JETISH: Journal of Education Technology Information Social Sciences and Health
E-ISSN: 2964-2507 P-ISSN: 2964-819X
Vol. 5 No. 2 September 2026

Implementasi Sistem Deteksi Serangan Port Scanning pada Jaringan Komputer Dengan Pendekatan XGboost

Felix John Pardamean Hutabarat[1] Dedy Kiswanto[2] Tegas Ramadhan[3] Muhammad Dzaki Arjun[4]
Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[1,2,3,4]
Email: hutabaratfelix8.4233250008@mhs.unimed.ac.id[1] dedykiswanto@unimed.ac.id[2] kuy410zml@gmail.com[3] mdzakiarjunzaki@gmail.com[4]

Abstrak
Serangan *Port Scanning* merupakan salah satu tahapan awal yang umum dilakukan oleh penyerang untuk mengidentifikasi layanan dan celah keamanan pada suatu sistem jaringan. Oleh karena itu, diperlukan mekanisme deteksi yang mampu mengenali aktivitas tersebut secara cepat dan akurat. Penelitian ini bertujuan mengimplementasikan dan mengevaluasi sistem deteksi serangan *Port Scanning* menggunakan algoritma Extreme Gradient Boosting (XGBoost). Dataset yang digunakan adalah CIC-IDS2017, khususnya berkas *Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX*. Tahapan penelitian meliputi seleksi fitur bertahap, *Exploratory Data Analysis* (EDA), *preprocessing*, serta pelatihan dan evaluasi model menggunakan metode *Stratified 5-Fold Cross-Validation*. Proses seleksi fitur berhasil mereduksi 85 fitur awal menjadi 8 fitur prediktif utama. Setelah penghapusan data duplikat, dataset terdiri atas 110.364 observasi unik dengan rasio ketidakseimbangan kelas sekitar 66:1. Hasil pengujian menunjukkan bahwa model XGBoost mencapai akurasi sebesar 99,89%, *precision* 94,00%, *recall* 99,27%, dan *F1-score* 96,56% untuk kelas *PortScan*. Analisis *learning curve* menunjukkan kemampuan generalisasi yang baik tanpa indikasi *overfitting* yang signifikan. Selain itu, analisis *eXplainable AI* menggunakan SHAP mengidentifikasi bahwa fitur *Total Length of Fwd Packets*, *PSH Flag Count*, dan *Fwd Packet Length Min* merupakan faktor yang paling berpengaruh dalam proses klasifikasi. Hasil penelitian menunjukkan bahwa pendekatan XGBoost efektif dalam mendeteksi serangan *Port Scanning* dengan tingkat akurasi tinggi serta mampu memberikan interpretasi terhadap proses pengambilan keputusan model.
Kata Kunci: *Intrusion Detection, Machine Learning, Network Security, Port Scanning, XGBoost*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa dampak signifikan terhadap berbagai sektor kehidupan, mulai dari pemerintahan, pendidikan, bisnis, hingga layanan publik. Seiring dengan perkembangan ini, menjaga keamanan jaringan komputer menjadi komponen yang sangat penting untuk diperhatikan. Salah satu jenis ancaman yang paling sering terjadi dalam jaringan komputer adalah serangan port scanning. Ini merupakan teknik yang digunakan untuk menemukan layanan jaringan yang tersedia pada suatu perangkat dengan memeriksa status port Transmission Control Protocol (TCP) (I. M. Razzanda & M. Koprawi, 2024). Teknik ini sering dimanfaatkan oleh peretas untuk menemukan celah keamanan yang bisa dieksploitasi, seperti pencurian data, penyisipan malware, hingga akses tidak sah ke sistem (M. R. Rusydianto et al., 2023; M. Z. Rifqi et al., 2021).

Serangan port scanning sering kali sulit terdeteksi secara manual karena aktivitasnya menyerupai lalu lintas jaringan normal, terutama dalam jaringan dengan volume data tinggi. Selain itu, alat seperti Nmap atau Netcut yang biasa digunakan dalam proses ini memungkinkan pelaku untuk secara sistematis mengidentifikasi port-port terbuka yang dapat dimanfaatkan sebagai pintu masuk ke dalam sistem (E. Kristianto et al., 2024). Oleh karena itu, diperlukan

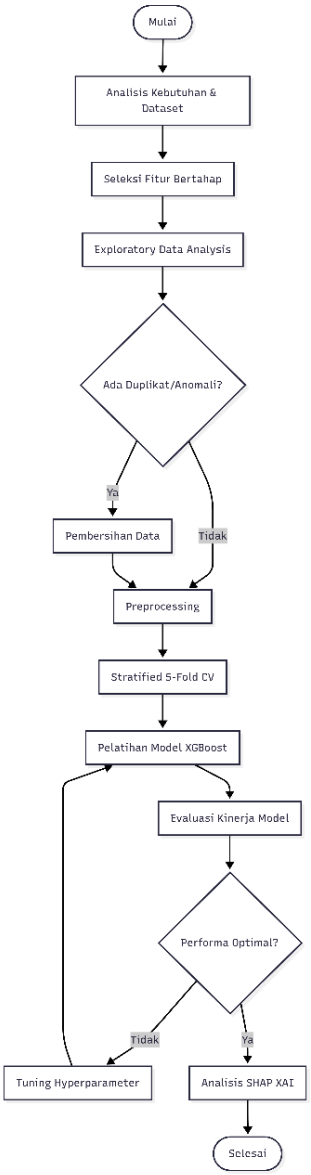
sistem deteksi otomatis yang dapat mengenali pola serangan secara cepat dan akurat, bahkan ketika data yang dihadapi tidak seimbang atau tersembunyi dalam lalu lintas jaringan normal.

Implementasi algoritma pembelajaran mesin (machine learning) merupakan salah satu cara yang efektif untuk membangun sistem deteksi tersebut. Pendekatan machine learning dinilai mampu mengenali pola lalu lintas jaringan secara otomatis dan beradaptasi terhadap karakteristik serangan yang semakin kompleks dibandingkan metode konvensional (D. Kiswanto et al., 2025). Salah satu algoritma yang cukup terkenal dan terbukti ampuh dalam berbagai tugas klasifikasi dan deteksi anomali adalah XGBoost (Extreme Gradient Boosting) (A. M. A. Rudianto et al., 2025; S. E. H. Yulianti et al., 2022). XGBoost merupakan pengembangan dari metode Gradient Boosting Decision Tree (GBDT) yang memiliki keunggulan dalam kecepatan pelatihan, ketahanan terhadap data besar, serta akurasi prediksi yang tinggi (A. Nugroho et al., 2023; D. S. Utomo & M. Lestari, 2024). Tidak seperti model Random Forest yang menggunakan pendekatan bagging, XGBoost menggunakan teknik gradient boosting yang bekerja dengan meningkatkan performa dari iterasi sebelumnya (M. G. A. Rianto et al., 2024).

Algoritma ini mampu mengenali pola serangan dalam data jaringan, bahkan dalam kasus-kasus kompleks seperti data yang tidak seimbang atau zero-day attack (R. Yunanto & U. Budiyanto, 2024; T. R. Karin et al., 2024). Beberapa studi sebelumnya menunjukkan bahwa penggunaan XGBoost dalam sistem deteksi intrusi jaringan menghasilkan akurasi yang tinggi, seperti pada pengujian dengan dataset UNSW-NB15 dan NSL-KDD yang mencatatkan akurasi hingga lebih dari 90% (F. Riza, 2023; G. Pradita & A. Pramono, 2024). Selain itu, penerapan metode seleksi fitur berbasis XGBoost juga mampu meningkatkan performa sistem secara signifikan dalam deteksi serangan (M. Hernowo & E. Sugiharti, 2024).

Dengan menerapkan sistem deteksi berbasis XGBoost, diharapkan dapat meningkatkan kemampuan pengawasan jaringan serta mempercepat proses identifikasi terhadap aktivitas mencurigakan. Hal ini terutama penting bagi organisasi yang bergantung pada sistem jaringan untuk menjaga integritas data dan mengurangi risiko keamanan yang dapat merugikan secara operasional maupun finansial (Nuroji, 2023). Penelitian ini berfokus pada pengembangan sistem deteksi serangan port scanning secara otomatis menggunakan algoritma XGBoost dengan memanfaatkan dataset CIC-IDS2017, khususnya berkas Port Scan. Permasalahan yang diangkat meliputi bagaimana memanfaatkan data tersebut secara akurat melalui pendekatan machine learning, bagaimana proses pemilihan fitur, pembersihan data, dan transformasi nilai memengaruhi kualitas model, serta seberapa efektif algoritma XGBoost dalam mengklasifikasikan aktivitas jaringan sebagai serangan atau lalu lintas normal. Untuk menjawab permasalahan tersebut, penelitian ini bertujuan mengimplementasikan sistem deteksi berbasis XGBoost, melakukan seleksi fitur dan preprocessing untuk menghasilkan dataset yang relevan, serta mengevaluasi performa model melalui metrik klasifikasi seperti akurasi, presisi, dan recall.

METODE PENELITIAN



Gambar 1. Flowchart Penelitian

Penelitian ini dirancang menggunakan metodologi *Research and Development* (R&D) yang bertujuan untuk menghasilkan dan menguji sebuah produk berupa sistem deteksi serangan *Port Scanning*. Tahap awal penelitian meliputi analisis kebutuhan untuk mengidentifikasi urgensi masalah keamanan jaringan, yang kemudian dilanjutkan dengan pemilihan dan pengambilan dataset publik CIC-IDS2017 sebagai bahan utama. Setelah dataset diperoleh, direncanakan tahap *Exploratory Data Analysis* (EDA) untuk melakukan investigasi awal terhadap karakteristik data, termasuk distribusi kelas dan potensi adanya anomali. Berdasarkan temuan dari EDA, dirancang tahap pra-pemrosesan data (*preprocessing*) yang mencakup rencana penanganan data duplikat, nilai yang hilang atau tidak valid, serta melakukan transformasi label target dari kategorikal ke numerik menggunakan *Label Encoding* agar dapat diproses oleh algoritma.

Pada tahap pengembangan, penelitian ini akan membangun model klasifikasi menggunakan algoritma XGBoost. Proses ini diawali dengan menentukan konfigurasi *hyperparameter* dasar sebagai fondasi awal model. Untuk mengevaluasi kinerja model secara

objektif dan andal, penelitian ini akan menerapkan skema pengujian *Stratified K-Fold Cross-Validation* dengan 5-fold (*k=5*). Pemilihan metode ini bertujuan untuk memastikan proses evaluasi yang stabil dan adil dengan menjaga proporsi kelas yang seimbang pada setiap iterasi pengujian. Tahap evaluasi akhir dirancang secara komprehensif untuk mengukur efektivitas sistem. Kinerja model akan dianalisis melalui metrik standar seperti akurasi, presisi, dan *recall* dari *classification report* serta visualisasi *confusion matrix*. Selain itu, direncanakan pula analisis diagnostik menggunakan kurva belajar (*learning curve*) untuk menginspeksi stabilitas model dan analisis SHAP untuk menginterpretasikan logika internal serta faktor-faktor yang paling memengaruhi keputusan model.

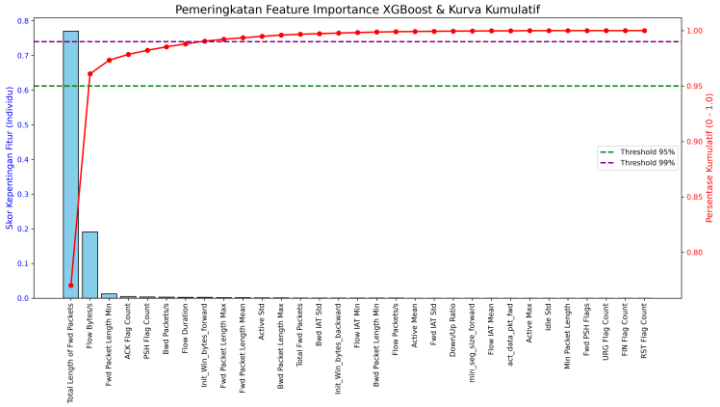
HASIL PENELITIAN DAN PEMBAHASAN

Hasil penelitian

Sumber Dataset dan Seleksi Fitur

Penelitian ini menggunakan dataset publik CIC-IDS2017 yang dikembangkan oleh *Canadian Institute for Cybersecurity (CIC)*. Fokus penelitian ini yakni pada satu berkas spesifik, yaitu "*Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX*". Pada bentuk mentahnya, dataset ini merangkum 286.467 rekaman aktivitas jaringan yang mendeskripsikan profil lalu lintas normal (BENIGN) serta aktivitas anomali berupa serangan PortScan. Setiap rekaman direpresentasikan oleh 85 fitur statistik dan temporal yang diekstraksi dari aliran paket jaringan. Mengingat tingginya dimensi data yang berpotensi memicu beban komputasi berlebih dan fenomena *curse of dimensionality*, penelitian ini mengimplementasikan pendekatan seleksi fitur berjenjang (*multi-stage feature selection*) untuk mereduksi ruang dimensi dan mengisolasi prediktor yang paling relevan. Tahap awal reduksi dimensi dilakukan melalui penyaringan berbasis pengetahuan domain keamanan siber (domain-based filtering). Pada tahap ini, fitur yang dianggap terlalu spesifik, seperti *Destination Port*, dihapus bersama anomali struktural dataset, misalnya duplikasi nama kolom. Penghapusan atribut port tujuan bertujuan mengurangi risiko overfitting, yaitu ketika model hanya menghafal port yang menjadi target serangan pada data pelatihan.

Setelah penyaringan berbasis domain, dilakukan penyaringan statistik (statistical filtering) untuk menghapus fitur yang tidak informatif atau redundan. Tahap ini diawali dengan eliminasi fitur zero-variance, yaitu atribut yang memiliki nilai konstan pada seluruh data. Selanjutnya, dilakukan analisis korelasi Pearson untuk mengidentifikasi multikolinearitas antar fitur. Pasangan fitur dengan nilai korelasi absolut di atas 0,90 dievaluasi, kemudian salah satu fitur dihapus guna mengurangi redundansi dan mencegah bias pada model XGBoost. Sebagai tahap akhir seleksi fitur, atribut yang lolos penyaringan statistik dievaluasi menggunakan Tree-Based Feature Importance. Model dasar XGBoost dilatih untuk menghitung nilai *Gain*, yang menggambarkan kontribusi setiap fitur dalam membedakan kelas target. Nilai tersebut kemudian diurutkan secara kumulatif dan divisualisasikan melalui Kurva Pareto. Dengan ambang kumulatif sebesar 99%, analisis menunjukkan adanya elbow effect, yaitu sebagian besar kemampuan prediksi model hanya berasal dari sejumlah kecil fitur yang paling dominan.



Gambar 2. Pemeringkatan Feature Importance XGBoost dan Kurva Kumulatif

Berdasarkan analisis Kurva Pareto, persentase kepentingan kumulatif mencapai ambang 99% pada fitur ke-8. Hasil ini menunjukkan bahwa delapan fitur teratas telah merepresentasikan hampir seluruh informasi yang diperlukan model untuk mendeteksi serangan, sementara fitur lainnya hanya memberikan kontribusi yang sangat kecil (<1%). Oleh karena itu, hanya delapan fitur tersebut yang dipertahankan sebagai fitur akhir dan digunakan sebagai dasar dalam proses pelatihan model klasifikasi.

Tabel 1. Fitur yang digunakan

No	Nama Fitur	Keterangan (Fungsi Fitur)
1	Total Length of Fwd Packets	Total volume ukuran data (byte) dari paket yang dikirim ke arah depan (*forward*).
2	PSH Flag Count	Jumlah paket dengan flag PUSH yang menginstruksikan sistem untuk segera memproses data.
3	Fwd Packet Length Min	Ukuran terkecil dari paket jaringan yang dikirim ke arah depan.
4	Init_Win_bytes_forward	Ukuran awal *window* (buffer) TCP yang dikirim pada arah *forward*.
5	Flow Duration	Durasi waktu spesifik dari paket pertama hingga paket terakhir dalam satu aliran.
6	Bwd Packets/s	Kecepatan transmisi jumlah paket per detik yang diterima pada arah mundur (*backward*).
7	ACK Flag Count	Jumlah paket yang memuat flag Acknowledgment (konfirmasi penerimaan data).
8	Flow Bytes/s	Kecepatan transmisi volume data (byte) per detik secara keseluruhan dalam aliran.

EDA (Exploratory Data Analysis)

Pada tahap Exploratory Data Analysis (EDA), dilakukan pemeriksaan terhadap struktur dan kualitas dataset. Hasil analisis menunjukkan adanya redundansi data yang signifikan setelah fitur *Destination Port* dihapus. Penghapusan fitur tersebut menyebabkan sejumlah besar paket serangan *Port Scanning* yang sebelumnya dibedakan oleh port tujuan menjadi memiliki karakteristik statistik yang identik.

Untuk mengatasi permasalahan tersebut, dilakukan proses penghapusan data duplikat menggunakan fungsi *.drop_duplicates()*, sehingga jumlah observasi berkurang menjadi 110.364 data unik. Setelah proses pembersihan, distribusi kelas menunjukkan kondisi ketidakseimbangan kelas yang tinggi (class imbalance), dengan kelas BENIGN berjumlah 108.722 sampel (98,51%) dan kelas PortScan sebanyak 1.642 sampel (1,49%). Rasio ketidakseimbangan sekitar 66:1 ini mencerminkan karakteristik lalu lintas jaringan yang didominasi oleh aktivitas normal serta menjadi tantangan penting dalam proses klasifikasi, sehingga memerlukan penyesuaian pada parameter model untuk mengurangi potensi bias terhadap kelas mayoritas.

Preprocessing

Setelah proses penghapusan duplikasi, tahap *preprocessing* dilanjutkan dengan penanganan nilai tak terhingga (*infinity*). Nilai tersebut terlebih dahulu dikonversi menjadi NaN (*Not a Number*), kemudian digantikan dengan nilai nol (*zero-filling*) untuk memastikan seluruh fitur dapat diproses secara optimal oleh algoritma pembelajaran mesin. Selanjutnya, variabel target ditransformasikan menggunakan Label Encoding, dengan memetakan kelas BENIGN menjadi nilai 0 dan kelas PortScan menjadi nilai 1. Transformasi ini diperlukan agar label kategorikal dapat digunakan dalam proses pelatihan model klasifikasi.

Stratified K-Fold Cross-Validation

Untuk memperoleh evaluasi kinerja model yang robust dan objektif, penelitian ini menggunakan metode Stratified 5-Fold Cross-Validation. Pendekatan stratifikasi diterapkan untuk memastikan proporsi kelas target tetap terjaga pada setiap *fold*, sehingga distribusi kelas PortScan yang berjumlah jauh lebih sedikit dibandingkan kelas BENIGN tetap terwakili secara proporsional dalam proses pelatihan maupun pengujian. Selain itu, untuk menangani ketidakseimbangan kelas yang tinggi, model XGBoost dikonfigurasi menggunakan parameter scale_pos_weight. Nilai parameter ini dihitung secara terpisah pada setiap *fold* berdasarkan rasio jumlah sampel kelas mayoritas terhadap kelas minoritas pada data pelatihan. Pendekatan tersebut memberikan bobot yang lebih besar pada kesalahan klasifikasi kelas PortScan, sehingga model lebih sensitif terhadap deteksi serangan. Perhitungan bobot yang dilakukan secara independen pada setiap *fold* juga membantu mencegah data leakage, karena informasi dari data pengujian tidak digunakan dalam proses pelatihan model.

Evaluasi Kinerja Model

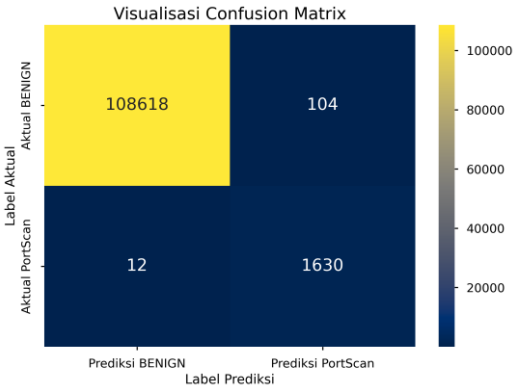
Berdasarkan hasil agregasi Stratified 5-Fold Cross-Validation, model XGBoost memperoleh akurasi sebesar 99,89%. Kinerja model dalam mendeteksi kelas PortScan ditunjukkan oleh nilai recall sebesar 99,27%, yang menunjukkan bahwa sebagian besar aktivitas pemindaian berhasil teridentifikasi dengan benar. Selain itu, model mencapai precision sebesar 94,00% dan F1-score sebesar 96,56%, mengindikasikan keseimbangan yang baik antara kemampuan deteksi dan tingkat kesalahan prediksi.

Laporan Klasifikasi (Agregat dari semua Fold):

	precision	recall	f1-score	support
BENIGN (0)	0.9999	0.9990	0.9995	108722
PortScan (1)	0.9400	0.9927	0.9656	1642
accuracy			0.9989	110364
macro avg	0.9700	0.9959	0.9826	110364
weighted avg	0.9990	0.9989	0.9990	110364

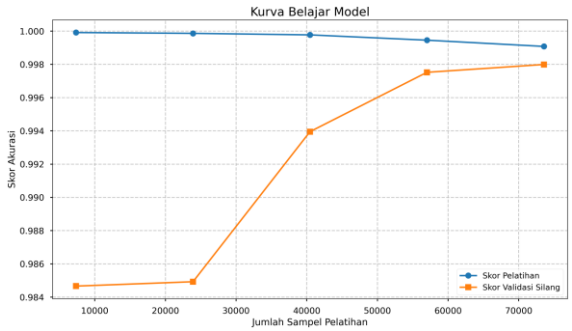
Gambar 3. Laporan Klasifikasi

Hasil tersebut didukung oleh analisis confusion matrix, yang menunjukkan bahwa dari total 110.364 observasi, model berhasil mengklasifikasikan 108.618 sampel BENIGN dan 1.630 sampel PortScan dengan benar. Kesalahan klasifikasi relatif rendah, ditunjukkan oleh 104 kasus false positive dan 12 kasus false negative. Temuan ini mengindikasikan bahwa model mampu mempertahankan tingkat deteksi yang tinggi sekaligus meminimalkan alarm palsu.



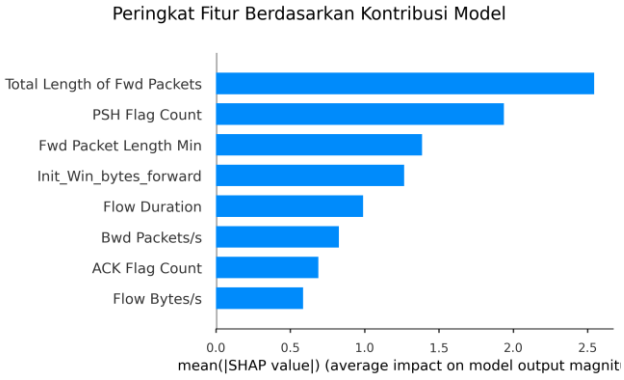
Gambar 4. ***Confusion Matrix***

Evaluasi lebih lanjut menggunakan learning curve menunjukkan adanya konvergensi antara skor pelatihan dan skor validasi seiring bertambahnya jumlah data pelatihan. Pola ini mengindikasikan bahwa model memiliki kemampuan generalisasi yang baik dan tidak menunjukkan gejala overfitting maupun underfitting yang signifikan.



Gambar 5. ***Learning Curve***

Untuk meningkatkan interpretabilitas model, dilakukan analisis eXplainable AI (XAI) menggunakan metode SHAP (SHapley Additive exPlanations). Analisis dilakukan terhadap sampel acak sebanyak 5.000 observasi guna menjaga efisiensi komputasi sekaligus mempertahankan representativitas distribusi data. Hasil SHAP Bar Plot menunjukkan bahwa fitur Total Length of Fwd Packets merupakan faktor yang paling berpengaruh dalam proses klasifikasi, diikuti oleh PSH Flag Count dan Fwd Packet Length Min. Temuan ini mengindikasikan bahwa model banyak memanfaatkan karakteristik terkait volume paket yang dikirim serta pola penggunaan flag PSH dalam membedakan lalu lintas normal dan aktivitas Port Scanning.



Gambar 6. ***SHAP Bar Plot***

Hasil analisis SHAP menunjukkan bahwa Total Length of Fwd Packets merupakan fitur dengan kontribusi terbesar dalam proses pengambilan keputusan model. Temuan ini mengindikasikan bahwa akumulasi volume data yang dikirim dari sumber ke target (*forward direction*) menjadi salah satu karakteristik utama yang digunakan model untuk membedakan aktivitas *Port Scanning* dari lalu lintas normal. Fitur PSH Flag Count menempati urutan kedua dalam tingkat kepentingan, yang menunjukkan bahwa frekuensi penggunaan flag PSH (Push) juga berperan penting dalam proses klasifikasi. Hal ini mengindikasikan bahwa pola penggunaan flag TCP tertentu dapat menjadi indikator yang relevan dalam mengidentifikasi aktivitas pemindaian jaringan. Selain itu, fitur Fwd Packet Length Min, Init_Win_bytes_forward, dan Flow Duration turut memberikan kontribusi yang signifikan. Ketiga fitur tersebut merepresentasikan karakteristik ukuran paket minimum, ukuran jendela awal koneksi, serta durasi aliran paket yang terjadi selama komunikasi jaringan.

KESIMPULAN

Penelitian ini berhasil mengembangkan sistem deteksi serangan *Port Scanning* menggunakan algoritma XGBoost pada dataset CIC-IDS2017. Melalui proses seleksi fitur bertahap, jumlah fitur berhasil direduksi dari 85 atribut menjadi 8 fitur utama yang tetap mampu mempertahankan hampir seluruh informasi prediktif yang relevan. Hasil evaluasi menggunakan Stratified 5-Fold Cross-Validation menunjukkan bahwa model mencapai akurasi sebesar 99,89%, dengan precision 94,00%, recall 99,27%, dan F1-score 96,56% untuk kelas *PortScan*. Nilai tersebut menunjukkan bahwa model mampu mendeteksi aktivitas pemindaian jaringan dengan tingkat kesalahan yang rendah meskipun menghadapi kondisi ketidakseimbangan kelas yang tinggi.

Analisis *learning curve* mengindikasikan bahwa model memiliki kemampuan generalisasi yang baik tanpa gejala *overfitting* maupun *underfitting* yang signifikan. Selain itu, penerapan metode SHAP memberikan interpretasi yang lebih transparan terhadap proses pengambilan keputusan model. Hasil analisis menunjukkan bahwa fitur Total Length of Fwd Packets, PSH Flag Count, dan Fwd Packet Length Min merupakan faktor yang paling berpengaruh dalam proses klasifikasi. Temuan ini menunjukkan bahwa deteksi serangan *Port Scanning* lebih banyak didasarkan pada karakteristik perilaku lalu lintas jaringan, seperti volume transmisi data dan pola penggunaan protokol, sehingga model yang dihasilkan tidak hanya memiliki kinerja yang tinggi tetapi juga dapat diinterpretasikan dengan baik.

Meskipun model yang dihasilkan menunjukkan kinerja yang sangat tinggi, terdapat beberapa area yang dapat dikembangkan untuk penelitian di masa depan. Pertama, penelitian selanjutnya dapat mencoba menerapkan teknik *hyperparameter tuning* yang lebih sistematis, seperti menggunakan *Grid Search* atau *Random Search*, untuk mencari kombinasi parameter XGBoost yang lebih optimal dan berpotensi meningkatkan nilai presisi pada kelas serangan. Kedua, mengingat keberhasilan model ini, disarankan untuk menguji efektivitasnya pada jenis serangan jaringan lain yang lebih kompleks, seperti DDoS atau serangan *zero-day*, untuk mengukur fleksibilitas dan skalabilitasnya. Terakhir, penelitian masa depan dapat berfokus pada implementasi model ini ke dalam sebuah sistem deteksi intrusi (*Intrusion Detection System*) yang berjalan secara *real-time* untuk memberikan perlindungan proaktif pada lingkungan jaringan yang sesungguhnya.

DAFTAR PUSTAKA

A. M. A. Rudianto, E. S. Pramukantoro, & D. Kurnianingtyas. (2025). Implementasi Sistem Deteksi Anomali pada Jaringan Komputer dengan Pendekatan XGBoost dan Data SNMP. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *9*(2).

A. Nugroho, B. Nugroho, & S. Prasetyo. (2023). Perbandingan Algoritma Naive Bayes, Decision Tree, dan XGBoost dalam Deteksi Intrusi Jaringan. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *7*(1), 42–50.

D. Kiswanto, F. Ramadhani, N. M. Surbakti, & N. A. Nasution. (2025). Pengembangan dan Implementasi Sistem Deteksi Serangan DDoS Berbasis Algoritma Random Forest. *Bulletin of Information Technology (BIT)*, *6*(3), 247–256.

D. S. Utomo, & M. Lestari. (2024). Deteksi Serangan Jaringan Menggunakan Algoritma XGBoost dengan Oversampling SMOTE. *Jurnal Teknologi Dan Sistem Komputer*, *12*(2), 155–162.

E. Kristianto, A. A. Waskita, & T. Thoyyibah. (2024). Analisis Kinerja Sistem Deteksi Intrusi Jaringan Internet of Things Berbasis Metode Ensemble. *Jurnal Ilmu Komputer*, *2*(2), 251–260.

F. Riza. (2023). Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging. *Jurnal Sistim Informasi Dan Teknologi*, *5*(1), 7–15.

G. Pradita, & A. Pramono. (2024). Implementasi Monitoring Keamanan Jaringan pada Server Ubuntu Menggunakan Snort Intrusion Detection Prevention System (IDPS) dan Telegram Bot sebagai Media Notifikasi di PT SS Utama. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(4), 5827–5835.

I. M. Razzanda, & M. Koprawi. (2024). Implementasi IDS dan IPS terhadap Serangan TCP Port Scanning dan ICMP Flooding. *The Indonesian Journal of Computer Science*, *13*(4).

M. G. A. Rianto, A. L. Prasasti, & A. Novianty. (2024). Implementasi Model XGBoost untuk Prediksi Jumlah Transaksi dan Total Pendapatan di Jaringan Restoran CV Balibul. *Jurnal Nasional SAINS Dan TEKNIK*, *2*(2), 43–46.

M. Hernowo, & E. Sugiharti. (2024). XGBoost Algorithm on Intrusion Detection System in Detecting Network Intrusions. *INNOVATIVE: Journal of Social Science Research*, *4*(1), 10572–10588.

M. R. Rusydianto, E. Budiman, & H. J. Setyadi. (2023). Implementasi Teknik Hacking Web Server dengan Port Scanning dalam Sistem Operasi Kali Linux. *Prosiding Seminar Nasional Ilmu Komputer Dan Teknologi Informasi*.

M. Z. Rifqi, M. Syahroni, & Misriana. (2021). Implementasi Sistem Keamanan Jaringan pada Mikrotik RB-951 Menggunakan Metode Port Knocking. *Jurnal TEKTRO*, *5*(2), 165–170.

Nuroji. (2023). Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan Komputer sebagai Pencegahan Serangan Port-Scanning. *Journal of Data Science and Information System (DIMIS)*, *1*(2), 41–49.

R. Yunanto, & U. Budiyanto. (2024). Implementasi XGBoost dan SMOTE untuk Meningkatkan Deteksi Transaksi Fraud di Industri Jasa Keuangan. *Jurnal Pendidikan Dan Teknologi Indonesia (JPTI)*, *4*(11), 525–535.

S. E. H. Yulianti, O. Soesanto, & Y. Sukmawaty. (2022). Penerapan Metode Extreme Gradient Boosting (XGBOOST) pada Klasifikasi Nasabah Kartu Kredit. *Journal of Mathematics: Theory and Applications (JOMTA)*, *4*(1), 20–21.

T. R. Karin, R. R. Sani, F. A. Zami, & A. Rohmani. (2024). Enhancing Bank Customer Protection Against Phishing Attacks Through XGBoost-Based Feature Analysis. *TRANSMISI: Jurnal Ilmiah Teknik Elektro*, *26*(3), 114–121.