ANALISIS PERBANDINGAN RANDOM FOREST DAN XGBOOST PADA DATASET IMBALANCED UNTUK KLASIFIKASI SERANGAN SIBER BERBASIS NETWORK TRAFFIC

Ulva Khairunnisa, Leony Santika, Vindira Yusefani, Fathoni
Fakultas Ilmu Komputer, Program Studi Sistem Informasi, Universitas Sriwijaya
Jl. Raya Palembang - Prabumulih No.KM. 32 Indralaya, Indonesia
09031282328101@student.unsri.ac.id

ABSTRAK

Keamanan siber menjadi isu penting seiring meningkatnya penggunaan infrastruktur digital yang rentan terhadap berbagai serangan. Permasalahan utama dalam klasifikasi serangan siber adalah ketidakseimbangan data (*imbalanced dataset)* yang menyebabkan model cenderung bias terhadap kelas mayoritas. Penelitian ini bertujuan untuk membandingkan performa algoritma *Random Forest* dan *XGBoost* dalam mengklasifikasikan serangan siber berbasis *network traffic* pada dataset yang tidak seimbang. Metode yang digunakan meliputi praproses data, *encoding* fitur, serta penerapan SMOTE pada data latih untuk mengatasi ketidakseimbangan kelas, dengan evaluasi menggunakan k-f*old cross-validation* dan metrik akurasi, *precision*, *recall*, dan F1-*score*. Hasil penelitian menunjukkan bahwa *XGBoost* memiliki performa lebih unggul dengan akurasi 95,85%, *precision* 49,26%, *recall* 57,25%, dan F1-*score* 52,76%, dibandingkan *Random Forest* yang hanya mencapai akurasi 89,33% dan F1-score 23,24%. Temuan ini menunjukkan bahwa *XGBoost* lebih efektif dan *robust* dalam menangani klasifikasi pada *dataset imbalanced*, khususnya dalam mendeteksi kelas minoritas berupa serangan siber.

Kata kunci : *Random Forest, XGBoost, Imbalanced Dataset, Network Traffic, Klasifikasi Serangan Siber, SMOTE.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital di berbagai sektor, seperti bisnis, pemerintahan, dan layanan publik [1]. Seiring dengan meningkatnya ketergantungan terhadap infrastruktur digital, ancaman keamanan siber juga mengalami peningkatan baik dari segi jumlah maupun kompleksitas [2]. Berbagai jenis serangan seperti *malware, phishing*, dan intrusi jaringan dapat menyebabkan kerugian yang signifikan, baik secara finansial maupun terhadap keamanan data. Oleh karena itu, keberadaan sistem keamanan jaringan seperti *Intrusion Detection System* (IDS) menjadi sangat penting untuk mendeteksi aktivitas mencurigakan secara cepat dan akurat [3]. Dalam perkembangannya, pendekatan berbasis *machine learning* banyak dimanfaatkan karena mampu mengidentifikasi pola serangan secara otomatis dari data dalam jumlah besar [4].

Meskipun demikian, proses klasifikasi serangan siber pada data *network traffic* masih menghadapi tantangan yang signifikan, terutama terkait dengan ketidakseimbangan distribusi data (*imbalanced dataset*). Pada umumnya, jumlah data normal jauh lebih dominan dibandingkan data serangan, sehingga model klasifikasi cenderung bias terhadap kelas mayoritas dan mengabaikan kelas minoritas yang justru lebih penting untuk dideteksi. Kondisi ini menyebabkan penurunan kemampuan model dalam mengidentifikasi serangan secara akurat. Selain itu, tingginya volume dan kompleksitas data jaringan juga membuat proses analisis manual menjadi tidak efektif, sehingga diperlukan metode komputasi yang mampu melakukan klasifikasi secara otomatis dan efisien [5].

Berbagai penelitian sebelumnya telah mengkaji penggunaan algoritma *machine learning* seperti *Decision Tree, Support Vector Machine, Random Forest*, dan *XGBoost* dalam mendeteksi serangan jaringan. Algoritma *ensemble* seperti *Random Forest* dan *XGBoost* dikenal memiliki performa yang baik dalam meningkatkan akurasi melalui kombinasi beberapa model prediktif serta mampu menangani data berukuran besar [6]. Selain itu, *XGBoost* juga dilaporkan memiliki efisiensi komputasi yang lebih tinggi dalam beberapa kasus klasifikasi berbasis network flow [7]. Namun demikian, masih terdapat keterbatasan dalam penelitian sebelumnya, khususnya dalam konteks penanganan dataset yang memiliki tingkat ketidakseimbangan kelas yang tinggi. Beberapa studi menunjukkan bahwa meskipun model mampu mencapai akurasi yang tinggi, performa dalam mendeteksi kelas minoritas masih rendah, yang ditunjukkan oleh nilai *recall* dan F1-*score* yang kurang optimal [8]. Hal ini menunjukkan bahwa akurasi saja tidak cukup untuk mengevaluasi performa model pada dataset yang tidak seimbang.

Selain itu, penelitian yang secara khusus membandingkan performa *Random Forest* dan *XGBoost* pada dataset *network traffic* yang bersifat *imbalanced* dengan pendekatan penanganan ketidakseimbangan data masih relatif terbatas [9]. Padahal, pendekatan berbasis *ensemble learning* memiliki potensi untuk menghasilkan model yang lebih robust terhadap dominasi kelas mayoritas dibandingkan algoritma tunggal [10]. Oleh karena itu,

diperlukan evaluasi yang lebih komprehensif dengan menggunakan metrik yang sensitif terhadap ketidakseimbangan data seperti *precision, recall,* dan F1-*score* [11].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis dan membandingkan performa algoritma *Random Forest* dan *XGBoost* dalam mengklasifikasikan serangan siber pada dataset network traffic yang bersifat *imbalanced.* Untuk mengatasi masalah ketidakseimbangan data, penelitian ini menerapkan teknik SMOTE pada data latih, serta menggunakan k-*fold cross-validation* dalam proses evaluasi model. Hasil penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai kemampuan kedua algoritma dalam menangani ketidakseimbangan data, serta memberikan kontribusi dalam pengembangan sistem deteksi intrusi berbasis machine learning yang lebih efektif dan andal.

2. TINJAUAN PUSTAKA

2.1. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) merupakan sistem yang dirancang untuk memantau dan menganalisis lalu lintas jaringan guna mendeteksi aktivitas yang mencurigakan atau berbahaya. IDS bekerja dengan cara mengamati pola trafik jaringan dan membandingkannya dengan basis data serangan yang telah diketahui maupun dengan perilaku normal jaringan. Terdapat dua pendekatan utama dalam IDS, yaitu *signature-based detection* yang mendeteksi berdasarkan pola serangan yang sudah diketahui, dan *anomaly-based detection* yang mendeteksi penyimpangan dari perilaku normal jaringan . Pendekatan berbasis machine learning semakin banyak dikembangkan untuk meningkatkan kemampuan deteksi secara otomatis.

2.2. Imbalanced Dataset

Imbalanced dataset adalah kondisi di mana distribusi kelas dalam sebuah dataset tidak merata secara signifikan. Dalam konteks keamanan jaringan, kelas data normal biasanya mendominasi dibandingkan kelas serangan. Ketidakseimbangan ini menyebabkan model machine learning cenderung bias ke arah kelas mayoritas dan mengabaikan kelas minoritas yang sebenarnya lebih penting untuk dideteksi. Teknik penanganan *imbalanced dataset* yang umum digunakan antara lain *oversampling* seperti SMOTE (*Synthetic Minority Over-sampling Technique*), *undersampling*, dan kombinasi keduanya [5]. SMOTE bekerja dengan membuat sampel sintetis dari kelas minoritas berdasarkan interpolasi antar sampel yang ada.

2.3. Algoritma Random Forest

Random Forest merupakan algoritma *ensemble learning* berbasis pohon keputusan *(decision tree)* yang menggunakan teknik *bagging* untuk membangun sejumlah pohon secara paralel. Setiap pohon dilatih menggunakan subset data yang dipilih secara acak dengan pengembalian (*bootstrap sampling*), dan prediksi akhir ditentukan berdasarkan *voting* mayoritas dari seluruh pohon. Kelebihan *Random Forest* antara lain kemampuannya dalam menangani data berdimensi tinggi, tahan terhadap overfitting, dan mampu mengestimasi pentingnya setiap fitur (*feature importance*). Algoritma ini juga efektif dalam menangani berbagai jenis data dan memiliki performa yang stabil pada berbagai kasus klasifikasi [10].

2.4. Algoritma XGBoost

XGBoost (*Extreme Gradient Boosting*) adalah algoritma *ensemble learning* berbasis g*radient boosting* yang membangun pohon keputusan secara sekuensial. Setiap pohon baru dibangun untuk mengoreksi kesalahan dari pohon sebelumnya menggunakan gradien dari fungsi loss. XGBoost dikenal karena efisiensi komputasinya yang tinggi berkat penggunaan teknik regularisasi L1 dan L2 untuk mencegah overfitting, serta kemampuannya menangani nilai yang hilang (*missing values*) secara otomatis. Dibandingkan dengan metode *boosting* lainnya, XGBoost memiliki kecepatan komputasi yang lebih baik karena memanfaatkan pemrosesan paralel dan optimasi memori [7]. Algoritma ini telah terbukti unggul dalam berbagai kompetisi *machine learning* dan kasus klasifikasi data nyata.

2.5. Metrik Evaluasi pada Imbalanced Dataset

Evaluasi model pada *imbalanced dataset* tidak cukup hanya menggunakan akurasi (*accuracy*), karena nilai akurasi yang tinggi dapat dicapai hanya dengan memprediksi semua sampel sebagai kelas mayoritas. Metrik yang lebih tepat digunakan mencakup *precision, recall,* dan F1-*score*. *Precision* mengukur proporsi prediksi positif yang benar, recall mengukur kemampuan model dalam mendeteksi seluruh sampel positif, dan F1-*score* merupakan rata-rata harmonik dari *precision* dan *recall* [6]. Selain itu, *confusion matrix* digunakan untuk memvisualisasikan distribusi prediksi benar dan salah.

2.6. Penelitian Terdahulu

Beberapa penelitian sebelumnya telah mengkaji penerapan algoritma *machine learning* dalam mendeteksi dan mengklasifikasikan serangan siber berbasis *network traffic*. Sun menyatakan bahwa ancaman keamanan siber terus berkembang seiring meningkatnya ketergantungan terhadap infrastruktur digital, sehingga diperlukan pendekatan deteksi yang semakin adaptif dan otomatis [2]. Sejalan dengan hal tersebut, Liu et al. melakukan kajian komprehensif terhadap teknologi deteksi anomali jaringan berbasis machine learning dan menyimpulkan bahwa pendekatan tersebut mampu mengidentifikasi pola serangan secara lebih efektif dibandingkan metode konvensional [4].

Dalam konteks penggunaan algoritma *ensemble*, Estupiñán et al. menerapkan Random Forest dan XGBoost untuk mendeteksi serangan DDoS berbasis

HTTP pada jaringan SDN, dengan hasil Random Forest mencapai akurasi tertinggi sebesar 99,99% dan XGBoost sebesar 99,97% menggunakan NTL-Dataset [9]. Sementara itu, Kunku et al. menggunakan kedua algoritma tersebut untuk mendeteksi dan mengklasifikasikan serangan ransomware, di mana XGBoost menghasilkan akurasi 99,61% dan Random Forest sebesar 99,70% pada dataset Kaggle [7]. Onyebueke et al. juga membandingkan XGBoost dan Random Forest pada dataset KDD untuk sistem deteksi intrusi jaringan, meskipun akurasi XGBoost mencapai 99%, nilai recall hanya sebesar 69% dan F1-score 70%, yang mengindikasikan kelemahan model dalam mendeteksi kelas minoritas berupa serangan [8].

Terkait penanganan ketidakseimbangan data, Bagui dan Li meneliti berbagai teknik resampling pada dataset deteksi intrusi jaringan dan menemukan bahwa penerapan SMOTE secara signifikan meningkatkan kemampuan model dalam mendeteksi kelas minoritas [5]. Sameer et al. mengembangkan kerangka deteksi intrusi dengan mengintegrasikan SMOTE-ENN bersama Random Forest dan XGBoost, dan membuktikan bahwa kombinasi tersebut menghasilkan performa yang lebih stabil dibandingkan tanpa penanganan imbalanced [10]. Shanmugam et al. melakukan evaluasi menyeluruh terhadap berbagai pendekatan machine learning dalam mengatasi ketidakseimbangan kelas pada sistem deteksi intrusi dan menekankan pentingnya penggunaan metrik seperti precision, recall, dan F1-score sebagai indikator yang lebih representatif [11]. Senada dengan itu, Abdelkhalek dan Mashaly mengusulkan pendekatan gabungan antara data resampling dan deep learning untuk mengatasi masalah class imbalance pada sistem deteksi intrusi jaringan, dan menunjukkan bahwa strategi tersebut mampu meningkatkan performa deteksi pada kelas yang jumlahnya lebih sedikit [6].

Berdasarkan kajian terhadap penelitian-penelitian di atas, dapat disimpulkan bahwa meskipun Random Forest dan XGBoost telah banyak digunakan dalam klasifikasi serangan siber dengan hasil yang menjanjikan, perbandingan performa keduanya secara spesifik pada dataset network traffic yang bersifat imbalanced dengan penerapan SMOTE masih relatif terbatas. Penelitian ini hadir untuk mengisi celah tersebut dengan melakukan analisis komparatif yang lebih terstruktur menggunakan dataset *Cybersecurity Threat Detection Dataset* dari Kaggle.

3. METODE PENELITIAN

Penelitian ini merupakan penelitian eksperimental dengan pendekatan kuantitatif dengan metode eksperimen.Tujuannya untuk membandingkan kinerja Random Forest dan XGBoost dalam klasifikasi serangan siber pada dataset *network traffic* yang bersifat *imbalanced.* Seluruh tahapan penelitian, mulai dari preprocessing data, pemodelan, hingga evaluasi model, diimplementasikan menggunakan Altair AI Studio atau yang sebelumnya bernama Rapidminer sebagai tools utama. Altair AI Studio dipilih karena menyediakan antarmuka visual berbasis drag-and-drop yang memudahkan implementasi algoritma machine learning secara terintegrasi dalam satu platform tanpa memerlukan pemrograman secara manual.

3.1. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah metode sekunder, yaitu dengan memanfaatkan dataset publik yang telah tersedia. Dataset yang digunakan adalah dataset *Cybersecurity Threat Detection Dataset* diperoleh dari platform Kaggle. Dataset ini dipilih karena menyediakan data terkait aktivitas jaringan yang telah dilengkapi dengan label klasifikasi serangan siber, sehingga dapat digunakan untuk proses pembelajaran model klasifikasi.

Tabel 1. Dataset Cybersecurity Threat Detection Dataset

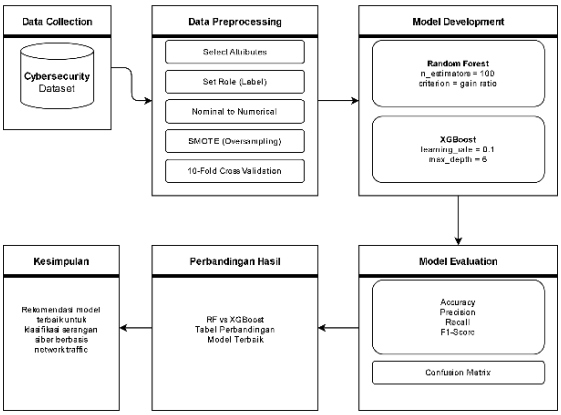
src_port	dst_port	protocol	bytes_sent	bytes_recieved	is_internal_traffic	label
25167	443	TCP	3592	1081	TRUE	0
33599	25	ICMP	4640	9110	FALSE	0
80	213	TCP	3150	11715	FALSE	1
47914	677	UDP	317	733	TRUE	1
12283	21	TCP	17289	35727	FALSE	0

Tabel tersebut menunjukkan contoh dataset *Cybersecurity Threat Detection* yang berisi sejumlah fitur yang merepresentasikan karakteristik aktivitas jaringan, yaitu src_port, dst_port, protocol, bytes_sent, bytes_received, dan is_internal_traffic, serta label yang mengindikasikan kategori serangan dan aktivitas normal. Dataset ini memiliki distribusi kelas yang tidak seimbang (*imbalanced*) dengan jumlah data normal sebesar 9.600 *record* (96%) dan data serangan sebesar 400 record (4%), sehingga relevan digunakan dalam penelitian yang berfokus pada penanganan ketidakseimbangan data dalam klasifikasi serangan siber.

3.2. Alur Penelitian

Metodologi penelitian ini dirancang secara terstruktur menggunakan pendekatan berbasis data mining dan pembelajaran mesin untuk membandingkan performa algoritma *Random Forest* dan *XGBoost* dalam klasifikasi serangan siber pada dataset yang memiliki ketidakseimbangan kelas.

Tahapan metodologi penelitian divisualisasikan pada gambar 1.



Gambar 1. Alur Penelitian

3.3. Praproses Data

Tahap praproses data dilakukan untuk mempersiapkan dataset agar siap digunakan dalam proses pemodelan klasifikasi. Praproses yang tepat sangat penting karena kualitas data secara langsung mempengaruhi performa model *machine learning* yang dihasilkan [4].

Seleksi atribut dilakukan untuk mengeliminasi kolom yang tidak relevan terhadap karakteristik *network traffic*, yaitu timestamp, src_ip, dst_ip, url, dan user_agent. Kolom-kolom tersebut memiliki kardinalitas yang sangat tinggi sehingga tidak memberikan informasi yang bermakna bagi model klasifikasi dan berpotensi menambah kompleksitas komputasi secara tidak perlu.

Penetapan label (*Set Role*) dilakukan dengan menetapkan atribut label sebagai target klasifikasi, di mana nilai 0 merepresentasikan aktivitas normal (*benign*) dan nilai 1 merepresentasikan aktivitas serangan (*attack*).

Konversi atribut nominal ke numerik dilakukan menggunakan dua operator *Nominal to Numerical* secara terpisah. Atribut protocol dikonversi menggunakan metode *dummy coding* sehingga menghasilkan tiga kolom biner baru, yaitu protocol_TCP, protocol_UDP, dan protocol_ICMP. Sementara itu, atribut is_internal_traffic dikonversi menggunakan metode *unique integers* sehingga nilai *False* dan *True* masing-masing direpresentasikan sebagai 0 dan 1. Proses encoding ini diperlukan karena algoritma *Random Forest* dan *XGBoost* hanya dapat memproses data dalam format numerik [12].

3.4. Penanganan *Imbalanced* Dataset dengan SMOTE

Teknik SMOTE diterapkan hanya pada data latih untuk menghindari kebocoran informasi (*data leakage*) ke data uji. SMOTE bekerja dengan membuat sampel sintetis pada kelas minoritas berdasarkan interpolasi linier antara sampel yang ada dan k-tetangganya (*k-nearest neighbors*). Dalam penelitian ini digunakan parameter k=5 sebagai jumlah tetangga terdekat. Penerapan SMOTE menghasilkan distribusi kelas yang lebih seimbang sehingga model dapat belajar secara optimal dari kedua kelas.

3.5 Validasi Hasil Penelitian

Validasi model dalam penelitian ini menggunakan metode *k-fold cross-validation* dalam pembagian dataset untuk proses pelatihan dan pengujian model. Metode ini dipilih karena mampu memberikan estimasi performa yang lebih stabil dan tidak bergantung pada satu pembagian data tertentu, sehingga hasil evaluasi lebih representatif dan mengurangi risiko overfitting. Metrik evaluasi yang digunakan meliputi: (1) Akurasi, yaitu proporsi prediksi yang benar dari seluruh prediksi; (2) *Precision*, yaitu proporsi prediksi kelas serangan yang benar dari seluruh prediksi serangan; (3*) Recall*, yaitu kemampuan model dalam mendeteksi seluruh serangan yang sebenarnya; (4) *F1-score*, yaitu rata-rata harmonik dari *precision* dan *recall*; serta (5) *Confusion Matrix* untuk visualisasi distribusi hasil prediksi. Selain itu, hasil evaluasi juga dibandingkan dengan penelitian-penelitian sebelumnya yang menggunakan pendekatan serupa pada dataset NSL-KDD untuk melihat sejauh mana peningkatan performa yang dicapai oleh framework yang diusulkan [11].

4. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil evaluasi model *Random Forest* dan *XGBoost* dalam mengklasifikasikan serangan siber pada dataset *Cybersecurity Threat Detection* yang bersifat *imbalanced*, dilanjutkan dengan analisis perbandingan antara kedua algoritma serta pembahasan terhadap penelitian-penelitian terdahulu.

4.1. Hasil Evaluasi Random Forests

Pengujian algoritma *Random Forest* menggunakan *k-fold cross-validation* dengan penerapan SMOTE pada data latih menghasilkan evaluasi sebagaimana disajikan pada Tabel 2.

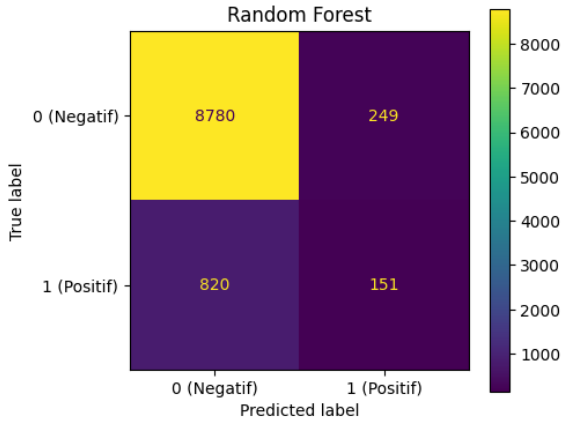
Tabel 2. Hasil evaluasi random forest

Metrik	Nilai (%)	Std Dev	Micro Avg (%)
Accuracy	89.33	±3.58	89.33
Precision	16.93	±4.56	15.79
Recall	38.50	±6.89	38.50
F1-Score	23.24	±5.44	22.40

Berdasarkan Tabel 2, algoritma *Random Forest* memperoleh akurasi sebesar 89,33%. Meskipun angka akurasi ini tergolong cukup tinggi, nilai tersebut tidak merepresentasikan kemampuan model yang sesungguhnya dalam mendeteksi serangan, mengingat distribusi kelas dataset sangat tidak seimbang (96:4). Hal ini terbukti dari rendahnya nilai *precision* sebesar 16,93% dan *F1-score* 23,24%, yang secara langsung mengindikasikan bahwa model masih kesulitan dalam

mengidentifikasi kelas serangan (kelas minoritas) secara tepat dan konsisten. Nilai recall sebesar 38,50% menunjukkan bahwa dari seluruh serangan yang sebenarnya terjadi, hanya sekitar 38,5% yang berhasil terdeteksi oleh model.

Tingginya *standard deviation* pada metrik *recall* (±6,89%) dan *F1-score* (±5,44%) juga mengindikasikan bahwa performa *Random Forest* tidak stabil dan bervariasi cukup signifikan antar fold. Kondisi ini menunjukkan bahwa meskipun SMOTE diterapkan, algoritma *Random Forest* tetap mengalami kesulitan dalam mempertahankan konsistensi deteksi kelas minoritas pada rasio ketidakseimbangan yang ekstrem sebesar 24:1.



Gambar 2. Gambar hasil evaluasi random forest

Berdasarkan gambar 2, dapat dilihat bahwa model *Random Forest* berhasil mengklasifikasikan 8780 data normal (*true negative*) dengan benar, namun masih terdapat 249 data normal yang salah diklasifikasikan sebagai serangan (*false positive*). Pada kelas serangan (positif), model hanya mampu mendeteksi 151 data serangan dengan benar (true positive), sementara 820 data serangan lainnya tidak terdeteksi dan diklasifikasikan sebagai normal (false negative).

Jumlah *false negative* yang jauh lebih besar dibandingkan *true positive* menunjukkan bahwa model memiliki kelemahan signifikan dalam mendeteksi serangan, yang sejalan dengan rendahnya nilai recall. Selain itu, perbandingan antara *false positive* dan *true positive* juga mengindikasikan bahwa prediksi serangan yang dihasilkan model masih kurang akurat, sehingga berdampak pada rendahnya nilai precision dan *F1-score.*

Secara keseluruhan, *confusion matrix* ini memperjelas bahwa meskipun model memiliki kemampuan yang baik dalam mengenali data normal, performanya dalam mengidentifikasi kelas serangan (kelas minoritas) masih sangat terbatas, terutama akibat ketidakseimbangan distribusi data.

4.2. XGBoost

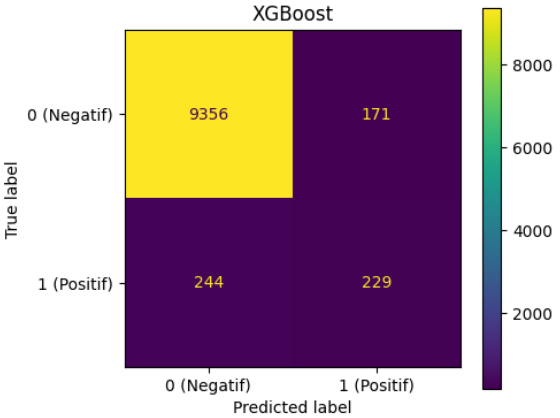
Pengujian algoritma XGBoost dengan konfigurasi yang sama menghasilkan performa yang lebih baik dibandingkan *Random Forest*, sebagaimana ditampilkan pada Tabel 3.

Tabel 3. Hasil evaluasi XGBoost

Metrik	Nilai (%)	Std Dev	Micro Avg (%)
Accuracy	95.85	±0.88	95.85
Precision	49.26	±8.98	48.41
Recall	57.25	±6.61	57.25
F1-Score	52.76	±7.53	52.46

Berdasarkan Tabel 3, XGBoost mencapai akurasi tertinggi sebesar 95,85% dengan *precision* 49,26%, *recall* 57,25%, dan *F1-score* 52,76%. Dibandingkan dengan *Random Forest*, seluruh metrik evaluasi XGBoost menunjukkan peningkatan yang signifikan. Peningkatan paling mencolok terjadi pada *precision* (+32,33 poin persentase) dan *F1-score* (+29,52 poin persentase), yang mencerminkan kemampuan XGBoost dalam mendeteksi serangan dengan lebih presisi sekaligus mengurangi *false positive*. Nilai *recall* sebesar 57,25% pun secara substansial lebih tinggi dibandingkan *Random Forest*, yang berarti lebih banyak serangan nyata yang berhasil terdeteksi.

Selain performa yang lebih tinggi, XGBoost juga menunjukkan kestabilan yang lebih baik, terlihat dari *standard deviation* akurasi yang sangat kecil (±0,88%), jauh lebih kecil dibandingkan *Random Forest* (±3,58%). Hal ini mengindikasikan bahwa XGBoost menghasilkan prediksi yang lebih konsisten di seluruh *fold* validasi. Keunggulan XGBoost ini sejalan dengan karakteristik algoritma *gradient boosting* yang secara iteratif memperbaiki kesalahan prediksi sebelumnya, sehingga lebih efektif dalam menangani pola data minoritas yang sulit dikenali.



Gambar 3. Gambar hasil evaluasi XGBoost

Berdasarkan gambar 3, model XGBoost berhasil mengklasifikasikan 9356 data normal *(true negative*) dengan benar dan hanya menghasilkan 171 kesalahan klasifikasi sebagai serangan (*false positive*). Pada kelas serangan (positif), model mampu mendeteksi 229 data serangan dengan benar (*true positive*), sementara 244 data serangan lainnya masih tidak terdeteksi (*false negative*).

Jumlah *true positive* yang lebih tinggi serta penurunan *false negative* dibandingkan Random Forest menunjukkan bahwa XGBoost memiliki kemampuan yang lebih baik dalam mendeteksi serangan. Selain itu, jumlah *false positive* yang relatif lebih kecil juga menunjukkan bahwa prediksi serangan yang dihasilkan lebih akurat, yang sejalan dengan peningkatan nilai precision.

Secara keseluruhan, *confusion matrix* ini memperkuat hasil evaluasi sebelumnya bahwa XGBoost tidak hanya lebih efektif dalam mengenali data normal, tetapi juga значительно lebih baik dalam mengidentifikasi kelas serangan (kelas minoritas), sehingga menghasilkan performa yang lebih seimbang antara *precision* dan *recall*.

4.3. Hasil Perbandingan

Tabel 4. Perbandingan Performa Random Forest dan XGBoost

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Random Forest	3,73	0,68	1,62	0,94
XGBoost	95.89	48.83	2,39	52.70

Berdasarkan Tabel 4, XGBoost secara konsisten mengungguli *Random Forest* pada semua metrik. Perbedaan yang paling signifikan terlihat pada *precision* (49,26% vs 16,93%) dan *F1-score* (52,76% vs 23,24%). Keunggulan ini dapat dikaitkan dengan mekanisme *gradient boosting* pada XGBoost yang memungkinkan model belajar secara sekuensial dari kesalahan sebelumnya, sehingga lebih adaptif terhadap pola data yang tidak seimbang. Sebaliknya, *Random Forest* yang menggunakan teknik *bagging* dan *majority voting* cenderung lebih dominan diarahkan oleh kelas mayoritas (normal), sehingga kemampuannya dalam mendeteksi kelas minoritas (serangan) menjadi terbatas meskipun SMOTE telah diterapkan.

Aspek kestabilan model juga menjadi keunggulan XGBoost. Nilai *standard deviation* pada akurasi XGBoost (±0,88%) menunjukkan variasi yang sangat kecil dibandingkan *Random Forest* (±3,58%), mengindikasikan bahwa XGBoost menghasilkan performa yang lebih andal dan tidak terlalu bergantung pada distribusi data pada setiap *fold*. Dari perspektif sistem deteksi intrusi (IDS), keandalan model yang tinggi sangat krusial karena kegagalan mendeteksi serangan (*false negative*) dapat berdampak jauh lebih besar dibandingkan peringatan palsu (*false positive*).

4.4. Perbandingan dengan Penelitian Terdahulu

Hasil penelitian ini berbeda secara signifikan dibandingkan beberapa penelitian terdahulu, terutama yang dilakukan oleh Estupiñán et al. [6] dan Kunku et al. [7]. Estupiñán et al. melaporkan akurasi *Random Forest* sebesar 99,99% dan XGBoost 99,97% pada NTL-Dataset untuk deteksi serangan DDoS di jaringan SDN. Demikian pula, Kunku et al. mencatat akurasi *Random Forest* 99,70% dan XGBoost 99,61% untuk klasifikasi ransomware pada dataset Kaggle. Perbedaan performa yang mencolok ini tidak serta-merta mengindikasikan kelemahan pada algoritma, melainkan lebih mencerminkan perbedaan karakteristik dataset yang digunakan. Dataset pada kedua penelitian tersebut memiliki distribusi kelas yang jauh lebih seimbang, sehingga kedua algoritma dapat belajar secara optimal dari seluruh kelas tanpa bias dominasi kelas mayoritas.

Penelitian yang paling relevan untuk dibandingkan adalah Onyebueke et al. [8], yang juga menggunakan XGBoost pada dataset yang bersifat *imbalanced* (KDD Dataset). Meskipun Onyebueke et al. melaporkan akurasi XGBoost mencapai 99%, nilai *recall* hanya sebesar 69% dan *F1-score* 70%, yang mengindikasikan kelemahan serupa dalam mendeteksi kelas minoritas. Fenomena ini mengkonfirmasi gap yang diidentifikasi dalam penelitian ini, yaitu bahwa akurasi tinggi pada dataset *imbalanced* belum tentu mencerminkan kemampuan deteksi serangan yang baik. XGBoost pada penelitian ini memperoleh *recall* sebesar 57,25% dan *F1-score* 52,76%, yang lebih rendah dari Onyebueke et al. Hal ini dapat dikaitkan dengan perbedaan tingkat ketidakseimbangan kelas: rasio imbalance pada penelitian ini jauh lebih ekstrem (96:4 atau 24:1) dibandingkan dataset KDD yang digunakan Onyebueke et al., sehingga tantangan deteksi kelas minoritas menjadi lebih besar.

Temuan penelitian ini juga memiliki keterkaitan dengan penelitian Sameer et al. [10] yang mengintegrasikan SMOTE-ENN bersama *Random Forest* dan XGBoost, menghasilkan performa yang lebih stabil dibandingkan tanpa penanganan *imbalanced*. Penelitian ini menggunakan SMOTE standar (bukan SMOTE-ENN) dan menunjukkan hasil yang konsisten bahwa penanganan *imbalanced dataset* memang meningkatkan kemampuan deteksi kelas minoritas, namun masih terdapat ruang peningkatan yang signifikan, khususnya pada nilai *precision* dan *F1-score*. Penggunaan teknik resampling yang lebih canggih seperti SMOTE-ENN atau strategi *cost-sensitive learning* berpotensi menghasilkan performa yang lebih baik pada dataset dengan rasio ketidakseimbangan ekstrem seperti yang digunakan dalam penelitian ini.

Secara keseluruhan, hasil penelitian ini mengisi celah yang telah diidentifikasi dalam kajian literatur: perbandingan performa *Random Forest* dan XGBoost secara spesifik pada dataset *network traffic* yang memiliki tingkat ketidakseimbangan kelas sangat tinggi (rasio 24:1). Temuan ini menegaskan bahwa XGBoost merupakan pilihan yang lebih tepat dibandingkan *Random Forest* untuk skenario klasifikasi serangan siber dengan kondisi data *imbalanced*, sekaligus menunjukkan bahwa penggunaan metrik evaluasi yang komprehensif (*precision, recall, F1-score*) tidak hanya akurasi sangat penting dalam menilai efektivitas model pada dataset yang tidak seimbang.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa algoritma XGBoost memiliki performa yang lebih unggul dibandingkan *Random Forest* dalam klasifikasi serangan siber pada dataset yang tidak seimbang, dengan nilai akurasi, *precision*, *recall*, dan *F1-score* yang lebih tinggi serta kestabilan model yang lebih baik. Meskipun penerapan SMOTE mampu meningkatkan deteksi kelas minoritas, metode tersebut belum sepenuhnya mengatasi ketidakseimbangan data yang ekstrem, sehingga penggunaan metrik evaluasi seperti *precision*, *recall*, dan *F1-score* menjadi sangat penting dibandingkan hanya mengandalkan akurasi. Oleh karena itu, penelitian selanjutnya disarankan untuk menggunakan teknik penanganan data imbalanced yang lebih canggih seperti SMOTE-ENN atau ADASYN, menerapkan pendekatan cost-sensitive learning, melakukan hyperparameter tuning, serta menguji model pada dataset lain agar hasil penelitian lebih general dan optimal, serta dapat dikembangkan ke dalam sistem deteksi intrusi berbasis machine learning secara real-time.

DAFTAR PUSTAKA

[1] J. J. P. Latupeirissa, N. L. Y. Dewi, I. K. R. Prayana, M. B. Srikandi, S. A. Ramadiansyah, and I. B. G. A. Y. Pramana, "Transforming Public Service Delivery: A Comprehensive Review of Digitization Initiatives," *Sustain.* , vol. 16, no. 7, 2024, doi: 10.3390/su16072818.

[2] X. Sun, "The Current Status and Challenges of Cybersecurity Risks," *Internet Things Cloud Comput.*, vol. 12, no. 1, pp. 10–16, 2024, doi: 10.11648/j.iotcc.20241201.12.

[3] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, pp. 1–29, 2021, doi: 10.1002/ett.4150.

[4] R. Liu, J. Shi, X. Chen, and C. Lu, "Network anomaly detection and security defense technology based on machine learning: A review," *Comput. Electr. Eng.*, vol. 119, no. PA, p. 109581, 2024, doi: 10.1016/j.compeleceng.2024.109581.

[5] S. Bagui and K. Li, "Resampling imbalanced data for network intrusion detection datasets," *J. Big Data*, vol. 8, no. 1, 2021, doi: 10.1186/s40537-020-00390-x.

[6] A. Abdelkhalek and M. Mashaly, *Addressing the class imbalance problem in network intrusion detection systems using data resampling and deep learning*, vol. 79, no. 10. Springer US, 2023. doi: 10.1007/s11227-023-05073-x.

[7] K. Kunku, A. N. K. Zaman, and K. Roy, "Ransomware Detection and Classification using Machine Learning," *2023 IEEE Symp. Ser. Comput. Intell. SSCI 2023*, pp. 862–866, 2023, doi: 10.1109/SSCI52147.2023.10371924.

[8] A. E. Onyebueke, A. David, and S. Munu, "Network Intrusion Detection SystemUsing XGBoost and Random ForestAlgorithms," *Orig. Res. Artic. Onyebueke al.; Asian J. Pure Appl. Math*, vol. 5, no. 1, pp. 321–335, 2023, [Online]. Available: www.kaggle.com

[9] E. P. Estupiñán Cuesta, J. C. Martínez Quintero, and J. D. Avilés Palma, "DDoS Attacks Detection in SDN Through Network Traffic Feature Selection and Machine Learning Models," *Telecom*, vol. 6, no. 3, 2025, doi: 10.3390/telecom6030069.

[10] T. Sameer, J. Rashmi, B. Khushi, M. Khushi, R. Rahul, and J. Prachi, "Enhanced intrusion detection framework: Integrating SMOTE-ENN with random forest and XGBoost," *i-manager's J. Inf. Technol.*, vol. 13, no. 3, p. 19, 2024, doi: 10.26634/jit.13.3.21454.

[11] V. Shanmugam, R. Razavi-Far, and E. Hallaji, "Addressing Class Imbalance in Intrusion Detection: A Comprehensive Evaluation of Machine Learning Approaches," *Electron.*, vol. 14, no. 1, pp. 1–19, 2025, doi: 10.3390/electronics14010069.

[12] W. ZEWDU and G. CHEN, "Impact of Categorical Feature Encoding on Machine Learning Based Shear Strength Prediction," 2025, doi: 10.12783/shm2025/37535.