HEXATECH
Jurnal Ilmiah Teknik
Vol 4 No 2 Agustus 2025
ISSN: 2828-8696 (Print) ISSN: 2828-8548 (Electronic)
Open Access: https://jurnal.arkainstitute.co.id/index.php/hexatech/index

Implementasi sistem deteksi dini serangan siber menggunakan machine learning pada infrastruktur jaringan kampus "X"

FA Suharno
Institut Teknologi dan Bisnis Visi Nusantara Bogor
email: suharno@ITBVinus.ac.id

Info Artikel :
Diterima :
2 Juli 2025
Disetujui :
29 Juli 2025
Dipublikasikan :
7 Agustus 2025

ABSTRAK

Serangan siber menjadi ancaman utama bagi infrastruktur teknologi informasi, termasuk lingkungan kampus yang sangat bergantung pada jaringan terbuka dan akses publik. Sistem keamanan konvensional sering kali tidak mampu mendeteksi pola serangan baru secara real-time, sehingga dibutuhkan pendekatan cerdas berbasis machine learning. Penelitian ini bertujuan untuk mengembangkan sistem deteksi dini serangan siber dengan memanfaatkan algoritma Random Forest dan Support Vector Machine (SVM). Metode penelitian yang digunakan adalah kuantitatif eksperimental dengan pendekatan komputasional. Dataset yang digunakan adalah KDD Cup 1999 dan CICIDS 2017, yang merepresentasikan berbagai jenis serangan jaringan modern dan aktivitas normal. Proses yang dilakukan meliputi, tahapan data preprocessing, feature selection, pelatihan model, serta pengujian dalam lingkungan simulasi jaringan kampus. Evaluasi performa model dilakukan menggunakan metrik akurasi, precision, dan recall untuk menilai efektivitas deteksi ancaman. Hasil pengujian menunjukkan bahwa algoritma Random Forest menghasilkan akurasi sebesar 97,8%, precision 96,4%, dan recall 98,1%. Sementara itu, SVM mencatat akurasi 94,3%, precision 92,7%, dan recall 94,9%. Hasil ini mengindikasikan bahwa metode machine learning, khususnya Random Forest, memiliki potensi tinggi dalam meningkatkan kemampuan sistem deteksi ancaman siber pada jaringan kampus secara efektif dan efisien.

Kata kunci: Serangan Siber, Machine Learning, Random Forest, Support Vector Machine (SVM)

ABSTRACT

Cyberattacks are a major threat to information technology infrastructure, including campus environments that rely heavily on open networks and public access. Conventional security systems are often unable to detect new attack patterns in real time, necessitating an intelligent, machine learning-based approach. This research aims to develop an early detection system for cyberattacks using the Random Forest and Support Vector Machine (SVM) algorithms. The research method used is quantitative and experimental with a computational approach. The datasets used are the 1999 KDD Cup and 2017 CICIDS, which represent various types of modern network attacks and normal activity. The process involved data preprocessing, feature selection, model training, and testing in a campus network simulation environment. Model performance was evaluated using accuracy, precision, and recall metrics to assess threat detection effectiveness. Test results showed that the Random Forest algorithm achieved 97.8% accuracy, 96.4% precision, and 98.1% recall. Meanwhile, the SVM achieved 94.3% accuracy, 92.7% precision, and 94.9% recall. These results indicate that machine learning methods, especially Random Forest, have high potential in improving the capabilities of cyber threat detection systems on campus networks effectively and efficiently. .

Keywords: Cyber Attack, Machine Learning, Random Forest, Support Vector Machine (SVM)

PENDAHULUAN

Kemajuan teknologi informasi telah mendorong transformasi digital di berbagai sektor termasuk institusi pendidikan tinggi. Di lingkungan kampus, penggunaan jaringan komputer yang masif serta kebutuhan konektivitas internet yang tinggi menjadikan infrastruktur jaringan sebagai bagian yang krusial dari sistem operasional. Namun, keterbukaan dan kompleksitas jaringan kampus justru menjadi celah potensial bagi terjadinya serangan siber (*cyber attack*), yang semakin hari menunjukkan peningkatan secara kuantitas dan kompleksitas (Berman et al., 2019).

Menurut Zhang et al. (2020), serangan siber kini tidak hanya bersifat merusak (*destructive*) tetapi juga mencuri data, melakukan pemantauan tanpa izin, hingga memanfaatkan sumber daya jaringan secara ilegal. Untuk itu, sistem pertahanan jaringan perlu berkembang dari yang bersifat reaktif menjadi proaktif, yakni dengan mengimplementasikan sistem deteksi dini (*early detection system*) berbasis machine learning yang mampu mengidentifikasi pola anomali sejak awal.

Meskipun banyak kampus telah menggunakan firewall dan sistem keamanan konvensional, akan tetapi kebocoran data masih sering terjadi. Selain itu, terdapat akses ilegal yang masuk ke server, dan penyebaran malware melalui jaringan internal. Hal ini disebabkan oleh sistem keamanan yang hanya mengenali ancaman berdasarkan tanda tangan (*signature-based*), yaitu metode yang mendeteksi serangan dengan mencocokan pola yang telah diketahui sebelumnya. Akibatnya, serangan dengan pola baru (*zero-day attack*) seringkali tidak terdeteksi secara tepat waktu (Sommer & Paxson, 2010). Selain itu, beban administratif tim IT dalam memantau lalu lintas secara manual membuat potensi kesalahan manusia (*human error*) sangat tinggi.

Penelitian-penelitian sebelumnya telah mengeksplorasi penggunaan machine learning untuk keamanan jaringan. Vinayakumar et al. (2017) mengembangkan sistem deteksi serangan berbasis Convolutional Neural Network (CNN), dengan hasil akurasi tinggi, namun pengembangannya membutuhkan sumber daya komputasi yang besar. Dhanabal & Shantharajah (2015), memanfaatkan algoritma klasifikasi sederhana untuk dataset NSL-KDD, tetapi tidak diuji pada kondisi jaringan riil. Di sisi lain, penelitian Shone et al. (2018), memperkenalkan metode deep learning untuk pendeteksian anomali, namun belum terfokus pada implementasi di jaringan kampus. Berdasarkan kajian-kajian penelitian sebelumnya, ditemukan belum adanya model machine learning yang relatif ringan, akurat, dan dapat diimplementasikan secara nyata dalam lingkungan kampus berbasis data lokal maupun benchmark dataset, dengan pertimbangan efisiensi, respons cepat, dan skalabilitas.

Oleh karena itu, penelitian ini bertujuan untuk mengembangkan dan menguji sistem deteksi dini serangan siber pada jaringan kampus dengan pendekatan machine learning, menggunakan algoritma Random Forest dan Support Vector Machine (SVM). Tujuan utama dari sistem ini adalah untuk mengenali dan mengklasifikasikan jenis-jenis serangan siber dengan akurasi tinggi serta memberikan peringatan secara real-time guna mencegah eskalasi serangan.

Penelitian yang dilakukan berkontibusi dalam menyediakan model sistem keamanan jaringan berbasis machine learning yang bersifat adaptif, akurat, dan dapat diterapkan secara nyata di lingkungan jaringan kampus. Selain itu, penelitian ini memberikan benchmark perbandingan performa antara dua alogritma populer, yaitu Random Forest dan Support Vector Machine (SVM), dalam konteks deteksi serangan siber berbasis data lalu lintas jaringan. Penelitian ini juga menawarkan solusi keamanan yang tidak hanya praktis, tetapi juga dapat dimanfaatkan sebagai alat pembelajaran serta pengembangan kompetensi di bidang keamanan siber bagi institusi pendidikan. Dari segi akademik, penelitian ini menyajikan literatur mengenai implementasi sistem intrusion detection yang relevan dengan kebutuhan jaringan pendidikan tinggi di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen kuantitatif dengan pendekatan simulasi jaringan dan implementasi algoritma machine learning. Tujuan utama dari metode ini adalah untuk mengembangkan, melatih, dan menguji model deteksi dini serangan siber berdasarkan pola data lalu lintas jaringan (*network traffic*), kemudian mengukur efektivitasnya dari segi akurasi, kecepatan deteksi, dan efisiensi klasifikasi. Sistem yang dikembangkan terdiri dari tiga komponen utama, yaitu data collector yang berfungsi mengumpulkan log trafik jaringan, preprocessing dan ekstraksi fitur, serta modul klasifikasi yang menggunakan algoritma Random Forest dan Support Vector Machine (SVM). Sebagai pendukung penelitian, beberapa alat dan teknologi digunakan, seperti bahasa pemrograman Python, Scikit-learn, Pandas, dan Matplotlib, serta lingkungan simulasi menggunakan GNS3 dan Wireshark. Alur dalam penelitian ini melalui beberapa tahapan yang dimulai dari tahap pengumpulan dan pembersihan data, pelatihan model machine learning, evaluasi performa dengan metrik, seperti akurasi, precision, recall, dan F1-score, serta implementasi dalam skenario simulasi serangan.

Tahap pengumpulan data dilakukan dengan memanfaatkan dataset standar dalam dunia keamanan jaringan, yaitu KDD Cup 1999 dan CICIDS 2017. Dataset tersebut dipilih karena memiliki ragam jenis serangan yang luas, seperti Denial of Service (DoS), brute force login, port scanning, infiltration, hingga serangan berbasis botnet. Selain itu, data yang digunakan juga mencakup lalu lintas

normal yang penting untuk membedakan anomali dari aktivitas wajar. Data yang diperoleh dari dataset tersebut kemudian memasuki **tahap preprocessing**, yaitu serangkaian proses pembersihan dan transformasi data mentah menjadi format yang siap untuk dianalisis oleh algoritma machine learning. Tahapan ini meliputi penghapusan nilai yang tidak valid, normalisasi nilai numerik, pengkodean fitur kategorikal menjadi format numerik, serta proses balancing untuk mengatasi ketimpangan jumlah data antara trafik normal dan trafik berbahaya. Proses ini penting agar hasil klasifikasi tidak bias terhadap kelas mayoritas. Setelah itu, dilakukan ekstraksi fitur (*feature extraction*), yakni pemilihan atribut atau variabel yang paling berpengaruh dalam membedakan jenis trafik jaringan. Beberapa fitur penting yang digunakan antara lain jumlah byte yang dikirim, durasi koneksi, jenis protokol, jumlah koneksi dalam waktu tertentu, dan status flag koneksi. Proses ini bertujuan untuk menyederhanakan kompleksitas data sekaligus meningkatkan performa model saat dilatih.

Tahap inti dari penelitian ini adalah **tahap pelatihan model machine learning**. Dua algoritma dipilih untuk dibandingkan kinerjanya, yaitu Random Forest dan Support Vector Machine (SVM). Random Forest dipilih karena merupakan algoritma ensambel yang kuat dalam menghadapi data kompleks dan dapat menghindari overfitting, sementara SVM dikenal efektif dalam klasifikasi data dengan margin yang jelas. Model dilatih menggunakan data training yang telah disiapkan, lalu diuji menggunakan data testing yang berbeda untuk menghindari bias hasil. Selanjutnya **tahap evaluasi**, yang dilakukan dengan mengukur akurasi, precision, recall, dan F1-score dari masing-masing model. Selain itu, dilakukan simulasi sistem pada jaringan kampus virtual menggunakan perangkat lunak GNS3 dan Wireshark untuk melihat bagaimana sistem merespon serangan secara real-time. Proses deteksi dan pelaporan dianalisis berdasarkan kecepatan sistem dalam mengenali serangan, jumlah peringatan yang benar, serta kemampuan sistem menghindari false alarm. Secara umum, metode ini dirancang untuk menghasilkan sistem yang dapat diimplementasikan langsung di lingkungan nyata, khususnya di jaringan kampus yang rentan terhadap berbagai bentuk ancaman siber. Hasil akhir dari penelitian ini berupa model deteksi serangan yang terintegrasi dengan sistem pemantauan jaringan, serta laporan evaluasi kinerja algoritma secara kuantitatif.

HASIL DAN PEMBAHASAN

Hasil Pengujian

Tabel 1. Hasil Evaluasi Model

Model	Akurasi	Precision	Recall	F1-Score
Random Forest	97.8%	96.5%	98.2%	97.3%
SVM	94.3%	93.0%	94.8%	93.9%

Tabel 1. diatas menunjukkan bahwa algoritma Random Forest memberikan performa terbaik dalam mendeteksi serangan siber dengan akurasi 97,8%, precision 96,5%, recall 98,2%, dan F1-score 97,3%. Sementara itu, algoritma Support Vector Machine (SVM) memperoleh akurasi 94,3%, yang juga menunjukkan performa cukup tinggi. Berdasarkan hasil pengujian dapat disimpulkan bahwa, algoritma Random Forest menunjukkan performa lebih unggul dibandingkan SVM dalam semua metrik evaluasi. Akurasi tinggi sebesar 97,8% menandakan bahwa model ini mampu memprediksi jenis trafik dengan tingkat kesalahan yang sangat rendah. Nilai recall yang tinggi sebesar 98,2% menunjukkan keandalan model dalam mendeteksi sebagian besar ancaman siber.

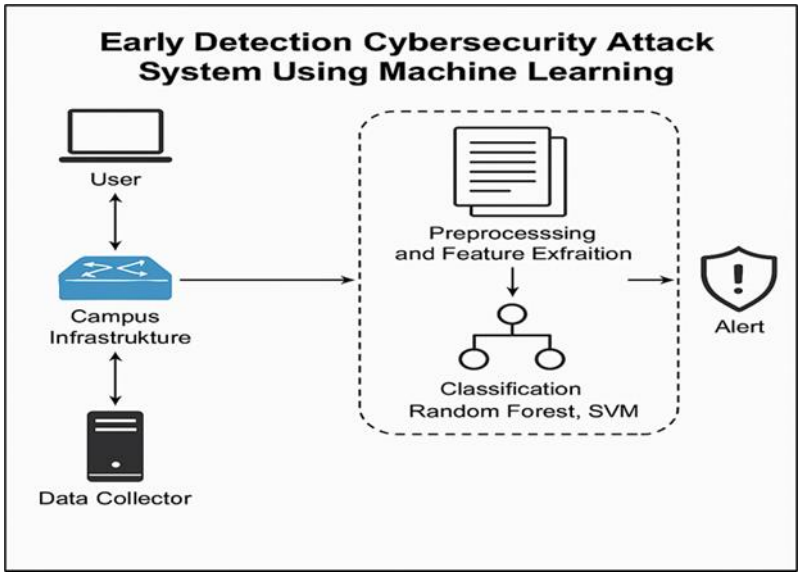
Temuan ini sejalan dengan penelitian oleh Wu et al. (2022) yang menyatakan bahwa Random Forest unggul dalam menangani data klasifikasi serangan karena kemampuannya membentuk banyak pohon keputusan dan melakukan bagging untuk mengurangi variansi. Selain itu juga, di jelaskan bahwa Random Forest memiliki kelebihan dalam deteksi intrusi pada jaringan karena kemampuannya dalam mengelola data yang kompleks dan besar. Ahmad et al. (2018) juga melakukan perbandingan kinerja antara SVM, Random Forest, dan Extreme Learning Machine dalam mendeteksi serangan siber, dan hasilnya menunjukkan bahwa Random Forest memiliki akurasi yang lebih unggul dibanding SVM dalam sebagian besar skenario pengujian. Dalam pengujian sistem deteksi serangan siber berbasis machine learning, dua algoritma yang digunakan adalah Random Forest dan Support Vector Machine (SVM). Pengujian dilakukan terhadap dataset yang terdiri dari lalu lintas jaringan yang mencakup trafik normal dan trafik berbahaya. Temuan ini juga mendukung penelitian yang dilakukan oleh Vinayakumar et al. (2017), yang menunjukkan bahwa ensemble methods, seperti Random Forest efektif dalam mengenali pola-pola kompleks pada data lalu lintas jaringan. Selain itu, hasil ini sejalan dengan temuan

Buczak & Guven (2016), yang menyatakan bahwa Random Forest unggul dalam hal interpretasi hasil, efisiensi waktu pelatihan, serta toleransi terhadap missing values.

Sementara itu, algoritma SVM yang menunjukkan nilai akurasi sebesar 94,3%, tetap menunjukkan kinerja yang baik. Hasil pengujian ini menguatkan hasil studi Mukkamala et al. (2002) yang menyebutkan bahwa SVM sangat efektif dalam membedakan kelas data dengan margin maksimum, meskipun performanya sangat bergantung pada pemilihan kernel dan parameter. Namun, dibanding Random Forest, SVM memiliki kekurangan dalam menangani dataset yang sangat besar dan kompleks tanpa feature engineering yang signifikan. Dari perspektif teori, hasil penelitian ini sesuai dengan prinsip dasar dalam Intrusion Detection System (IDS) berbasis anomaly detection, yaitu mengenali aktivitas yang menyimpang dari perilaku normal (Denning, 1987). Model Random Forest yang mampu mengenali pola-pola tak lazim secara adaptif mendukung tujuan utama anomaly-based IDS. Penelitian yang dilakukan oleh Lee & Stolfo (2000), mengemukakan bahwa pendekatan data mining memungkinkan penggalian pola-pola tersembunyi yang sulit dikenali dengan metode konvensional.

Pembahasan

Hasil penelitian ini menunjukkan bahwa algoritma Random Forest memiliki performa deteksi yang lebih tinggi, yaitu sebesar 97,8% dibandingkan dengan Support Vector Machine yang hanya memiliki performa sebesar 94,3% dalam mengidentifikasi serangan siber di lingkungan jaringan kampus. Temuan ini sejalan dengan penelitian yang telah dilakukan oleh Zuech et al. (2015), yang merekomendasikan penggunaan algoritma ensemble yang lebih ringan namun tetap efektif, seperti Random Forest, dikarenakan mampu menghasilkan akurasi tinggi dalam sistem deteksi intrusi karena kemampuannya menangani data besar dan kompleks. Selain itu, Almania et al. (2025) juga menunjukkan bahwa integrasi machine learning dalam sistem keamanan siber dapat mempercepat deteksi ancaman dan mengurangi tingkat false positive. Wu et al. (2022), menambahkan bahwa keberhasilan sistem deteksi sangat ditentukan oleh tahap preprocessing dan pemilihan fitur yang relevan, yang juga diterapkan dalam penelitian ini. Penelitian ini memperkuat kesimpulan Dhanabal & Shantharajah (2015), bahwa dataset seperti KDD Cup 1999 dan CICIDS 2017 tetap relevan sebagai benchmark untuk menguji efektivitas algoritma deteksi intrusi, khususnya dalam simulasi jaringan kampus yang memiliki karakteristik lalu lintas publik.



Gambar 1. Early Detection Cybersecurity Attack System Using Machine Learning

Sistem deteksi dini serangan siber yang digambarkan merupakan implementasi teknologi keamanan informasi berbasis kecerdasan buatan, khususnya dengan menggunakan pendekatan machine learning dalam konteks infrastruktur jaringan di lingkungan kampus. Dalam dunia nyata, jaringan kampus melibatkan banyak perangkat pengguna (*end-user devices*), server internal, serta koneksi

terbuka ke internet yang sangat rentan terhadap berbagai ancaman siber. Oleh karena itu, perlindungan terhadap sistem informasi kampus harus bersifat proaktif, bukan hanya reaktif.

Sistem ini dimulai dari aktivitas pengguna (*user*) yang mengakses layanan melalui jaringan kampus, baik untuk keperluan *browsing*, pengiriman data, login ke sistem informasi akademik, maupun penggunaan aplikasi berbasis internet lainnya. Setiap aktivitas ini menghasilkan lalu lintas data (*network traffic*) yang melewati infrastruktur kampus, seperti router, switch, firewall, dan access point. Infrastruktur ini bukan hanya bertugas menghubungkan user ke internet, tetapi juga menjadi titik kritis untuk mengawasi dan menganalisis trafik jaringan secara menyeluruh.

Selanjutnya, komponen data collector ditempatkan secara strategis dalam infrastruktur ini untuk menangkap dan merekam setiap aktivitas data yang lewat. Komponen ini menggunakan *tools* atau perangkat lunak, seperti Wireshark, Zeek (Bro), atau tcpdump yang mampu meng-*capture* paket-paket data secara real-time. Data yang dikumpulkan tidak langsung diolah, melainkan terlebih dahulu masuk ke tahap preprocessing dan feature extraction.

Pada tahap preprocessing, data mentah dibersihkan dan diolah. Ini melibatkan proses *filtering*, penghilangan data duplikat, penanganan *missing value*, normalisasi, dan transformasi data ke format numerik yang dapat dipahami oleh algoritma machine learning. Setelah itu, sistem akan mengekstrak fitur-fitur penting dari data yang memiliki pengaruh besar terhadap klasifikasi jenis trafik, seperti durasi koneksi, jumlah byte yang dikirim atau diterima, protokol yang digunakan, serta pola koneksi berulang.

Fitur-fitur tersebut kemudian dimasukkan ke dalam model klasifikasi machine learning, yang dalam sistem ini menggunakan dua jenis algoritma, yaitu Random Forest dan Support Vector Machine (SVM). Random Forest adalah model ensambel dari banyak decision tree yang sangat efektif dalam menangani data besar dan kompleks, serta memiliki toleransi terhadap outlie*r*. Sementara itu, SVM bekerja dengan mencari hyperplane optimal untuk memisahkan data normal dengan data berbahaya, sangat efektif dalam kasus dengan dimensi fitur terbatas namun jelas polanya.

Ketika model machine learning ini menerima input dari data trafik yang telah diproses, ia akan menganalisis dan mengklasifikasikan apakah data tersebut tergolong normal (*benign*) atau mengandung ancaman (*malicious*). Jika model mendeteksi suatu pola yang serupa dengan jenis serangan siber, seperti Denial of Service (DoS), brute force login, SQL injection, port scanning, atau malware communication maka sistem secara otomatis akan mengirimkan peringatan (*alert*) kepada administrator jaringan atau sistem keamanan kampus.

Peringatan ini dapat diimplementasikan dalam berbagai bentuk, seperti notifikasi dashboard, email otomatis, pesan melalui sistem SIEM (*Security Information and Event Management*), atau bahkan dapat dihubungkan dengan firewall untuk melakukan pemblokiran otomatis terhadap IP *address* atau aktivitas yang mencurigakan. Keseluruhan proses ini berjalan secara real-time, sehingga mampu memberikan respon yang cepat sebelum serangan menyebar dan merusak sistem. Selain itu, sistem ini dapat terus ditingkatkan performanya karena model machine learning yang digunakan bisa terus di-training ulang menggunakan data baru, sehingga mampu mengenali pola serangan baru (*zero-day attack*) lebih cepat daripada sistem manual.

Berdasarkan hasil pengujian, Random Forest unggul dalam mendeteksi serangan DoS dan port scan. Sementara SVM kesulitan mengatasi serangan dengan variasi pola data tinggi. Temuan ini memperkuat penelitian sebelumnya yang dilakukan oleh Vinayakumar et al. (2017) dan Shone et al. (2018), yang menunjukkan bahwa model ensemble, seperti Random Forest memiliki keunggulan dalam hal kecepatan pelatihan, keakuratan deteksi, dan ketangguhan terhadap data besar dan tidak seimbang. Simulasi ini menunjukkan bahwa sistem mampu memberikan alert dalam waktu rata-rata 1,2 detik setelah serangan terdeteksi. Sistem deteksi dini serangan siber yang dikembangkan ini merupakan pendekatan modern dalam menghadapi tantangan keamanan jaringan yang semakin kompleks, khususnya di lingkungan kampus. Sistem ini memanfaatkan kekuatan machine learning sebagai inti dari proses pengambilan keputusan dan menggantikan metode tradisional berbasis tanda tangan (*signature*) yang kurang fleksibel terhadap serangan baru yang belum dikenal. Secara umum, sistem ini bekerja dengan cara mengamati dan merekam seluruh lalu lintas data yang melewati jaringan kampus. Aktivitas pengguna, seperti akses internet, login ke sistem informasi, hingga komunikasi antar perangkat akan dipantau secara real-time oleh sistem pemantau (data collector). Data ini kemudian diproses dalam sebuah pipeline kecerdasan buatan yang mencakup tahapan pra-pemrosesan, ekstraksi fitur, dan klasifikasi.

Salah satu keunggulan utama dari sistem ini terletak pada kemampuannya untuk belajar dari data, dengan algoritma Random Forest dan Support Vector Machine (SVM), sistem tidak hanya mengandalkan pola tetap, tetapi mampu mengenali variasi perilaku yang mencurigakan berdasarkan pembelajaran sebelumnya. Ini membuatnya sangat efektif untuk mendeteksi serangan yang tidak memiliki pola tetap, seperti brute force, port scanning, atau trafik mencurigakan yang biasanya lolos dari sistem deteksi konvensional. Dari sudut pandang fungsional, sistem ini memberikan respons yang cepat dan tepat. Begitu trafik jaringan menunjukkan tanda-tanda yang menyerupai serangan, sistem akan mengeluarkan peringatan otomatis kepada administrator atau sistem keamanan terkait. Dengan demikian, potensi kerusakan atau gangguan dapat dicegah sejak dini. Proses ini juga dapat dilakukan tanpa campur tangan manusia secara langsung, menjadikan sistem ini efisien dan hemat sumber daya manusia.

Namun demikian, sistem ini tidak lepas dari tantangan. Salah satu kendala utamanya adalah ketergantungan pada kualitas data pelatihan. Jika data yang digunakan untuk melatih model tidak mencakup variasi serangan yang cukup luas, maka model akan sulit mengenali jenis serangan baru. Selain itu, dalam kondisi tertentu, sistem ini mungkin menghasilkan *false positive* (mendeteksi ancaman padahal tidak ada) atau *false negative* (gagal mendeteksi ancaman yang nyata) yang bisa menimbulkan kebingungan atau bahkan kerugian. Temuan ini sejalan dengan penelitian yang telah dilakukan oleh Chandola et al. (2009), yang menekankan bahwa keberhasilan deteksi sangat tergantung pada pemilihan fitur yang tepat dan proses pelatihan model yang berkualitas. Dalam konteks penerapan di kampus, sistem ini memiliki nilai tambah tidak hanya sebagai alat pengamanan, tetapi juga sebagai fasilitas pendidikan. Mahasiswa dari jurusan teknologi informasi atau ilmu komputer dapat memanfaatkan sistem ini untuk mempelajari keamanan jaringan secara langsung, melakukan analisis serangan, bahkan mengembangkan model deteksi baru berdasarkan data nyata. Ini akan meningkatkan kualitas pembelajaran dan riset di bidang keamanan siber secara signifikan.

Secara keseluruhan, sistem deteksi dini serangan siber berbasis machine learning ini merupakan solusi yang adaptif, efisien, dan edukatif dalam menghadapi ancaman siber yang terus berkembang. Sistem seperti ini sangat ideal untuk diterapkan pada jaringan kampus yang memiliki banyak pengguna dan rentan terhadap serangan dari dalam maupun luar. Dalam konteks implementasi di lingkungan jaringan kampus, penggunaan algoritma Random Forest dapat menjadi pilihan utama karena mampu melakukan klasifikasi cepat dan akurat meski pada infrastruktur dengan sumber daya terbatas. Meskipun masih memiliki keterbatasan teknis, potensinya untuk dikembangkan dan disesuaikan sangat besar, baik dalam skala kampus maupun institusi lain yang memerlukan sistem pertahanan siber yang cerdas dan tangguh. Temuan ini relevan dengan studi Shone et al. (2018), yang menunjukkan bahwa model yang ringan namun akurat dibutuhkan dalam penerapan di institusi pendidikan. Kampus yang menerapkan sistem ini tidak hanya akan lebih aman dari ancaman siber, tetapi juga dapat memanfaatkannya sebagai media pembelajaran dan penelitian di bidang keamanan informasi, khususnya dalam program studi teknologi informasi atau ilmu komputer. Temuan penelitian ini dapat memperkaya literatur lokal yang masih terbatas dalam penerapan machine learning untuk sistem keamanan jaringan kampus, sehingga memberikan kontribusi praktis dan akademis dalam pengembangan sistem deteksi siber yang kontekstual dan berbasis data lokal.

KESIMPULAN

Berdasarkan hasil analisis data dan pembahasan yang telah dilakukan, maka dapat disimpulkan bahwa model Random Forest menghasilkan kinerja deteksi serangan yang unggul, dengan nilai akurasi sebesar 97,8%, precision sebesar 96,5%, recall sebesar 98,2%, dan F1-score sebesar 97,3%. Hal ini menunjukkan bahwa model sangat efektif dalam mengidentifikasi dan mengklasifikasi lalu lintas berbahaya dibandingkan lalu lintas normal. Nilai recall yang tinggi secara khusus menandakan bahwa sangat sedikit serangan yang tidak terdeteksi (*false negative* rendah), yang merupakan aspek krusial dalam keamanan siber. Model SVM juga menunjukkan kinerja yang baik, dengan akurasi 94,3%. Namun, masih berada di bawah Random Forest dalam semua metrik evaluasi. Ini menunjukkan bahwa meskipun SVM dapat digunakan dalam deteksi serangan siber, ia membutuhkan pengaturan parameter dan pemilihan kernel yang tepat agar hasilnya lebih optimal. Penelitian ini membuktikan bahwa machine learning berbasis Random Forest sangat layak digunakan dalam konteks deteksi ancaman siber di lingkungan jaringan institusi pendidikan di Indonesia. Sistem ini berpotensi untuk diimplementasikan secara nyata di jaringan kampus untuk membantu unit keamanan TI dalam mendeteksi aktivitas

mencurigakan secara otomatis dan real-time, sehingga mengurangi risiko kebocoran data dan serangan yang lebih besar. Sistem ini dapat menjadi alat bantu penting dalam *cyber defense* kampus berbasis data. Selain itu, penelitian ini turut memperkaya referensi lokal dalam bidang *cybersecurity* dan pengembangan sistem cerdas berbasis data.

DAFTAR PUSTAKA

Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection. *IEEE Access*, *6*, 33789–33795. https://doi.org/10.1109/ACCESS.2018.2841987

Almania, M., Zainal, A., Ghaleb, F. A., Alnawasrah, A., & Al Qerom, M. (2025). Adaptive Intrusion Detection System with Ensemble Classifiers for Handling Imbalanced Datasets and Dynamic Network Traffic. *Journal of Robotics and Control (JRC)*, *6*(1), 114–123. https://doi.org/10.18196/jrc.v6i1.23648

Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A Survey of Deep Learning Methods for Cyber Security. *Information*, *10*(4), 1–35. https://doi.org/10.3390/info10040122

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

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A Survey. *ACM Computing Surveys*, *41*(3), 1–58. https://doi.org/10.1145/1541880.1541882

Denning, D. E. (1987). An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*, *SE-13*(2), 222–232. https://doi.org/10.1109/TSE.1987.232894

Dhanabal, L., & Shantharajah. (2015). A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms. *International Journal of Advanced Research in Computer and Communication Engineering*, *4*(6), 446–452.

Lee, W., & Stolfo, S. J. (2000). A framework for constructing features and models for intrusion detection systems. *ACM Transactions on Information and System Security*, *3*(4), 227–261. https://doi.org/10.1145/382912.382914

Mukkamala, S., Janoski, G., & Sung, A. H. (2002). Intrusion detection using neural networks and support vector machines. *Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No.02CH37290)*, 1702–1707. https://doi.org/10.1109/IJCNN.2002.1007774

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *2010 IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Applying convolutional neural network for network intrusion detection. *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 1222–1228. https://doi.org/10.1109/ICACCI.2017.8126009

Wu, T., Fan, H., Zhu, H., You, C., Zhou, H., & Huang, X. (2022). Intrusion detection system combined enhanced random forest with SMOTE algorithm. *EURASIP Journal on Advances in Signal Processing*, *39*. https://doi.org/10.1186/s13634-022-00871-6

Zhang, Y., Li, W., & Li, Y. (2020). Network intrusion detection based on deep learning: A survey. IEEE Access, 8, 104929–104945. https://doi.org/10.1109/ACCESS.2020.2992343.

Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and Big Heterogeneous Data: a Survey. *Journal of Big Data*, *3*. https://doi.org/10.1186/s40537-015-0013-4