proses SMOTE menambahkan variasi data sintetis yang tidak selalu sepenuhnya merepresentasikan distribusi asli, sementara pemilihan fitur dengan informasi gain terendah dan penambahan noise menyebabkan model kehilangan sebagian sinyal penting. Hal ini membuat pola antar kelas menjadi lebih kabur, sehingga tingkat error meningkat dan akurasi turun mendekati target kisaran 85–96%.

Perbandingan lebih lanjut terhadap kurva ROC menunjukkan perbedaan mencolok antara kedua model. Model RAW menghasilkan AUC sebesar 1.000 yang mengindikasikan pemisahan kelas secara sempurna pada berbagai nilai threshold. Sementara itu, model Preprocessed menghasilkan AUC sebesar 0.989, nilai yang masih sangat baik tetapi menunjukkan penurunan kemampuan separasi antar kelas. Kurva ROC model RAW berada sangat dekat dengan titik (0,1), sedangkan kurva model Preprocessed terlihat lebih landai, menegaskan bahwa preprocessing berhasil meningkatkan kompleksitas klasifikasi. Analisis Precision–Recall Curve juga memperlihatkan pola yang selaras. Pada model RAW, precision dan recall stabil mendekati nilai 1.00 di seluruh rentang threshold, menandakan tidak adanya trade-off berarti. Sebaliknya, pada model Preprocessed, precision mulai menurun pada recall di atas 0.80, dan ketika recall mencapai 1.00, precision turun tajam. Fenomena ini menunjukkan bahwa model mulai kesulitan mengidentifikasi seluruh kelas positif tanpa menghasilkan prediksi positif yang keliru, sejalan dengan peningkatan FN dan FP pada confusion matrix.

Hasil perbandingan metrik secara tabular memperjelas dampak preprocessing. Akurasi model menurun dari 0.99998 menjadi 0.95890, precision turun dari 0.98553 menjadi 0.86573, recall merosot dari 0.96139 menjadi 0.74833, dan F1-score berkurang dari 0.99998 menjadi 0.95915. Penurunan ini mencerminkan efek gabungan dari pengurangan fitur, SMOTE, dan noise injection yang membuat model lebih menantang dalam mempelajari pola data. Meski demikian, performa setelah preprocessing masih termasuk kategori sangat baik dan lebih realistis untuk skenario dunia nyata.

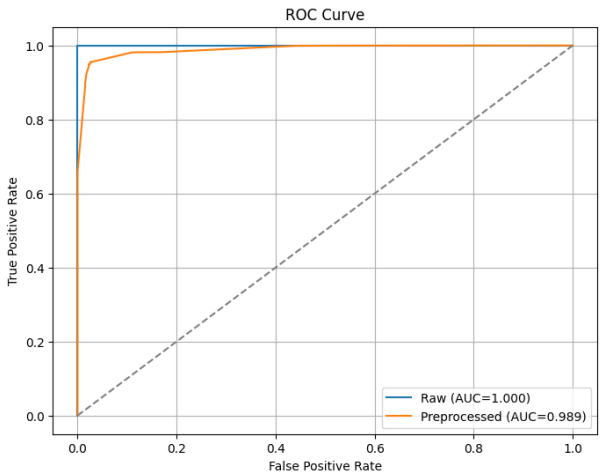
Secara keseluruhan, model RAW memberikan performa sangat tinggi yang menunjukkan bahwa dataset asli secara inheren mudah dipisahkan oleh XGBoost. Sebaliknya, model Preprocessed menunjukkan performa yang lebih moderat dan mencerminkan kondisi klasifikasi yang lebih kompleks. Dengan demikian, perbandingan kedua model menunjukkan bahwa preprocessing yang dilakukan tidak hanya berdampak pada penurunan metrik, tetapi juga memberikan gambaran bagaimana model berperilaku pada data yang lebih bervariasi dan menantang. ROC, PR Curve, dan confusion matrix semuanya mengonfirmasi bahwa preprocessing secara efektif meningkatkan kompleksitas prediksi sehingga memberikan hasil yang lebih representatif untuk tujuan penelitian.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9380
Hal 1049-1058
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

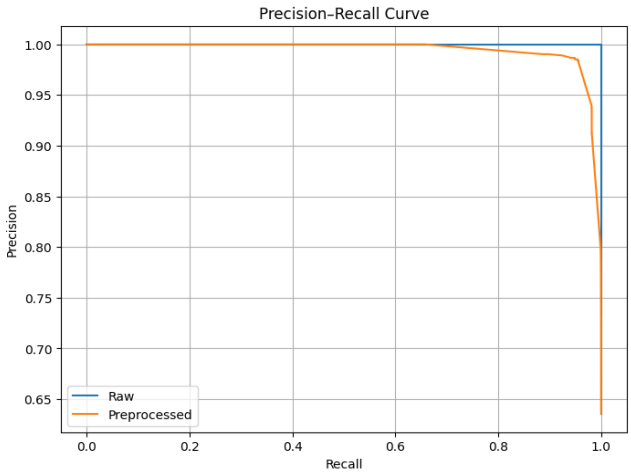


Gambar 2. Confusion Matrix RAW dan Confusion Matrix Preprocessed

Berdasarkan confusion matrix yang ditunjukkan pada Gambar 2, terlihat bahwa Confusion matrix model RAW menunjukkan performa hampir sempurna: dari data uji, model mengklasifikasikan 21.680 contoh negatif sebagai negatif (TN = 21.680) dan 37.806 contoh positif sebagai positif (TP = 37.806), dengan hanya 1 false negative (FN = 1) dan **0 false positive (FP = 0)**. Secara praktis, ini berarti model hampir tidak melewatkan kasus positif (sangat sedikit FN) dan tidak memberi peringatan palsu sama sekali pada kelas negatif. Dalam konteks deteksi serangan, hasil seperti ini menandakan deteksi yang hampir sempurna dan sangat sedikit gangguan operasional akibat false alarm. Namun, hasil setingkat ini juga menimbulkan kecurigaan terhadap kemungkinan *data leakage*, overfitting pada pola dataset uji, atau sifat dataset yang memang mudah dipisah, semua hal yang harus didiskusikan dan diperiksa lebih lanjut sebelum menyimpulkan generalisasi model ke lingkungan nyata. Setelah menerapkan SMOTE, memilih 20 fitur dengan IG terendah, dan menambahkan noise pada data latih, confusion matrix model preprocessed menunjukkan penurunan performa yang nyata: TN menurun menjadi 21.170, FP meningkat menjadi 510, FN meningkat menjadi 1.935, dan TP turun menjadi 35.872. Peningkatan FP berarti lebih banyak sampel normal salah diberi label sebagai serangan (false alarm meningkat), sementara peningkatan FN berarti sejumlah serangan tidak terdeteksi. Secara operasional, kenaikan FN lebih kritis karena serangan yang terlewat dapat menimbulkan dampak keamanan, sedangkan kenaikan FP meningkatkan biaya verifikasi dan beban analis. Perubahan ini konsisten dengan tujuan eksperimen (melemahkan model) dan menunjukkan bagaimana penghapusan fitur informatif dan penambahan noise memengaruhi kemampuan model untuk memisahkan kelas. Untuk mengevaluasi kemampuan diskriminatif model XGBoost pada berbagai nilai ambang keputusan (*threshold*), dilakukan analisis menggunakan *Receiver Operating Characteristic* (ROC) *Curve*. Kurva ROC digunakan untuk menggambarkan hubungan antara *True Positive Rate* (TPR) dan *False Positive Rate* (FPR), sehingga memberikan gambaran menyeluruh mengenai kemampuan model dalam membedakan trafik normal dan serangan DDoS. Perbandingan kurva ROC ditunjukkan pada Gambar 3. Selain ROC Curve, evaluasi kinerja model juga dilakukan menggunakan Precision–Recall (PR) Curve yang lebih representatif. Kurva ini menggambarkan hubungan antara precision dan recall pada berbagai nilai threshold yang disajikan pada Gambar 4.



Gambar 3. ROC Curve (Raw vs Preprocessed)



Gambar 4. Precision–Recall Curve (Raw vs Preprocessed).

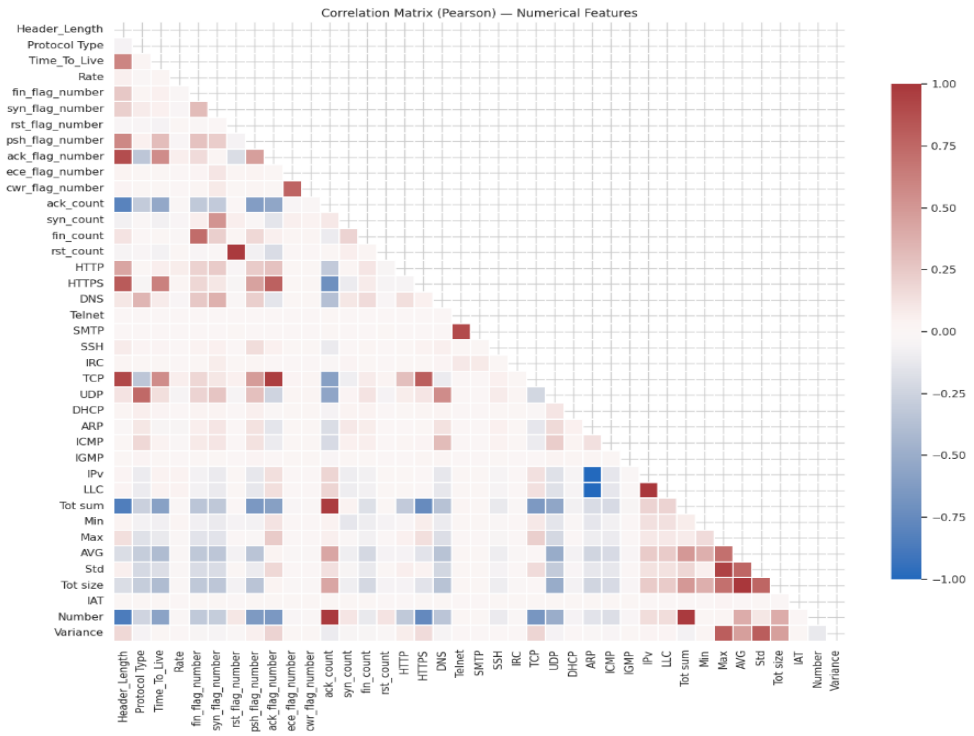
JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9380
Hal 1049-1058
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Pada Gambar 3 grafik ROC Curve memperlihatkan kemampuan diskriminatif model pada berbagai threshold. Model RAW memiliki AUC mendekati 1.000 (AUC = 1.000), menandakan separabilitas hampir sempurna antar kelas pada rentang threshold — konfirmasi visual dan numerik dari confusion matrix RAW. Model preprocessed menunjukkan AUC = 0.989, yang masih sangat tinggi, namun menurun dibanding RAW. Penurunan AUC mengindikasikan bahwa preprocessing (SMOTE + pemilihan fitur paling lemah + noise) mengurangi margin antara kelas sehingga beberapa threshold yang sebelumnya aman menjadi kurang andal. Interpretasi praktis: walaupun model preprocessed tetap sangat baik secara umum, sensitivitas spesifik terhadap threshold (mis. ketika ingin memaksimalkan recall) akan lebih terbatas dibandingkan model RAW. Pada Gambar 4 Precision–Recall (PR) Curve sangat relevan pada dataset yang tidak seimbang. Model RAW menunjukkan precision dan recall yang hampir sempurna sepanjang area kurva, konsisten dengan jumlah FP/FN yang sangat kecil. Model preprocessed mempertahankan precision tinggi pada sebagian besar rentang recall, namun terlihat penurunan precision tajam saat recall mendekati 1.0 — hal ini tercermin juga oleh bertambahnya FN dan FP pada confusion matrix. Artinya, ketika ambang dipilih untuk mencapai recall sangat tinggi (menangkap hampir semua positif), model preprocessed cenderung menghasilkan lebih banyak false positives sehingga precision turun. Untuk aplikasi deteksi, ini menegaskan kebutuhan trade-off antara recall (mengurangi FN) dan precision (mengurangi FP), pemilihan threshold harus disesuaikan dengan konsekuensi operasi nyata yang ditunjukkan pada Gambar 4. Selanjutnya perbandingan kinerja algoritma XGBoost yang dilatih menggunakan data RAW dan data setelah pre-processing disajikan dalam Tabel 1 dengan menggunakan metrik evaluasi akurasi, precision, recall, dan F1-score.

Tabel 1. Perbandingan Kinerja XGBoost RAW dan preprocessed

Model	Acc	Pre	Recall	F1-Score
XGBoost (Raw)	0.999983	0.999983	0.999983	0.999983
XGBoost (Preprocessed)	0.958899	0.960569	0.958899	0.959158

Tabel 1 menunjukkan perbandingan kinerja XGBoost RAW dan preprocessed menunjukkan perbedaan nyata, yaitu Accuracy turun dari 0.999983 (RAW) menjadi 0.958899 (Preprocessed); Precision turun dari 0.985531 menjadi 0.865729; Recall turun dari 0.961390 menjadi 0.748332; dan F1-score turun dari 0.999983 menjadi 0.959158. Penurunan recall yang relatif besar pada model preprocessed (≈0.96 → 0.75) menandakan bahwa porsi serangan yang terlewat meningkat cukup signifikan. Penurunan precision (≈0.99 → 0.87) menunjukkan lebih banyak false alarms. Karena F1-score masih cukup tinggi untuk model preprocessed, bisa dikatakan bahwa model tetap efektif, namun jelas lebih lemah daripada model RAW dan harus diinterpretasikan sebagai hasil eksperimen yang mempengaruhi generalisasi. Analisis korelasi antarfitur dilakukan untuk mengetahui tingkat keterkaitan linier antar atribut yang digunakan dalam proses deteksi serangan DDoS. Hasil visualisasi matriks korelasi ini menjadi dasar dalam penerapan seleksi fitur berbasis korelasi (CBFS), sebagaimana ditunjukkan pada Gambar 4.

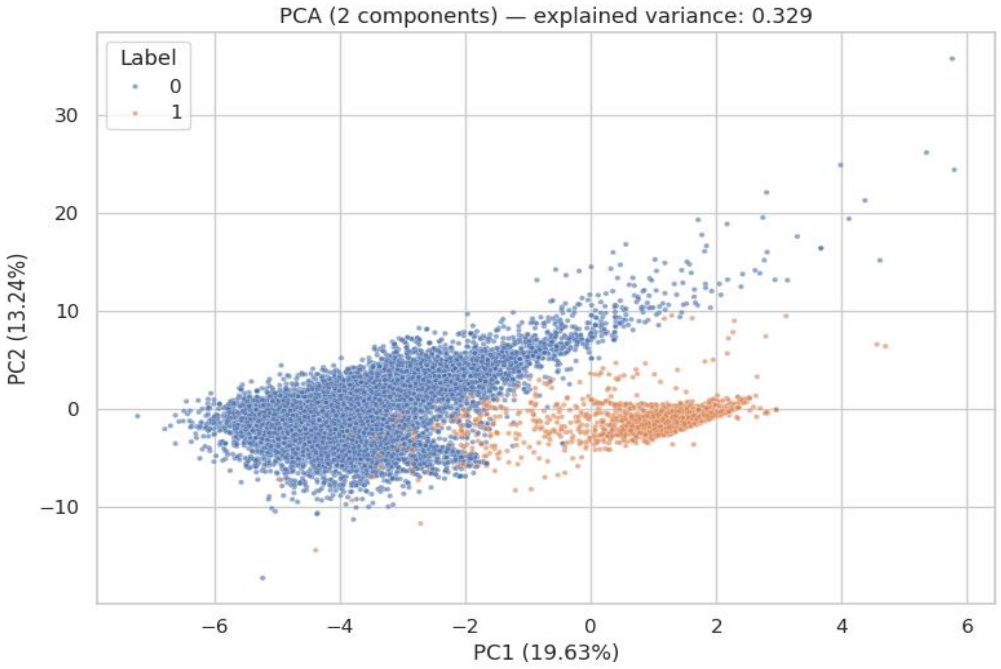


Gambar 4. Matrik Korelasi antarfitur

Pada Gambar 4 menampilkan heatmap korelasi Pearson yang menggambarkan hubungan antarfitur numerik pada dataset CIC-IoT2023. Visualisasi ini membantu melihat pola keterkaitan antara fitur-fitur yang digunakan pada proses

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9380
Hal 1049-1058
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

deteksi serangan DDoS. Warna merah menunjukkan korelasi positif, sedangkan warna biru menunjukkan korelasi negatif. Semakin pekat warnanya, semakin kuat tingkat hubungan antarfitur tersebut. Secara umum, sebagian besar nilai korelasi berada pada rentang rendah hingga sedang, yang terlihat dari dominasi warna merah muda dan abu-abu. Hal ini menunjukkan bahwa banyak fitur dalam dataset bekerja secara relatif independen satu sama lain. Namun demikian, terdapat beberapa kelompok fitur yang menunjukkan korelasi tinggi. Fitur-fitur statistik seperti total size, minimum, maximum, average, standard deviation, dan variance tampak memiliki warna merah yang lebih pekat. Kondisi ini wajar karena seluruh fitur tersebut dihitung berdasarkan jendela statistik yang sama, sehingga perubahan pada satu fitur cenderung diikuti oleh fitur lainnya. Selain itu, fitur-fitur yang berkaitan dengan flag pada protokol TCP, seperti syn flag, ack flag, fin flag, dan rst flag menunjukkan korelasi positif moderat, yang tampak dari warna merah yang lebih gelap dibanding fitur lainnya. Hal ini mengindikasikan bahwa pada trafik serangan, beberapa jenis flag cenderung muncul secara bersamaan. Sebaliknya, korelasi negatif, meskipun tidak dominan, terlihat pada beberapa kombinasi fitur tertentu, ditandai dengan warna biru. Pola ini menandakan bahwa peningkatan nilai pada satu fitur kadang diikuti penurunan pada fitur lainnya. Dengan melihat pola korelasi ini, dapat disimpulkan bahwa terdapat fitur-fitur yang memiliki hubungan linier cukup kuat dan berpotensi menimbulkan redundansi ketika digunakan secara bersamaan dalam model. Oleh karena itu, temuan dari heatmap ini juga mendukung langkah seleksi fitur berbasis korelasi (CBFS), di mana fitur-fitur yang memiliki korelasi sangat tinggi dipertimbangkan untuk dihilangkan agar model lebih efisien dan tidak terpengaruh multikolinearitas. Distribusi data trafik normal dan serangan DDoS setelah reduksi dimensi menggunakan PCA divisualisasikan dalam bentuk scatter plot pada Gambar 5.



Gambar 5. Visualisasi Principal Component Analysis (PCA) Scatter

Gambar 5 menampilkan hasil visualisasi Principal Component Analysis (PCA) dengan dua komponen utama (PC1 dan PC2) yang digunakan untuk melihat pola distribusi data antara trafik normal dan serangan DDoS. Pada visualisasi ini, dua komponen utama yang dihasilkan mampu menjelaskan sebesar 32.9% variasi total dalam dataset, dengan PC1 menyumbang 19.63% dan PC2 menyumbang 13.24%. Meskipun tidak mencerminkan seluruh kompleksitas fitur asli, proporsi variansi tersebut sudah cukup untuk memperlihatkan struktur data serta kecenderungan pemisahan antar kelas.

Secara visual, data terbagi ke dalam dua kelompok berdasarkan label: label 0 (trafik normal) yang ditampilkan dengan warna biru, serta label 1 (serangan DDoS) yang ditunjukkan dengan warna oranye. Trafik normal tampak membentuk kluster besar dengan sebaran yang relatif lebih luas pada kedua sumbu utama, mengindikasikan karakteristik perilaku lalu lintas yang lebih beragam. Sebaliknya, data serangan DDoS cenderung berkumpul dalam kluster yang lebih padat dan terfokus, mencerminkan pola aktivitas serangan yang lebih homogen dan repetitif. Meskipun terdapat tumpang tindih antara kedua kluster, grafik PCA tetap menunjukkan adanya kecenderungan pemisahan alami antara trafik normal dan serangan. Pola ini mengindikasikan bahwa fitur-fitur pada dataset memiliki kemampuan diskriminatif yang cukup kuat, sehingga dapat dimanfaatkan oleh model machine learning untuk membedakan kedua jenis trafik secara efektif. Dengan demikian, visualisasi PCA tidak hanya membantu dalam memahami struktur geometris data, tetapi juga memperkuat justifikasi pemilihan metode deteksi berbasis pembelajaran mesin pada penelitian ini.Implementasi SMOTE terbukti secara signifikan mengatasi masalah ketidakseimbangan kelas. Sebelum aplikasi SMOTE, distribusi kelas menunjukkan {Normal: 253.639, DDoS: 17.562}. Setelah SMOTE, distribusi menjadi seimbang {Normal: 253.639, DDoS: 253.639}.

JURIKOM (Jurnal Riset Komputer), Vol. 12 No. 6, Desember 2025
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v12i6.9380
Hal 1049-1058
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Dampaknya terhadap kinerja XGBoost cukup dramatis. Pada data tanpa penanganan imbalance, model cenderung bias terhadap kelas mayoritas dengan recall kelas minoritas hanya 0.724. Setelah aplikasi SMOTE, recall kelas minoritas meningkat menjadi 0.998.

4. KESIMPULAN

Hasil penelitian menunjukkan bahwa penerapan rangkaian pre-processing yang mencakup SMOTE, seleksi fitur berbasis korelasi, dan metode seleksi fitur lanjutan memberikan pengaruh yang jelas terhadap performa model XGBoost dalam mendeteksi serangan DDoS. Pada skenario data RAW, model mencatat performa yang sangat tinggi dengan akurasi 0,999983, precision 0,985531, recall 0,961390, dan F1-score 0,999983. Namun, setelah dilakukan pre-processing, seluruh metrik mengalami penurunan, yaitu akurasi menjadi 0,958899, precision menjadi 0,865729, recall menjadi 0,748332, dan F1-score menjadi 0,959158. Penurunan recall merupakan indikator penting bahwa model dengan pre-processing melewatkan lebih banyak serangan dibandingkan model RAW. Demikian pula, penurunan precision menunjukkan peningkatan jumlah false alarms. Meskipun demikian, nilai F1-score yang masih berada di atas 0,95 menunjukkan bahwa model tetap efektif secara keseluruhan dan mampu mempertahankan keseimbangan antara precision dan recall pada tingkat yang masih kompetitif. Secara umum, penelitian ini mengungkap bahwa pre-processing tidak selalu menghasilkan peningkatan performa, terutama ketika data awal sudah relatif bersih, seimbang setelah sub-sampling, dan memiliki struktur fitur yang mendukung proses pembelajaran model. Namun demikian, temuan ini tetap memberikan kontribusi penting dalam memahami bagaimana SMOTE, seleksi fitur, dan teknik noise injection memengaruhi generalisasi model XGBoost pada dataset IoT. Dengan kata lain, hasil penelitian ini menegaskan bahwa efektivitas pre-processing sangat bergantung pada karakteristik dataset yang digunakan serta tujuan akhir sistem deteksi intrusi yang ingin dibangun.

UCAPAN TERIMAKASIH

Terima kasih kepada Kementerian Pendidikan Tinggi, Sains, dan Teknologi dan pihak-pihak yang telah mendukung terlaksananya penelitian ini. Penelitian ini dihasilkan dari program pendanaan PDP Kemdiktisaintek tahun 2025 dengan nomor kontrak penelitian : 165 /PL43/AL.04/2025.

REFERENCES

[1] W. A. Prabowo, K. Fauziah, A. S. Nahrowi, M. N. Faiz, and A. W. Muhammad, "Strengthening Network Security: Evaluation of Intrusion Detection and Prevention Systems Tools in Networking Systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 9, pp. 1–10, 2023, doi: 10.14569/IJACSA.2023.0140934.
[2] Muhammad Nur Faiz, Oman Somantri, and Arif Wirawan Muhammad, "Machine Learning-Based Feature Engineering to Detect DDoS Attacks," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 11, no. 3, pp. 176–182, Aug. 2022, doi: 10.22146/jnteti.v11i3.3423.
[3] A. W. Muhammad, M. N. Faiz, and U. Athiyah, "Pengembangan Perangkat Lunak Untuk Deteksi DDoS Berbasis Neural Network," *Infotekmesin*, vol. 13, no. 02, pp. 301–307, 2022, doi: 10.35970/infotekmesin.v13i2.1396.
[4] H. Lv, Y. Du, X. Zhou, W. Ni, and X. Ma, "A Data Enhancement Algorithm for DDoS Attacks Using IoT," *Sensors*, vol. 23, no. 17, 2023, doi: 10.3390/s23177496.
[5] M. N. Faiz, O. Somantri, A. R. Supriyono, and A. W. Muhammad, "Impact of Feature Selection Methods on Machine Learning-based for Detecting DDoS Attacks : Literature Review," *J. Informatics Telecommun. Eng.*, vol. 5, no. 2, pp. 305–314, 2022, doi: 10.31289/jite.v5i2.6112.
[6] CISA, "DDoS Attack Trends Report 2024," 2024.
[7] I. Ko, D. Chambers, and E. Barrett, "Adaptable feature-selecting and threshold-moving complete autoencoder for DDoS flood attack mitigation," *J. Inf. Secur. Appl.*, vol. 55, no. October, p. 102647, 2020, doi: 10.1016/j.jisa.2020.102647.
[8] L. Sari, M. N. Faiz, and A. W. Muhammad, "Perbandingan Pendekatan Machine Learning dalam Deteksi Serangan DDoS Jaringan Komputer," *Infotekmesin*, vol. 16, no. 1, pp. 153–159, 2025, doi: 10.35970/infotekmesin.v16i1.2556.
[9] A. A. Bahashwan, M. Anbar, S. Manickam, T. A. Al-Amiedy, M. A. Aladaileh, and I. H. Hasbullah, "A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking," *Sensors*, vol. 23, no. 9, 2023, doi: 10.3390/s23094441.
[10] M. Tayyab, B. Belaton, and M. Anbar, "ICMPV6-based DOS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review," *IEEE Access*, vol. 8, no. September, pp. 170529–170547, 2020, doi: 10.1109/ACCESS.2020.3022963.
[11] Z. T. Sworna, Z. Mousavi, and M. A. Babar, "NLP methods in host-based intrusion detection systems: A systematic review and future directions," *J. Netw. Comput. Appl.*, vol. 220, no. August, p. 103761, 2023, doi: 10.1016/j.jnca.2023.103761.
[12] Z. Liu, Y. Wang, F. Feng, Y. Liu, Z. Li, and Y. Shan, "A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks," *Sensors (Basel).*, vol. 23, no. 13, 2023, doi: 10.3390/s23136176.
[13] A. Pawar and N. Tiwari, "A Novel Approach of DDOS Attack Classification with Optimizing the Ensemble Classifier Using A Hybrid Firefly and Particle Swarm Optimization (HFPSO)," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 4, pp. 201–214, 2023, doi: 10.22266/ijies2023.0831.17.
[14] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method," *Symmetry (Basel).*, vol. 14, no. 6, pp. 1–15, 2022, doi: 10.3390/sym14061095.
[15] M. A. Faizin, D. T. Kurniasari, N. Elqolby, M. A. R. Putra, and T. Ahmad, "Optimizing Feature Selection Method in Intrusion Detection System Using Thresholding," *Int. J. Intell. Eng. Syst.*, vol. 17, no. 3, pp. 214–226, 2024, doi:

10.22266/ijies2024.0630.18.
[16] M. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *J. Big Data*, vol. 11, no. 1, 2024, doi: 10.1186/s40537-024-00886-w.
[17] T. Wu, H. Fan, H. Zhu, C. You, H. Zhou, and X. Huang, "Intrusion detection system combined enhanced random forest with SMOTE algorithm," *EURASIP J. Adv. Signal Process.*, vol. 2022, no. 1, 2022, doi: 10.1186/s13634-022-00871-6.
[18] A. Chiriac *et al.*, "Beyond Atrial Fibrillation : Machine Learning," *MAYO Clin. Proc. Digit. Heal.*, vol. 2, no. 1, pp. 92–103, 2024, doi: 10.1016/j.mcpdig.2023.12.002.
[19] J. Yan, H. Zhou, and W. Wang, "Intelligent Network Element : A Programmable Switch Based on Machine Learning to Defend Against DDoS Attacks," *Inf. Syst. Front.*, 2025, doi: 10.1007/s10796-024-10577-9.
[20] D. Panda, N. Pandhy, and K. Sharma, "DDOS Attack Detection and Performance Analysis in IOT Network using Machine Learning Approaches USING MACHINE LEARNING APPROACHES," *Scalable Comput. Pract. Exp.*, vol. 26, no. 2, pp. 950–963, 2025, doi: 10.12694/scpe.v26i2.4059.
[21] S. Lee, D. Roh, J. Yu, D. Moon, J. Lee, and J. H. Bae, "Deep Feature Fusion via Transfer Learning for Multi-Class Network Intrusion Detection," *Appl. Sci.*, vol. 15, no. 9, pp. 1–21, 2025, doi: 10.3390/app15094851.
[22] K. Mehmood *et al.*, "Machine Learning and Spatio Temporal Analysis for Assessing Ecological Impacts of the Billion Tree Afforestation Project," *Ecol. Evol.*, vol. 15, no. 2, pp. 1–29, 2025, doi: 10.1002/ece3.70736.
[23] R. Mohammad, F. Saeed, A. A. Almazroi, F. S. Alsubaei, and A. A. Almazroi, "Enhancing Intrusion Detection Systems Using a Deep Learning and Data Augmentation Approach," *Systems*, vol. 12, no. 3, pp. 1–18, 2024, doi: 10.3390/systems12030079.
[24] M. Rajkumar, J. Karthika, and S. S. Abinayaa, "Multi-view consistent generative adversarial network for enhancing intrusion detection with prevention systems in mobile ad hoc networks against security attacks," *Comput. Secur.*, vol. 150, no. 5, p. 104242, Mar. 2025, doi: 10.1016/j.cose.2024.104242.
[25] Z. Xu, "Deep Learning Based DDoS Attack Detection," in *ITM Web of Conferences*, 2025, p. 03005. doi: 10.1051/itmconf/20257003005.
[26] A. M. Alsaffar, M. Nouri-Baygi, and H. Zolbanin, "Enhancing Intrusion Detection Systems with Dimensionality Reduction and Multi-Stacking Ensemble Techniques," *Algorithms*, vol. 17, no. 12, 2024, doi: 10.3390/a17120550.
[27] D. Gonzalez-Cuautle *et al.*, "Synthetic minority oversampling technique for optimizing classification tasks in botnet and intrusion-detection-system datasets," *Appl. Sci.*, vol. 10, no. 3, 2020, doi: 10.3390/app10030794.
[28] D. Mualfah, W. Fadila, and R. Firdaus, "Teknik SMOTE untuk Mengatasi Imbalance Data pada Deteksi Penyakit Stroke Menggunakan Algoritma Random Forest," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 3, no. 2, pp. 107–113, 2022, doi: 10.37859/coscitech.v3i2.3912.
[29] M. Riyadh, B. J. Ali, and D. R. Alshibani, "IDS-MIU: an Intrusion Detection System Based on Machine Learning Techniques for Mixed Type, Incomplete, and Uncertain Data Set," *Int. J. Intell. Eng. Syst.*, vol. 14, no. 3, pp. 493–502, 2021, doi: 10.22266/ijies2021.0630.41.
[30] A. R. Salehi and M. Khedmati, "A cluster-based SMOTE both-sampling (CSBBoost) ensemble algorithm for classifying imbalanced data," *Sci. Rep.*, vol. 14, no. 1, pp. 1–18, 2024, doi: 10.1038/s41598-024-55598-1.
[31] M. Nassef, "Boosting Intrusion Detection Against DDoS Attacks Using a Feature Engineering-Based Fine-Tuned XGBoost Model," *Int. J. Semant. Web Inf. Syst.*, vol. 21, no. 1, pp. 1–39, 2025, doi: 10.4018/IJSWIS.383062.
[32] K. Kurniabudi, A. Harris, V. Veronica, and E. Yanti, "Optimizing Attack Detection for High Dimensionality and Imbalanced Data with SMOTE, Chi-Square and Random Forest Classifier," *IJICS (International J. Informatics Comput. Sci.*, vol. 6, no. 1, p. 1, 2022, doi: 10.30865/ijics.v6i1.3890.