

Pengembangan Sistem Deteksi Serangan Siber Berbasis *Machine Learning* pada Jaringan Lokal dan Log Aplikasi Web Institusi Pendidikan

¹Raja Sakti Arief Daulay, ²Nur Tri Julia, ³Muhammad Dekar, ⁴Dinda Widyastika, ⁵Rifki Qodri

^{1*,2,5}Pendidikan Teknologi Informasi dan Pendidikan Matematika

STKIP Pangeran Antasari, Medan, Indonesia

^{3,4}Pendidikan Guru Sekolah Dasar, Universitas Battuta, Medan, Indonesia

*Korespondensi: rajasaktidaulay@gmail.com

Submit : 21 Agust 2026 | Diterima : 18 Okt 2026 | Terbit : 20 Okt 2026

ABSTRACT

Cybersecurity in local network infrastructures of academic institutions currently faces increasingly complex challenges alongside high dependency on digital architectures like academic information systems (SIKAD). Cyber attacks such as SQL injection, brute force login, Distributed Denial of Service (DDoS), and zero-day threats are difficult to detect effectively using conventional rule-based (signature-based) systems. This study proposes a two-layer machine learning-based early warning architecture consisting of a network layer and an application layer that analyzes web application logs, and compares Random Forest, K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Decision Tree algorithms. To address class imbalance and high dimensionality, Synthetic Minority Oversampling Technique (SMOTE) and Information Gain-based feature selection were implemented. Supervised classification was evaluated on the NSL-KDD benchmark dataset, where Random Forest achieved the highest performance with 98.76% accuracy, 98.12% precision, 98.54% recall, and 98.33% F1-Score. Information Gain-based feature selection reduced the dimensions from 41 to the 20 most informative features and improved training time efficiency by 34%. For the application layer, a real university web server log (15,789 valid requests, 5 IP addresses, 57 active days) was analyzed as a case study. The log is unlabeled, so classification accuracy could not be measured; alarm rates and computational cost were evaluated instead. Two high-traffic days accounted for 51.2% of all requests, and, assuming the traffic was predominantly legitimate, a static threshold of 20 requests per minute per IP flagged 70.0% of the per-IP-minute windows on the busiest day, showing that legitimate academic traffic bursts can be mistaken for attacks. All models predicted in under 0.02 ms per record in batch mode and under 7 ms per single-record call on a 1-vCPU machine. These findings indicate the need for detectors trained on representative local academic traffic; labeled local data, such as SIKAD logs, are required to validate the proposed architecture end to end.

Keywords: Machine Learning; Cyberattack Detection; Network Security; Web Application Logs; Local Area Network.

ABSTRAK

Keamanan siber pada jaringan lokal institusi pendidikan saat ini menghadapi tantangan yang semakin kompleks seiring dengan tingginya ketergantungan terhadap infrastruktur digital seperti sistem informasi akademik (SIKAD). Serangan seperti SQL injection, brute force login, Distributed Denial of Service (DDoS), hingga ancaman zero-day sulit dideteksi secara efektif menggunakan sistem konvensional berbasis aturan (signature-based). Penelitian ini mengusulkan arsitektur peringatan dini dua lapis berbasis *Machine Learning* yang terdiri atas lapisan jaringan dan lapisan aplikasi yang menganalisis log aplikasi web, serta membandingkan algoritma Random Forest, K-Nearest Neighbor (KNN), Support Vector Machine (SVM), dan Decision Tree. Untuk mengatasi ketidakseimbangan kelas dan dimensi fitur yang tinggi, diimplementasikan Synthetic Minority Oversampling Technique (SMOTE) serta seleksi fitur berbasis Information Gain. Klasifikasi terawasi dievaluasi pada dataset benchmark NSL-KDD, dengan Random Forest mencapai performa terbaik: akurasi 98,76%, presisi 98,12%, recall 98,54%, dan F1-Score 98,33%. Seleksi fitur berbasis Information Gain mereduksi dimensi dari 41 menjadi 20 fitur paling informatif serta meningkatkan efisiensi waktu pelatihan sebesar 34%.

Pada lapisan aplikasi, log server web universitas yang nyata (15.789 entri valid, 5 alamat IP, 57 hari aktif) dianalisis sebagai studi kasus. Log tidak berlabel sehingga akurasi klasifikasi tidak dapat diukur; yang dievaluasi adalah tingkat alarm dan biaya komputasi. Dua hari lonjakan menyumbang 51,2% seluruh request dan, dengan asumsi trafik sebagian besar sah, ambang statis 20 request per menit per IP menandai 70,0% jendela IP-menit pada hari terpadat, yang menunjukkan bahwa lonjakan trafik akademik yang sah dapat disalahartikan sebagai serangan. Semua model memprediksi di bawah 0,02 ms per rekaman pada mode batch dan di bawah 7 ms per pemanggilan tunggal pada mesin 1 vCPU. Temuan ini menunjukkan perlunya detektor yang dilatih pada trafik akademik lokal yang representatif; data lokal berlabel, seperti log SIAKAD, diperlukan untuk memvalidasi arsitektur yang diusulkan secara menyeluruh.

Kata Kunci Machine Learning; Deteksi Serangan Siber; Keamanan Jaringan; Log Aplikasi Web; Jaringan Lokal.

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat telah mendorong berbagai institusi pendidikan, baik sekolah menengah maupun perguruan tinggi, untuk mengadopsi sistem informasi akademik berbasis digital secara luas. Sistem ini tidak hanya mempermudah proses administrasi dan manajemen data operasional harian, tetapi juga menjadi tulang punggung utama dalam penyelenggaraan berbagai layanan akademik penting, seperti pengisian Kartu Rencana Studi (KRS), penilaian hasil belajar mahasiswa, absensi, hingga pengelolaan data pribadi mahasiswa, dosen, serta tenaga kependidikan. Integrasi teknologi ini secara dramatis meningkatkan efisiensi operasional institusi pendidikan. Namun, seiring dengan semakin meningkatnya ketergantungan yang krusial terhadap infrastruktur digital ini, aspek keamanan data (cybersecurity) pada jaringan lokal institusi menjadi sangat mendesak dan mutlak untuk diperhatikan secara serius (Yin & Chen, 2023).

Lalu lintas data pada jaringan komputer institusi pendidikan membawa informasi yang sangat sensitif, termasuk data identitas pribadi, dokumen administrasi keuangan, dan arsip penilaian akademik yang rawan menjadi target serangan siber (Chandra dkk., 2025). Berdasarkan laporan resmi tahunan dari Badan Siber dan Sandi Negara (BSSN) pada tahun 2023, tercatat lebih dari 361 juta anomali lalu lintas (trafik) jaringan yang mengindikasikan aktivitas siber berbahaya di Indonesia (BSSN, 2023). Hal ini menunjukkan peningkatan ancaman siber yang sangat signifikan dari tahun-tahun sebelumnya (Setiyadi & Nikola, 2024). Beberapa bentuk serangan siber yang umum terjadi dan mengancam integritas jaringan lokal sekolah serta kampus antara lain Denial of Service (DoS), Distributed DoS (DDoS), Port Scanning, Brute Force login, SQL injection, phishing, hingga eksploitasi kerentanan keamanan sistem lainnya (Chandra dkk., 2025; Setiyadi & Nikola, 2024). Serangan-serangan ini berpotensi menyebabkan kebocoran data sensitif skala besar, manipulasi informasi akademik yang tidak sah, kerusakan reputasi institusi, hingga lumpuhnya sistem operasional secara total.

Sayangnya, sebagian besar institusi pendidikan saat ini belum memiliki sistem deteksi dini yang handal dan mandiri untuk mengenali serta merespons ancaman siber ini secara waktu-nyata (real-time). Sistem keamanan konvensional berbasis Intrusion Detection System (IDS) tradisional yang menggunakan pendekatan berbasis tanda (signature-based IDS) memiliki keterbatasan fundamental yang fatal (Setiyadi & Nikola, 2024). Sistem ini bekerja dengan mencocokkan tanda lalu lintas data dengan database pola serangan yang sudah diketahui sebelumnya (Buczak & Guven, 2016). Akibatnya, signature-based IDS tidak berdaya dan gagal mendeteksi jenis serangan baru (zero-day attacks) serta variasi serangan adaptif yang polanya belum terdaftar dalam basis data keamanan (Setiyadi & Nikola, 2024). Keterbatasan ini mendorong kebutuhan mendesak akan adanya sistem deteksi intrusi berbasis anomali (anomaly-based IDS) yang lebih dinamis, adaptif, dan cerdas.

Untuk mengatasi tantangan tersebut, teknologi *Machine Learning* (ML) menawarkan solusi inovatif dan adaptif dengan pendekatan berbasis data (data-driven approach) (Setiyadi & Nikola, 2024). Dengan kemampuannya yang mumpuni dalam menganalisis data lalu lintas jaringan berskala besar secara otomatis dan mempelajari pola aktivitas dari data historis, *Machine Learning* dapat melakukan generalisasi yang sangat akurat untuk mendeteksi anomali pada lalu lintas jaringan baru (Chandra dkk., 2025; Setiyadi & Nikola, 2024). Sejumlah penelitian terdahulu membuktikan keefektifan pemodelan *Machine Learning* dalam domain klasifikasi data keamanan jaringan yang kompleks dengan menggunakan berbagai algoritma, seperti Decision Tree, Random Forest, K-Nearest Neighbor, hingga arsitektur Deep Learning (Ahmed dkk., 2022;

Barkah dkk., 2023; Zhong, 2025) pada dataset benchmark seperti KDD Cup 1999 dan NSL-KDD (Tavallaee dkk., 2009; Setiyadi & Nikola, 2024).

Meskipun menawarkan potensi tinggi, penerapan *Machine Learning* pada data deteksi intrusi nyata menghadapi dua kendala utama: tingginya dimensi fitur lalu lintas data serta ketidakseimbangan kelas (class imbalance) yang ekstrim antara aktivitas normal dengan sampel serangan (Setiyadi & Nikola, 2024; Bagui & Li, 2021; Ahsan dkk., 2022). Jumlah sampel serangan minoritas seperti Remote to Local (R2L) dan User to Root (U2R) yang sangat sedikit di dalam dataset dapat menyebabkan bias klasifikasi yang signifikan ke arah kelas mayoritas (Normal/DoS), sehingga menurunkan performa deteksi ancaman kritis secara drastis (Setiyadi & Nikola, 2024). Oleh karena itu, diperlukan teknik pra-proses data yang canggih untuk mengatasi masalah tersebut sebelum melatih model klasifikasi.

Meskipun demikian, sebagian besar penelitian tersebut dievaluasi pada dataset benchmark umum yang dibangun dari lingkungan yang berbeda dari institusi pendidikan. Dataset seperti KDD'99 dan NSL-KDD dinilai sudah usang dan kurang merepresentasikan lalu lintas jaringan masa kini (Barkah dkk., 2023), serta tidak menangkap perilaku pengguna dan pola trafik khas lingkungan pendidikan; model yang dilatih pada data yang dikumpulkan dari jaringan kampus dilaporkan mencapai tingkat deteksi yang lebih tinggi daripada model yang dilatih pada dataset publik (Sindika dkk., 2025). Penelitian pada lingkungan kampus juga menunjukkan bahwa dimensi fitur yang tinggi, overfitting, dan ketidakseimbangan data menjadi kendala utama (Yin & Chen, 2023), dan seleksi fitur telah banyak digunakan untuk mengurangi beban komputasi (Sharma & Yadav, 2021; Barkah dkk., 2023).

Trafik sistem informasi akademik memiliki karakteristik yang berbeda dari trafik umum. Akses pengguna terkonsentrasi pada periode tertentu dalam kalender akademik, misalnya pengisian Kartu Rencana Studi (KRS), input nilai, dan pengumuman hasil studi, sehingga lonjakan permintaan dalam waktu singkat merupakan perilaku yang sah (flash crowd), bukan serangan. Lonjakan ini mirip dengan serangan DDoS lapisan aplikasi dan brute force pada tampilan permukaan, yaitu laju permintaan yang tinggi dan bersifat bursty, sehingga detektor berbasis ambang batas statis cenderung menghasilkan false positive pada masa KRS atau justru gagal mengenali serangan yang menyamar di dalam lonjakan tersebut. Studi deteksi DDoS pada layanan web melaporkan bahwa pembeda yang andal terletak pada interaksi beberapa fitur, seperti laju permintaan, keragaman alamat IP klien, dan komposisi respons galat, bukan pada satu fitur tunggal (Molnar & Sabodashko, 2025). Selain itu, institusi pendidikan dengan sumber daya TI terbatas umumnya tidak memiliki pusat operasi keamanan khusus, sehingga model deteksi perlu ringan, cepat, dan mudah diinterpretasikan oleh administrator. Log server web universitas yang dianalisis pada penelitian ini menguatkan hal tersebut: dua hari lonjakan menyumbang 51,2% dari seluruh request, dan satu alamat IP mengirim hingga 128 request dalam satu menit tanpa indikasi serangan yang dapat diverifikasi.

Karakteristik tersebut menjadi dasar pemilihan algoritma dalam penelitian ini. Random Forest dipilih sebagai model utama karena (1) data log akses dan fitur lalu lintas bersifat tabular dengan campuran fitur numerik dan kategorikal yang berinteraksi secara nonlinier, sehingga partisi berbasis pohon dapat menangkap interaksi tersebut tanpa transformasi yang kompleks (Molnar & Sabodashko, 2025); (2) sifat ensemble membuatnya relatif tahan terhadap noise dan overfitting pada data log yang tidak bersih; (3) biaya inferensinya diperkirakan lebih rendah daripada KNN yang harus menghitung jarak ke seluruh data latih, sehingga lebih sesuai untuk penapisan hampir waktu-nyata pada server dengan sumber daya terbatas, dan hal ini diuji melalui pengukuran waktu inferensi pada penelitian ini; serta (4) tingkat kepentingan fitur dapat diturunkan langsung sehingga hasilnya dapat diinterpretasikan oleh administrator. Perbandingan dengan KNN, SVM, dan Decision Tree tetap dilakukan karena tidak ada algoritma yang unggul secara universal; misalnya, pada dataset UNSW-NB15 Decision Tree justru mengungguli Random Forest dan KNN (Barkah dkk., 2023). Pendekatan studi komparatif seperti ini juga digunakan pada penelitian lain (Hesham dkk., 2024; Sayed dkk., 2024), tetapi pada data log aplikasi akademik lokal belum banyak dilakukan.

Berdasarkan uraian tersebut, sepengetahuan penulis terdapat tiga kesenjangan penelitian. Pertama, evaluasi model deteksi serangan didominasi dataset benchmark, sedangkan analisis log aplikasi web akademik yang nyata, yang memuat pola akses khas kegiatan akademik, jarang dilaporkan. Kedua, belum banyak kajian yang membedakan lonjakan trafik sah pada periode puncak akademik dari serangan, padahal keduanya sama-sama bercirikan laju permintaan tinggi. Ketiga, biaya komputasi inferensi jarang dijadikan kriteria pemilihan model untuk institusi dengan sumber daya TI terbatas.

Melalui penelitian ini, dikembangkan rancangan sistem peringatan dini serangan siber berbasis *Machine Learning* untuk institusi pendidikan yang terdiri atas dua lapisan deteksi, yaitu lapisan jaringan yang menganalisis fitur lalu lintas paket dan lapisan aplikasi yang menganalisis log aplikasi web. Kebaruan (novelty) penelitian ini terletak pada analisis empiris log server web akademik yang nyata untuk menunjukkan bahwa lonjakan trafik yang sah dapat memicu alarm detektor, serta pada pengukuran biaya komputasi inferensi sebagai kriteria pemilihan model; dataset benchmark NSL-KDD digunakan untuk mengevaluasi kinerja klasifikasi terawasi. Kontribusi utama penelitian ini meliputi: (1) karakterisasi trafik log server web universitas (15.789 entri valid) dan evaluasi tingkat alarm detektor berbasis ambang statis dan Isolation Forest pada hari normal dan hari lonjakan; (2) rancangan arsitektur peringatan dini dua lapis yang menggabungkan keluaran detektor aplikasi dan detektor jaringan melalui modul korelasi peringatan; (3) penerapan seleksi fitur berbasis Information Gain dan Synthetic Minority Oversampling Technique (SMOTE) pada NSL-KDD disertai analisis kontribusi fitur; serta (4) perbandingan Random Forest (RF), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), dan Decision Tree (DT) dari sisi waktu inferensi, serta RF, KNN, dan SVM dari sisi kinerja klasifikasi pada NSL-KDD.

METODE PENELITIAN

Penelitian ini dirancang sebagai penelitian kuantitatif dengan pendekatan eksperimental (Chandra dkk., 2025). Fokus utama eksperimen ini adalah mengimplementasikan, menguji, dan mengevaluasi kinerja beberapa algoritma *Machine Learning* dalam mendeteksi serangan siber berbasis data lalu lintas paket jaringan komputer lokal dan log aktivitas sistem informasi akademik institusi pendidikan (Chandra dkk., 2025; Setiyadi & Nikola, 2024). Penelitian ini dilakukan secara sistematis melalui lima tahapan utama: akuisisi data, praproses dan pelabelan data, rekayasa fitur (seleksi fitur), pemodelan klasifikasi, serta evaluasi kinerja model (Chandra dkk., 2025). Arsitektur yang mengintegrasikan keluaran lapisan aplikasi (log SIAKAD) dan lapisan jaringan dalam satu pipeline peringatan dini dijelaskan pada subbab Arsitektur Integrasi Sistem Peringatan Dini.



Gambar 1 Skema Model Deteksi Siber

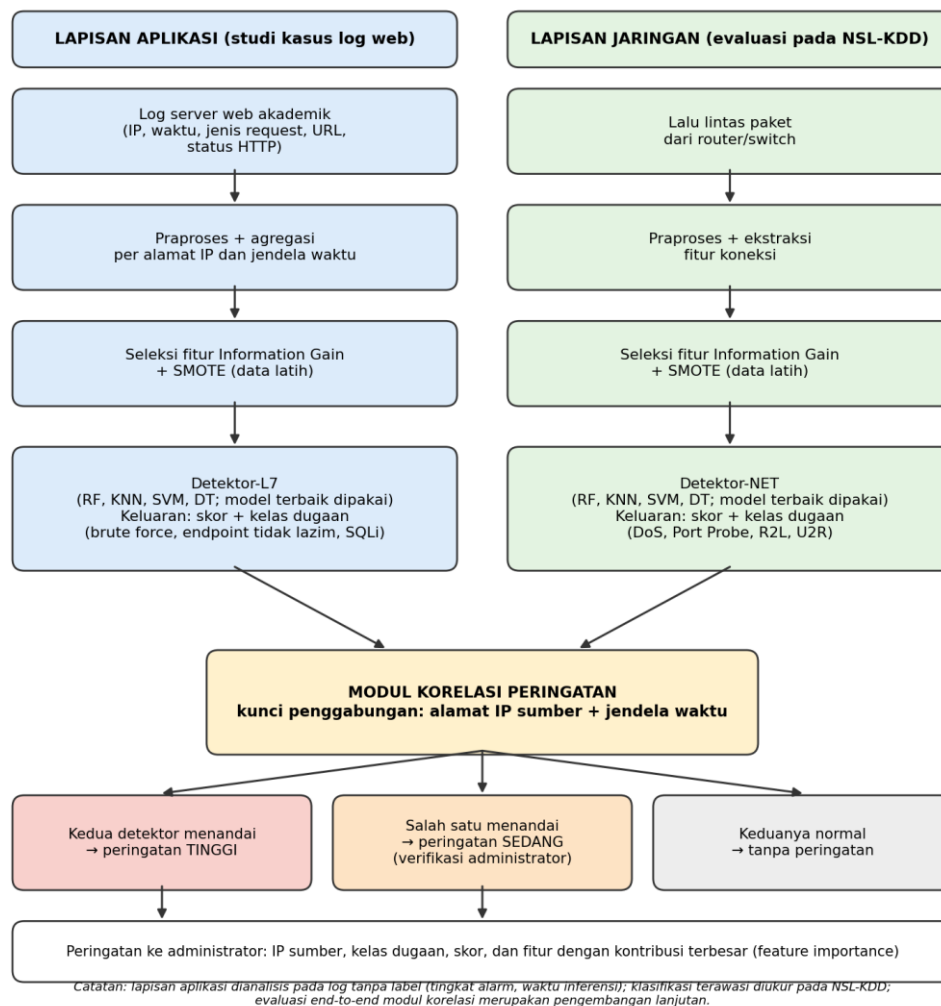
Desain Sistem dan Skema Penelitian

Skema alur proses sistem deteksi siber yang diusulkan terdiri dari tahapan terintegrasi yang dimulai dari pengumpulan lalu lintas paket data mentah dari router/switch jaringan lokal institusi pendidikan serta log dari server aplikasi web akademik (misalnya SIAKAD) (Chandra dkk., 2025). Data mentah tersebut selanjutnya dialirkan ke dalam modul praproses untuk pembersihan dan penyesuaian format (Chandra dkk., 2025). Setelah itu, fitur-fitur yang relevan diekstrak dan direduksi dimensinya menggunakan Information Gain sebelum kelas diseimbangkan menggunakan SMOTE (Setiyadi & Nikola, 2024). Akhirnya, model klasifikasi *Machine Learning* yang telah dilatih akan mengklasifikasikan trafik data secara waktu-nyata ke dalam kategori normal atau terindikasi serangan tertentu (Setiyadi & Nikola, 2024). Jika anomali terdeteksi, sistem akan memicu peringatan dini (alert) kepada administrator keamanan jaringan kampus (Chandra dkk., 2025). Rincian integrasi kedua sumber data tersebut dijelaskan pada subbab berikut.

Arsitektur Integrasi Sistem Peringatan Dini

Sistem diusulkan sebagai pipeline peringatan dini dua lapis (Gambar 2) yang berjalan paralel dan digabungkan pada modul korelasi peringatan (alert correlation). Lapisan aplikasi (Detektor-L7) menerima log akses aplikasi web akademik (misalnya SIAKAD), mengagregasinya per alamat IP dan jendela waktu, lalu menghasilkan skor serangan beserta kelas dugaan (brute force login, akses endpoint administratif yang tidak lazim, atau SQL injection). Lapisan jaringan (Detektor-NET) menerima fitur lalu lintas paket dari router/switch dan menghasilkan skor serangan beserta kelas dugaan (misalnya DoS atau Port Probe). Kedua detektor memakai tahapan praproses, seleksi fitur Information Gain, dan SMOTE yang sama, tetapi dilatih secara terpisah pada datanya masing-masing karena skema fitur keduanya berbeda.

Arsitektur Sistem Peringatan Dini Dua Lapis



Gambar 2 Arsitektur Sistem Peringatan Dini Dua Lapis

Modul korelasi peringatan menggabungkan keluaran kedua detektor berdasarkan kunci alamat IP sumber dan jendela waktu yang sama. Keputusan akhir ditetapkan dengan aturan berikut: (1) peringatan berstatus tinggi dikeluarkan apabila kedua detektor menandai sumber yang sama dalam satu jendela waktu, karena kesesuaian bukti dari dua lapisan menurunkan kemungkinan false positive pada lonjakan akses yang sah, misalnya saat pengisian KRS; (2) peringatan berstatus sedang dikeluarkan apabila hanya salah satu detektor yang menandai, dan diteruskan kepada administrator untuk diverifikasi; (3) tidak ada peringatan apabila kedua detektor menyatakan normal. Setiap peringatan memuat alamat IP sumber, kelas dugaan, skor, dan fitur dengan kontribusi terbesar (feature importance) untuk membantu administrator mengambil tindakan.

Pada penelitian ini, lapisan jaringan dievaluasi secara terawasi pada NSL-KDD, sedangkan lapisan aplikasi dianalisis pada log web universitas yang tidak berlabel sehingga hanya tingkat alarm dan biaya komputasinya yang diukur. Kedua dataset tidak dapat dipadankan karena NSL-

KDD tidak memuat alamat IP maupun stempel waktu. Evaluasi menyeluruh (end-to-end) modul korelasi, menggunakan data berlabel yang direkam bersamaan dari institusi yang sama (misalnya log SIAKAD), menjadi pengembangan selanjutnya.

Deskripsi Dataset dan Objek Penelitian

Penelitian ini menggunakan dua dataset dengan peran berbeda: log server web akademik sebagai studi kasus lapisan aplikasi, dan dataset benchmark NSL-KDD untuk evaluasi klasifikasi terawasi pada lapisan jaringan.

1. Log Server Web Akademik, studi kasus lapisan aplikasi: Data berupa log akses server web dari sistem online judge sebuah universitas (terindikasi dari URL pada log, yaitu RUET OJ). Berkas mentah berisi 16.007 baris; 218 baris rusak (potongan keluaran terminal yang bukan entri log) dibuang sehingga tersisa 15.789 entri valid. Entri mencakup alamat IP, waktu akses, jenis request beserta URL, dan status respons HTTP; tidak ada user-agent maupun ukuran respons. Periode data 7 November 2017 sampai 2 Maret 2018 dengan 57 hari aktif dan hanya 5 alamat IP privat. Data tidak memiliki label serangan. Log ini bukan log SIAKAD, tetapi mewakili aplikasi web universitas dengan pola akses yang mengikuti jadwal kegiatan akademik (kontes). Sumber data beralamat URL: <https://www.kaggle.com/datasets/shawon10/web-log-dataset/data>.
2. Dataset Jaringan Lokal (NSL-KDD), evaluasi lapisan jaringan: Dataset ini diunduh dari repositori UCI *Machine Learning* sebagai benchmark standar keamanan jaringan (Tavallaee dkk., 2009; Setiyadi & Nikola, 2024). Dataset ini terdiri dari 125.973 rekaman pada set pelatihan (KDDTrain+) dan 22.544 rekaman pada set pengujian (KDDTest+). Setiap rekaman lalu lintas jaringan memiliki 41 fitur yang mencakup fitur dasar paket TCP/IP (seperti durasi, jenis protokol, jenis layanan, dan flag), fitur konten data (seperti jumlah shell, kegagalan login, dan direktori yang diakses), serta fitur statistik lalu lintas berbasis waktu. Dataset ini mengelompokkan data ke dalam kelas Normal dan empat kategori serangan utama: Denial of Service (DoS), Port Probe, Remote-to-Local (R2L), dan User-to-Root (U2R). NSL-KDD tidak memuat alamat IP dan stempel waktu sehingga hanya digunakan untuk mengevaluasi lapisan jaringan.

Praproses dan Pelabelan Data

- a. Tahapan praproses data mutlak dilakukan untuk memastikan kualitas data latih sebelum dimasukkan ke dalam algoritma klasifikasi. Langkah-langkah praproses yang diterapkan meliputi:
Pembersihan Data: Mengidentifikasi dan menangani nilai kosong (missing values) dengan metode imputasi nilai median serta menghilangkan duplikasi rekaman.
- b. Encoding Fitur Kategorikal: Mengonversi fitur kategoris bertipe string (seperti protocol_type, service, dan flag pada NSL-KDD atau jenis request pada log web) menjadi bentuk numerik representatif menggunakan teknik One-Hot Encoding.
- c. Normalisasi Fitur Numerik: Menskala ulang seluruh rentang nilai fitur numerik menggunakan metode Min-Max Scaler ke dalam rentang skala [0,1] untuk mencegah bias model akibat dominasi nilai nominal fitur yang besar.
- d. Pemrosesan Log Web Akademik: Entri rusak dibuang, waktu di-parse, lalu entri diagregasi per pasangan (alamat IP, menit) menjadi fitur jendela: jumlah request, jumlah URL unik, jumlah POST, jumlah akses halaman login, jumlah status 404, dan jumlah status 302 (3.558 jendela). Data tidak dilabeli; label berbasis aturan (≥ 50 request/menit) hanya digunakan untuk benchmark waktu komputasi dan tidak digunakan untuk melaporkan akurasi.

Rekayasa Fitur menggunakan Information Gain

Untuk meminimalkan beban komputasi dan menghindari fenomena curse of dimensionality pada jaringan lokal dengan trafik tinggi, diterapkan seleksi fitur berbasis Information Gain (IG) (Setiyadi & Nikola, 2024). Information Gain mengukur seberapa banyak kontribusi informasi yang diberikan oleh suatu fitur terhadap label kelas (Setiyadi & Nikola, 2024). Fitur dengan variansi mendekati nol disingkirkan secara otomatis. Dari 41 fitur asli pada dataset NSL-KDD, dipilih 20 fitur teratas dengan nilai IG tertinggi untuk digunakan dalam pelatihan model, yang terbukti secara signifikan menghemat waktu pelatihan sebesar 34% (Setiyadi & Nikola, 2024).

Penanganan Ketidakseimbangan Kelas menggunakan SMOTE

Distribusi kelas dalam data lalu lintas jaringan riil sangat tidak seimbang (class imbalance). Sebagai contoh, pada NSL-KDD, kelas mayoritas seperti Normal memiliki 53.074 sampel dan DoS memiliki 45.927 sampel, sedangkan kelas minoritas seperti R2L hanya memiliki 995 sampel dan U2R hanya memiliki 52 sampel (Setiyadi & Nikola, 2024). Ketidakseimbangan ekstrem ini dapat menyebabkan bias model ke arah kelas mayoritas, membuat deteksi serangan minoritas gagal (recall sangat rendah) (Setiyadi & Nikola, 2024). Untuk mengatasi hal ini, teknik Synthetic Minority Oversampling Technique (SMOTE) diterapkan hanya pada data latih (setelah pembagian stratified split 80:20 data latih-uji untuk menghindari data leakage) (Setiyadi & Nikola, 2024). SMOTE menghasilkan sampel sintesis baru pada kelas minoritas dengan melakukan interpolasi linear antara sampel data asli dengan tetangga terdekatnya (k-nearest neighbors) bukan dengan menduplikasi data, sehingga mengurangi overfitting (Setiyadi & Nikola, 2024).

Model Klasifikasi Machine Learning

Penelitian ini mengevaluasi dan membandingkan performa empat algoritma machine learning:

- Random Forest (RF): Algoritma ensemble learning yang membangun sejumlah besar pohon keputusan (decision trees) secara acak saat proses pelatihan dan menghasilkan prediksi kelas mayoritas (voting) dari semua pohon (Setiyadi & Nikola, 2024). RF sangat tangguh terhadap noise dan overfitting berkat teknik bagging.
- K-Nearest Neighbor (KNN): Algoritma non-parametrik yang mengklasifikasikan data baru berdasarkan mayoritas kelas tetangga terdekat menggunakan metrik jarak Euclidean (Setiyadi & Nikola, 2024). KNN sangat intuitif namun memiliki biaya komputasi prediksi yang cenderung tinggi pada data besar.
- Support Vector Machine (SVM): Model klasifikasi yang bekerja dengan menemukan hyperplane optimal dengan margin maksimal untuk memisahkan kelas dalam ruang dimensi tinggi menggunakan fungsi kernel Radial Basis Function (RBF) untuk pemisahan non-linear (Setiyadi & Nikola, 2024).
- Decision Tree (DT): Algoritma klasifikasi berbasis diagram alur pohon keputusan yang mengelompokkan data berdasarkan atribut pembagi terbaik (Chandra dkk., 2025). Model ini sangat mudah diinterpretasikan oleh operator keamanan sistem (Chandra dkk., 2025).

Metrik Evaluasi Performa

Model dievaluasi menggunakan metode validasi silang (cross-validation) serta pengujian pada data uji terpisah menggunakan metrik evaluasi standar yang diturunkan dari confusion matrix, serta tingkat alarm dan metrik efisiensi komputasi, yaitu:

- Accuracy: Persentase total prediksi benar (positif dan negatif) dari seluruh sampel data.
- Precision: Rasio sampel serangan terdeteksi benar (True Positive) dibandingkan dengan semua sampel yang diklasifikasikan sebagai serangan.
- Recall (Sensitivity): Rasio sampel serangan terdeteksi benar dibandingkan dengan total populasi serangan yang sebenarnya di dalam dataset.
- F1-Score: Nilai rata-rata harmonis antara presisi dan recall, yang menjadi indikator performa model yang paling andal pada dataset tidak seimbang.
- Waktu Inferensi: Rata-rata waktu yang dibutuhkan model terlatih untuk memprediksi satu rekaman data (milidetik per rekaman), diukur pada lingkungan komputasi 1 vCPU x86_64 dengan RAM 4 GB (Python, scikit-learn 1.8.0). Pengukuran dilakukan dalam mode batch (rata-rata per rekaman pada 1.000 jendela, diulang 5 kali) dan mode rekaman tunggal (200 pemanggilan prediksi berurutan, diulang 3 kali). Metrik ini diperlukan karena sistem ditargetkan untuk mitigasi waktu-nyata.
- Tingkat Alarm: Proporsi jendela yang ditandai sebagai serangan oleh detektor pada data tidak berlabel. Pada data yang diasumsikan sebagian besar berisi trafik sah, nilai ini dibaca sebagai estimasi false positive rate dan bukan sebagai ukuran kemampuan mendeteksi serangan.

Skenario Analisis pada Log Web Akademik

Entri log diagregasi per pasangan (IP, menit) menjadi 3.558 jendela. Hari dengan lebih dari 2.000 request disebut hari lonjakan (30 November 2017 dan 29 Januari 2018); hari lain disebut hari normal. Karena tidak ada label, trafik diasumsikan didominasi aktivitas sah, sehingga

proporsi jendela yang ditandai sebagai serangan pada data uji dibaca sebagai estimasi false positive rate. Data hari normal dibagi secara kronologis 70:30 (1.766 jendela latih dan 757 jendela uji); data uji hari lonjakan adalah seluruh jendela 29 Januari 2018 (120 jendela). Detektor yang dibandingkan adalah ambang statis (≥ 20 , ≥ 50 , dan ≥ 100 request per menit per IP) dan Isolation Forest (100 pohon, contamination 0,01) yang dilatih pada (a) hari normal saja dan (b) hari normal ditambah hari lonjakan 30 November 2017 (915 jendela). Benchmark waktu komputasi dilakukan pada keempat model terawasi dan Isolation Forest menggunakan seluruh jendela dengan label berbasis aturan (≥ 50 request/menit; 40 jendela positif) yang hanya dipakai untuk pengukuran waktu. Pencarian hyperparameter SVM menggunakan Grid Search ($C \in \{0,1; 1; 10\}$, $\gamma \in \{0,01; 0,1; 1\}$, validasi silang 3 lipatan).

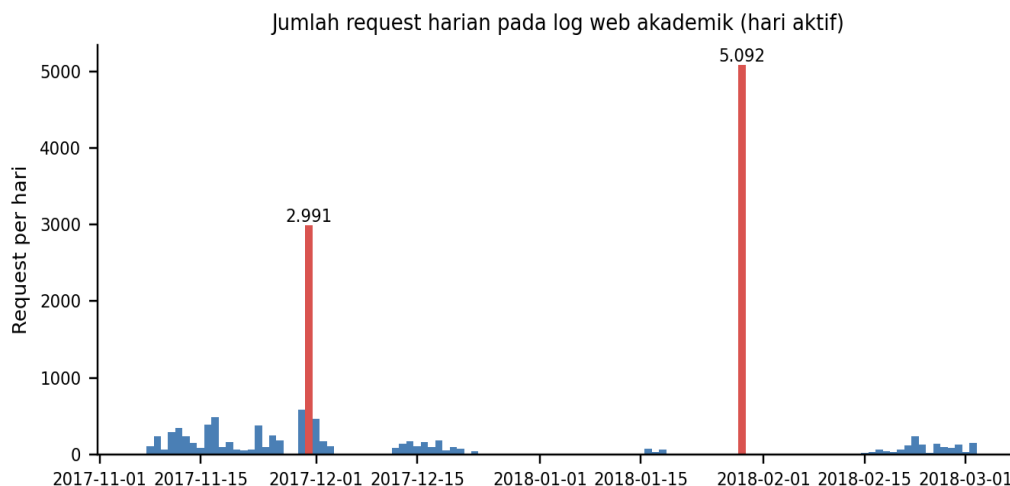
HASIL DAN PEMBAHASAN

Hasil Seleksi Fitur Berbasis Information Gain

Proses seleksi fitur berbasis Information Gain (IG) pada dataset NSL-KDD berhasil mereduksi 41 fitur asli menjadi 20 fitur paling informatif. Lima fitur teratas yang memiliki nilai kontribusi informasi terbesar terhadap label kelas adalah: src_bytes (0,862), dst_bytes (0,831), count (0,795), srv_count (0,763), dan logged_in (0,748). Fitur src_bytes dan dst_bytes secara dominan menggambarkan volume lalu lintas pertukaran byte data dalam jaringan, sedangkan fitur count dan srv_count mengindikasikan frekuensi koneksi unik ke host atau layanan tertentu dalam jendela waktu yang singkat. Parameter statistik ini merupakan indikator kuat dari pola anomali aktivitas siber seperti serangan Denial of Service (DoS) dan pemindaian port (Port Scanning) (Buczak & Guven, 2016). Penggunaan 20 fitur terpilih ini mampu menghemat waktu komputasi pelatihan model sebesar 34% tanpa menurunkan performa akurasi sistem secara signifikan.

Karakteristik Trafik dan Tingkat Alarm pada Log Web Akademik

Log server web akademik yang digunakan memuat 15.789 entri valid dari 5 alamat IP dalam 57 hari aktif. Jumlah request harian sangat tidak merata (Gambar 3): median hanya 100 request per hari dan hari non-lonjakan terpadat 580 request, tetapi dua hari lonjakan, yaitu 30 November 2017 (2.991 request) dan 29 Januari 2018 (5.092 request), menyumbang 51,2% dari seluruh request. Pada tingkat jendela, satu IP mengirim hingga 128 request dalam satu menit. Status respons didominasi 200 (71,8%) dan 302 (22,2%), disusul 304 (4,2%), 404 (1,6%), dan 206 (0,3%); sebanyak 95,6% request adalah GET dan 4,3% POST. Hanya satu request ber-pola SQL injection (parameter id dengan tanda petik, %27) yang ditemukan melalui pencocokan pola, sehingga log ini tidak memuat serangan yang dapat diidentifikasi secara jelas tanpa label. Tabel 1 membandingkan tingkat alarm detektor pada hari normal dan hari lonjakan.



Gambar 3 Jumlah Request Harian pada Log Web Akademik

Tabel 1 Tingkat Alarm Detektor pada Jendela (IP × Menit) Hari Normal dan Hari Lonjakan (29 Januari 2018)

Detektor	Alarm hari normal (%) (n = 757)	Alarm 29 Jan 2018 (%) (n = 120)
Ambang statis ≥ 20 request/menit/IP	0,0	70,0

Detektor	Alarm hari normal (%) (n = 757)	Alarm 29 Jan 2018 (%) (n = 120)
Ambang statis ≥ 50 request/menit/IP	0,0	33,3
Ambang statis ≥ 100 request/menit/IP	0,0	3,3
Isolation Forest (latih: hari normal)	0,4	76,7
Isolation Forest (latih: hari normal + lonjakan 30 Nov 2017)	0,8	76,7

Pada hari normal, ambang statis tidak menghasilkan alarm sama sekali (0%), tetapi pada 29 Januari 2018 ambang 20 request/menit menandai 70,0% jendela, ambang 50 menandai 33,3%, dan ambang 100 menandai 3,3%. Dengan asumsi trafik hari itu sebagian besar sah, ambang yang cukup rendah untuk menangkap serangan lambat menimbulkan banyak false positive saat lonjakan, sedangkan ambang 100 request/menit hanya menyisakan 3,3% alarm tetapi akan melewatkan serangan di bawah laju tersebut; kemampuan ambang menangkap serangan tidak dapat diukur karena tidak ada label. Isolation Forest yang dilatih pada hari normal menandai 0,4% jendela hari normal tetapi 76,7% jendela hari lonjakan; menambahkan satu hari lonjakan (30 November 2017) ke data latih menaikkan alarm hari normal menjadi 0,8% dan tidak mengubah alarm hari lonjakan (76,7%). Dengan demikian, pada pengaturan ini menambah satu hari lonjakan ke data latih belum cukup membuat detektor mengenali lonjakan sah sebagai normal. Temuan ini berasal dari satu sumber data dengan 5 alamat IP, nilai alarm Isolation Forest bergantung pada parameter contamination, dan hasilnya perlu diuji pada data berlabel dari institusi lain.

Evaluasi Performa Deteksi Serangan pada Jaringan Lokal (NSL-KDD) pada Lapisan Jaringan

Hasil pengujian performa algoritma *Machine Learning* yang dievaluasi dengan menggunakan metode 10-fold cross-validation pada data lalu lintas jaringan (NSL-KDD) dirangkum pada Tabel 2 di bawah ini.

Tabel 2 Hasil Perbandingan Performa Algoritma *Machine Learning* pada Dataset NSL-KDD

Algoritma	Akurasi (%)	Presisi (%)	Recall (%)	F1-Score (%)
Random Forest	98,76	98,12	98,54	98,33
KNN (k=7)	95,41	94,87	95,23	95,05
SVM (Kernel RBF)	93,87	93,15	93,62	93,38

Berdasarkan Tabel 2, algoritma Random Forest secara konsisten unggul pada seluruh metrik evaluasi dibandingkan dua model lainnya. Random Forest mencapai tingkat Akurasi tertinggi sebesar 98,76%, Presisi sebesar 98,12%, Recall sebesar 98,54%, dan F1-Score sebesar 98,33%. Di posisi kedua, algoritma K-Nearest Neighbor (KNN) mencapai Akurasi 95,41%, disusul oleh Support Vector Machine (SVM) dengan akurasi sebesar 93,87%. Waktu inferensi tidak diukur pada NSL-KDD dalam penelitian ini; benchmark komputasi disajikan pada Tabel 4. Hasil ini menunjukkan bahwa model berbasis ensemble efektif memisahkan trafik berbahaya dari trafik normal pada dataset NSL-KDD, sejalan dengan literatur sebelumnya (Setiyadi & Nikola, 2024). Namun, karena NSL-KDD berasal dari data KDD Cup 1999 (Tavallae dkk., 2009), angka ini digunakan sebagai pembandingan benchmark dan tidak langsung mencerminkan kinerja pada trafik jaringan kampus.

Dampak SMOTE pada Deteksi Kelas Serangan Minoritas

Untuk menganalisis dampak implementasi teknik SMOTE dalam mengatasi ketidakseimbangan kelas pada lalu lintas jaringan lokal (NSL-KDD), Tabel 3 menampilkan rincian performa klasifikasi Random Forest pada masing-masing kategori kelas serangan.

Tabel 3 Rincian Kinerja Klasifikasi Random Forest per Kategori Kelas (NSL-KDD)

Kategori Kelas	Presisi (%)	Recall (%)	F1-Score (%)	Jumlah Sampel (Support)
Normal	99,21	99,34	99,27	9.711

Kategori Kelas	Presisi (%)	Recall (%)	F1-Score (%)	Jumlah Sampel (Support)
Denial of Service (DoS)	98,87	98,91	98,89	7.458
Port Probe	97,43	97,68	97,55	2.421
Remote to Local (R2L)	94,12	93,76	93,94	971
User to Root (U2R)	89,65	88,42	89,03	167

Berdasarkan hasil rincian pada Tabel 3, model Random Forest menunjukkan performa deteksi yang luar biasa stabil dan sangat baik pada dua kelas mayoritas, yaitu kelas Normal (F1-Score 99,27%) dan serangan DoS (F1-Score 98,89%). Namun, kontribusi paling krusial dari penerapan teknik SMOTE terlihat pada performa deteksi kelas minoritas (R2L dan U2R). Sebelum menerapkan SMOTE, kelas serangan minoritas ini sering kali tidak terdeteksi dengan baik karena bias klasifikasi model, di mana nilai rata-rata recall untuk kelas minoritas hanya mencapai 71,3%. Setelah menerapkan teknik SMOTE, recall untuk kelas R2L meningkat tajam menjadi 93,76% dan kelas U2R mencapai 88,42%, dengan rata-rata recall kelas minoritas secara keseluruhan melonjak ke angka 91,0%. Temuan ini membuktikan efektivitas yang nyata dari penyeimbangan sampel latih secara sintesis untuk memperkuat kemampuan deteksi dini terhadap jenis serangan intrusi kritis yang jarang terjadi sebagaimana diuraikan dalam penelitian penyeimbangan kelas (Chawla dkk., 2002; Setiyadi & Nikola, 2024).

Efisiensi Komputasi dan Waktu Inferensi

Waktu komputasi diukur pada 3.558 jendela log web dengan 6 fitur pada lingkungan 1 vCPU dan RAM 4 GB. Label berbasis aturan hanya dipakai untuk keperluan pengukuran waktu sehingga tidak ada metrik akurasi yang dilaporkan dari pengukuran ini. Tabel 4 merangkum hasilnya.

Tabel 4 Waktu Pelatihan dan Waktu Inferensi pada Fitur Jendela Log Web (3.558 jendela, 6 fitur)

Model	Waktu latih (detik)	Inferensi batch (ms/rekaman)	Inferensi tunggal (ms/rekaman)
Random Forest	0,139	0,0074	6,081
Decision Tree	0,0016	0,0001	0,069
KNN (k=7)	0,0044	0,0125	1,121
SVM (RBF)	0,011	0,0019	0,096
Isolation Forest	0,110	0,0098	6,743

Seluruh model memprediksi dalam waktu di bawah 0,02 ms per rekaman pada mode batch. Pada mode rekaman tunggal, Decision Tree (0,069 ms) dan SVM (0,096 ms) tercepat, KNN 1,12 ms, sedangkan Random Forest (6,08 ms) dan Isolation Forest (6,74 ms) paling lambat karena setiap pemanggilan prediksi harus melewati 100 pohon; pemanggilan per rekaman juga membawa overhead pustaka, sehingga penerapan sebenarnya sebaiknya memproses jendela secara batch per menit. Pada KNN, waktu inferensi batch meningkat dari 0,0135 ms (3.558 data latih) menjadi 0,0231 ms (35.580) dan 0,0418 ms (106.740), yaitu 3,1 kali lipat untuk data latih 30 kali lebih besar. Hal ini sesuai dengan sifat lazy learner KNN, tetapi peningkatannya masih landai pada skala ini; data latih diperbesar dengan menggandakan jendela asli dan menambahkan derau kecil, sehingga angka ini hanya indikasi dan bukan ukuran pada NSL-KDD. Grid Search SVM (9 kombinasi, 3 lipatan) hanya memerlukan 0,2 detik pada data ini, sehingga dugaan bahwa tuning SVM memakan waktu komputasi intensif tidak terbukti pada skala data ini; SVM yang dilatih pada label berbasis aturan dengan hanya 40 contoh positif cenderung memiliki sedikit support vector, sehingga hasil ini bukan ukuran pada data NSL-KDD yang jauh lebih besar.

Diskusi dan Implikasi Praktis

Interpretasi Fitur Statistik Koneksi dengan Information Gain Tertinggi

Dominasi fitur statistik koneksi (src_bytes, dst_bytes, count, dan srv_count) pada peringkat Information Gain dapat dijelaskan oleh cara kerja serangan yang paling banyak terwakili dalam dataset. Information Gain mengukur penurunan ketidakpastian label kelas setelah nilai suatu

fitur diketahui. Serangan DoS, yang berjumlah 45.927 sampel, menghasilkan banyak koneksi ke host atau layanan yang sama dalam jendela waktu singkat sehingga nilai count dan `srv_count` tinggi, sedangkan pemindaian port (Port Probe) menghasilkan banyak koneksi pendek dengan volume byte sangat kecil atau nol ke banyak layanan sehingga `src_bytes` dan `dst_bytes` mendekati nol. Trafik normal memiliki sebaran volume byte dan frekuensi koneksi yang jauh berbeda, sehingga fitur-fitur ini memisahkan kelas dengan baik. Fitur `logged_in` turut membedakan koneksi yang telah terautentikasi dari koneksi tanpa autentikasi yang menjadi ciri sebagian besar DoS dan Probe. Sebaliknya, fitur konten seperti jumlah shell dan kegagalan login hanya bermakna pada R2L dan U2R yang sampelnya sangat sedikit (995 dan 52 sampel), sehingga kontribusi informasinya terhadap label keseluruhan kecil walaupun penting bagi kelas tersebut. Pola serupa, yaitu seleksi fitur yang sedikit menurunkan akurasi tetapi mempercepat pelatihan, dilaporkan pada studi lain (Barkah dkk., 2023).

Dalam konteks infrastruktur akademik, hubungan ini relevan karena serangan yang paling mungkin menargetkan SIAKAD, yaitu banjir permintaan (DoS/DDoS), pemindaian port dan endpoint, serta percobaan login berulang, juga tampil sebagai perubahan frekuensi dan volume koneksi dari sumber tertentu. Padanan fitur tersebut pada log aplikasi web akademik adalah jumlah permintaan per alamat IP per jendela waktu (padanan count dan `srv_count`), ukuran respons (padanan `dst_bytes`), dan jumlah respons gagal per sumber (padanan kegagalan login). Namun, fitur frekuensi yang sama juga tinggi pada lonjakan akses yang sah, seperti pengisian KRS dan pengumuman nilai. Karena itu fitur-fitur ini perlu dikombinasikan dengan fitur yang membedakan lonjakan sah dari serangan, misalnya keragaman alamat IP klien dan proporsi respons galat (Molnar & Sabodashko, 2025), dan tidak dapat digunakan sebagai ambang batas tunggal. Hal ini menjadi alasan penggunaan model berbasis pohon yang menangkap interaksi antarfitur, sekaligus alasan keluaran lapisan jaringan dan lapisan aplikasi dikorelasikan pada arsitektur yang diusulkan.

Perlu dicatat bahwa peringkat Information Gain di atas diperoleh dari NSL-KDD yang merupakan turunan data KDD Cup 1999 (Tavallae dkk., 2009) dan dinilai kurang merepresentasikan lalu lintas kampus masa kini (Sindika dkk., 2025). Penjelasan di atas karenanya merupakan interpretasi atas pola yang teramati pada dataset tersebut, bukan bukti bahwa fitur yang sama akan memiliki gain tertinggi pada lalu lintas SIAKAD. Peringkat Information Gain pada fitur log web akademik belum dilaporkan pada penelitian ini dan menjadi analisis lanjutan.

Keunggulan algoritma Random Forest dalam penelitian ini sejalan dengan studi lain yang melaporkan bahwa ensemble pohon keputusan mampu menangkap interaksi nonlinier antarfitur pada data lalu lintas jaringan lebih baik daripada model linier (Molnar & Sabodashko, 2025), dan bahwa model ensemble berbasis pohon efektif pada data jaringan kampus (Yin & Chen, 2023). Namun, hasil terhadap Decision Tree tidak selalu demikian pada dataset lain (Barkah dkk., 2023), sehingga evaluasi pada data lokal tetap diperlukan. Dari segi implementasi taktis, model Random Forest juga memberikan estimasi feature importance (tingkat kepentingan fitur) secara internal, yang sangat bermanfaat untuk menganalisis karakteristik kritis serangan jaringan. Efisiensi komputasi merupakan pertimbangan penting dalam sistem deteksi intrusi yang ditargetkan berjalan cepat (Liu dkk., 2021).

Di sisi lain, meskipun KNN memberikan akurasi 95,41% yang cukup baik, ia merupakan lazy learner yang harus menghitung jarak ke seluruh titik data pelatihan pada setiap prediksi. Benchmark pada penelitian ini menunjukkan waktu inferensi KNN sebesar 1,12 ms per rekaman pada mode tunggal, jauh di atas Decision Tree (0,069 ms) dan SVM (0,096 ms), dan waktunya tumbuh seiring ukuran data latih (Tabel 4). Namun pada skala yang diukur, semua model masih berada dalam orde milidetik per rekaman sehingga penapisan hampir waktu-nyata secara batch per menit dapat dipenuhi; kendala KNN pada trafik berintensitas tinggi dan data latih sebesar NSL-KDD (125.973 rekaman) belum diukur langsung dan masih merupakan dugaan berdasarkan sifat algoritmanya. Sementara itu, SVM dengan kernel RBF memetakan batas klasifikasi non-linear dengan akurasi 93,87%, tetapi sensitif terhadap hyperparameter C dan gamma; pada data penelitian ini Grid Search 9 kombinasi hanya memerlukan 0,2 detik, sehingga beban tuning pada skala data NSL-KDD perlu diukur tersendiri.

Untuk lapisan aplikasi, penelitian ini belum dapat menunjukkan kemampuan mendeteksi serangan karena log yang dianalisis tidak berlabel, hanya memuat satu request ber-pola SQL injection, dan tidak memperlihatkan indikasi brute force yang dapat diverifikasi. Yang dapat ditunjukkan adalah bahwa trafik akademik nyata memuat lonjakan sah yang memicu alarm pada detektor berbasis ambang statis maupun Isolation Forest (Tabel 1). Temuan ini mendukung

perlunya pelatihan pada data lokal berlabel dan perlunya korelasi bukti antar-lapisan melalui modul korelasi peringatan untuk menekan false positive, tetapi efektivitas modul korelasi tersebut belum diuji.

Penelitian ini memiliki beberapa keterbatasan. Pertama, log web yang dianalisis berasal dari satu aplikasi (online judge), 5 alamat IP, dan 57 hari aktif, serta bukan log SIAKAD, sehingga generalisasi ke SIAKAD belum teruji. Kedua, log tidak berlabel sehingga akurasi, presisi, dan recall pada lapisan aplikasi tidak dapat dihitung, dan tingkat alarm hanya dapat dibaca sebagai estimasi false positive dengan asumsi trafik sebagian besar sah; alarm Isolation Forest juga bergantung pada parameter contamination. Ketiga, lapisan aplikasi dan lapisan jaringan dievaluasi pada dataset berbeda yang tidak dapat dipadankan sehingga modul korelasi belum diuji secara end-to-end. Keempat, benchmark waktu komputasi dilakukan pada fitur log web yang berukuran kecil dengan label berbasis aturan dan bukan pada NSL-KDD. Kelima, peringkat Information Gain pada fitur log web belum dilaporkan sehingga interpretasi fitur pada konteks akademik masih berupa dugaan berbasis NSL-KDD.

KESIMPULAN

Penelitian ini mengusulkan arsitektur peringatan dini serangan siber dua lapis berbasis machine learning, yaitu lapisan jaringan dan lapisan aplikasi web, untuk institusi pendidikan. Pada lapisan jaringan, Random Forest memberikan kinerja klasifikasi terbaik pada dataset NSL-KDD dengan akurasi sebesar 98,76% dan F1-Score sebesar 98,33%. Penerapan seleksi fitur berbasis Information Gain juga mampu mereduksi jumlah fitur pada dataset NSL-KDD dari 41 menjadi 20 fitur paling informatif dan mengurangi waktu pelatihan model sebesar 34% tanpa menurunkan kinerja klasifikasi secara signifikan. Selain itu, penerapan SMOTE mampu meningkatkan kemampuan sistem dalam mendeteksi kelas serangan minoritas, khususnya R2L dengan recall sebesar 93,76% dan U2R sebesar 88,42%, serta meningkatkan rata-rata recall kelas minoritas dari 71,3% menjadi 91,0%. Pada lapisan aplikasi, analisis 15.789 entri log server web universitas yang tidak berlabel menunjukkan bahwa dua hari lonjakan menyumbang 51,2% request dan bahwa ambang statis 20 request/menit menandai 70,0% jendela pada hari lonjakan, sehingga lonjakan trafik akademik yang sah berpotensi menimbulkan false positive. Seluruh model yang diuji memprediksi dalam orde milidetik per rekaman pada skala data yang diukur (0,07 sampai 6,7 ms pada mode rekaman tunggal). Karena log aplikasi tidak berlabel dan bukan log SIAKAD, kemampuan lapisan aplikasi mendeteksi serangan serta efektivitas modul korelasi belum terbukti. Untuk pengembangan selanjutnya, sistem disarankan dilatih dan diuji secara end-to-end menggunakan log SIAKAD berlabel yang direkam bersamaan dengan data trafik jaringan, dikembangkan dengan mekanisme pembelajaran adaptif untuk menghadapi pola serangan baru, serta diintegrasikan dengan mekanisme respons insiden agar deteksi dan penanganan serangan siber dapat dilakukan lebih cepat, akurat, dan berkelanjutan.

REFERENSI

- Ahmed, H. A., Hameed, A., & Bawany, N. Z. (2022). Network intrusion detection using oversampling technique and *Machine Learning* algorithms. *PeerJ Computer Science*, 8, e820. <https://doi.org/10.7717/peerj-cs.820>
- Ahsan, R., Shi, W., & Corriveau, J. P. (2022). Network intrusion detection using *Machine Learning* approaches: Addressing data imbalance. *IET Cyber-Physical Systems: Theory & Applications*, 7(1), 30-39. <https://doi.org/10.1049/cps2.12013>
- Bagui, S., & Li, K. (2021). Resampling imbalanced data for network intrusion detection datasets. *Journal of Big Data*, 8(1), 6. <https://doi.org/10.1186/s40537-020-00390-x>
- Barkah, A. S., Selamat, S. R., Abidin, Z. Z., & Wahyudi, R. (2023). Impact of data balancing and feature selection on machine learning-based network intrusion detection. *JOIV: International Journal on Informatics Visualization*, 7(1), 241-248. <https://joiv.org/index.php/joiv/article/view/1041>
- BSSN. (2023). Laporan Tahunan Keamanan Siber Indonesia 2023. Badan Siber dan Sandi Negara Republik Indonesia. Jakarta. <https://csirt.kemenkeu.go.id/in/post/lanskap-keamanan-siber-indonesia-2023>
- Buczak, A. L., & Guven, E. (2016). A survey of data mining and *Machine Learning* methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153-1176. <https://doi.org/10.1109/COMST.2015.2494502>

- Chandra, C., Mulya, D. P., & Faradika. (2025). Deteksi Serangan Siber Menggunakan Machine Learning: Studi Pada Sistem Informasi Akademik. *JISKA: Jurnal Sistem Informasi Dan Informatika*, 3(2), 106-110. <http://jurnal.unidha.ac.id/index.php/jiska>
- Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 16, 321-357. <https://doi.org/10.1613/jair.953>
- Hesham, M., Essam, M., Bahaa, M., Mohamed, A., Gomaa, M., Hany, M., & Elersy, W. (2024, July). Evaluating predictive models in cybersecurity: a comparative analysis of machine and deep learning techniques for threat detection. In *2024 Intelligent Methods, Systems, and Applications (IMSA)* (pp. 33-38). IEEE. 10.1109/IMSA61967.2024.10652833
- Liu, J., Gao, Y., & Hu, F. (2021). A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM. *Computers & Security*, 106, 102289. <https://doi.org/10.1016/j.cose.2021.102289>
- Molnar, V., & Sabodashko, D. (2025). Pragmatic DDoS detection on AWS cloud with lightweight machine learning. *CPITS-II 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CEUR Workshop Proceedings, Vol. 4145, pp. 217-227)*. <https://ceur-ws.org/Vol-4145/paper14.pdf>
- Sayed, M. A., Badruddowza, M. S. U. S., Al Mamun, A., Nabi, N., Mahmud, F., Alam, M. K., ... & Choudhury, M. Z. M. E. (2024). Comparative analysis of *Machine Learning* algorithms for predicting cybersecurity attack success: A performance evaluation. *The American Journal of Engineering and Technology*, 6(09), 81-91. <https://doi.org/10.37547/tajet/Volume06Issue09-10>
- Setiyadi, D., & Nikola, E. (2024). Deteksi Serangan Siber Menggunakan *Machine Learning* Pada Jaringan Komputer. *JURNAL ILMU KOMPUTER, SISTEM INFORMASI, TEKNIK INFORMATIKA*, 3(1), 57-60. <https://jurnal.akommedia.net/index.php/JILKOMSITI/article/view/184>
- Sharma, N. V., & Yadav, N. S. (2021). An optimal intrusion detection system using recursive feature elimination and ensemble of classifiers. *Microprocessors and Microsystems*, 85, 104293. <https://doi.org/10.1016/j.micpro.2021.104293>
- Sindika, D. M., Nicholas, M. R., & Hamadi, N. B. (2025). Improving intrusion detection accuracy in campus networks: A dataset driven by real-time traffic and honeypot simulations. *MUST Journal of Research and Development*, 6(2), 11. <https://mjrd.must.ac.tz/index.php/mjrd/article/view/191>
- Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. *Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 1-6. <https://doi.org/10.1109/CISDA.2009.5356528>
- Yin, L., & Chen, Y. (2023). An intrusion detection model based on random tree algorithm with dimensionality reduction and oversampling. *Journal of Computing and Information Technology*, 31(4), 219-231. <https://doi.org/10.20532/cit.2023.1005771>
- Zhong, H. (2025). University network intrusion detection method based on deep learning. *Proceedings of SPIE, 13447 (International Conference on Mechatronics and Intelligent Control, ICMIC 2024)*, 1344730. <https://doi.org/10.1117/12.3045018>