p-ISSN: 2963-7856| e-ISSN: 2961-9890
Available online at jerkin.org/index.php/jerkin
Jurnal Pengabdian Masyarakat dan Riset Pendidikan
Volume 4 No. 3 Januari-Maret 2026, pp 14602-14607

Evaluasi Kinerja Algoritma Deep Learning Untuk Deteksi Dini Serangan Siber Pada Jaringan Komputer

Abdul Kohar[1], Aulia Rizky Muhammad Hendrik Noor Asegaff[2], Brian Sebastian Salim[3], Hamid Wijaya[4], Hariyono Rakhmad[5]
[1]Universitas Nahdlatul Ulama Cirebon
[2]Universitas Islam Kalimantan Muhammad Arsyad Al Banjari
[3]Institut Teknologi dan Bisnis Sabda Setia
[4]Universitas Sembilan Belas November Kolaka
[5]Politeknik Negeri Jember
E-mail: abd.kohar@unucirebon.ac.id
* Corresponding Author

https://doi.org/10.31004/jerkin.v4i3.4517

ARTICLE INFO

Article history
Received: 23 Nov 2025
Revised: 05 Dec 2025
Accepted: 23 Dec 2025

Kata Kunci:
deep learning, deteksi serangan siber, jaringan komputer

Keywords:
deep learning, cyber attack detection, computer networks

ABSTRACT

Perkembangan serangan siber yang semakin kompleks dan dinamis menuntut penerapan sistem deteksi intrusi yang mampu melakukan deteksi dini dengan akurasi tinggi. Penelitian ini bertujuan untuk mengevaluasi kinerja algoritma deep learning dalam mendeteksi serangan siber pada jaringan komputer melalui metode studi literatur. Studi ini mengkaji berbagai penelitian terdahulu yang relevan, termasuk penerapan arsitektur Convolutional Neural Network (CNN), VGGNet-16, dan Transformer-based deep learning, serta membandingkan performa algoritma berdasarkan metrik akurasi, precision, recall, dan F1-score. Hasil analisis menunjukkan bahwa algoritma deep learning secara konsisten lebih unggul dibandingkan pendekatan machine learning tradisional maupun metode konvensional berbasis signature dalam mengenali pola serangan yang kompleks dan dinamis. Model deep learning mampu mengekstraksi fitur secara otomatis dari data jaringan berdimensi tinggi, meningkatkan efektivitas deteksi dini, dan adaptif terhadap serangan baru, termasuk zero-day attack. Meskipun demikian, evaluasi literatur juga menunjukkan adanya variasi kinerja yang dipengaruhi oleh perbedaan dataset, metode evaluasi, dan konteks penerapan, sehingga menekankan pentingnya standardisasi evaluasi kinerja algoritma. Penelitian ini memberikan pemahaman komprehensif mengenai tren, tantangan, dan potensi pengembangan algoritma deep learning untuk sistem keamanan jaringan, sekaligus menjadi acuan bagi penelitian selanjutnya dalam meningkatkan efektivitas deteksi dini serangan siber.

The increasing complexity and dynamism of cyber attacks require intrusion detection systems capable of early detection with high accuracy. This study aims to evaluate the performance of deep learning algorithms in detecting cyber attacks on computer networks using a literature review method. The study analyzes previous research on the application of Convolutional Neural Network (CNN), VGGNet-16, and Transformer-based deep learning architectures, and compares algorithm performance based on metrics such as accuracy, precision, recall, and F1-score. The results indicate that deep learning algorithms consistently outperform traditional machine learning approaches and conventional signature-based methods in recognizing complex and dynamic attack patterns. Deep learning models can automatically extract features from high-dimensional network data, enhance early detection effectiveness, and adapt to new attacks, including zero-day attacks. However, the literature review also highlights performance variations influenced by differences in datasets, evaluation methods, and application contexts, emphasizing the importance of standardized performance evaluation. This study provides a comprehensive understanding of trends, challenges, and potential development of deep learning algorithms for network security systems, serving as a reference for future research aimed at improving early detection of cyber attacks.

This is an open access article under the CC–BY-SA license.

How to Cite: Abdul Kohar, et al (2025). Evaluasi Kinerja Algoritma Deep Learning Untuk Deteksi Dini Serangan Siber Pada Jaringan Komputer, 4(3) 14602-14607. https://doi.org/10.31004/jerkin.v4i3.4517

PENDAHULUAN

Perkembangan teknologi jaringan komputer yang semakin kompleks dan terintegrasi dengan berbagai layanan digital telah mendorong peningkatan risiko serangan siber yang bersifat dinamis dan sulit diprediksi. Jaringan komputer tidak hanya menjadi tulang punggung komunikasi data, tetapi juga menopang sistem kritis seperti layanan publik, industri, kesehatan, dan infrastruktur berbasis Internet of Things (IoT). Seiring dengan meningkatnya volume dan kecepatan lalu lintas data, pola serangan siber pun mengalami evolusi, mulai dari serangan berbasis tanda tangan (signature-based) hingga serangan canggih seperti zero-day attack yang tidak memiliki pola serangan sebelumnya. Kondisi ini menuntut sistem keamanan jaringan yang mampu melakukan deteksi dini secara adaptif dan akurat untuk meminimalkan dampak kerugian yang ditimbulkan.

Pendekatan konvensional dalam sistem deteksi intrusi (Intrusion Detection System/IDS) umumnya mengandalkan aturan statis dan teknik signature-based, yang terbukti kurang efektif dalam menghadapi serangan baru dan kompleks. Untuk mengatasi keterbatasan tersebut, berbagai penelitian mulai mengadopsi teknik kecerdasan buatan, khususnya machine learning dan deep learning, sebagai solusi yang lebih adaptif. Penelitian oleh Siswanto dan Latifah (2024), Uzlah et al. (2024), serta Inayah dan Ramli (2024) menunjukkan bahwa algoritma machine learning seperti Random Forest mampu meningkatkan akurasi deteksi serangan, meskipun masih menghadapi tantangan pada data yang tidak seimbang (unbalanced dataset) dan keterbatasan dalam mengenali pola serangan yang sangat kompleks.

Seiring dengan meningkatnya kompleksitas serangan, deep learning mulai mendapatkan perhatian lebih karena kemampuannya dalam mengekstraksi fitur secara otomatis dari data berdimensi tinggi. Beberapa studi telah mengimplementasikan model deep learning seperti Convolutional Neural Network (CNN) dan modifikasi arsitektur VGGNet-16 untuk mendeteksi serangan siber, dengan hasil performa yang relatif lebih unggul dibandingkan metode machine learning konvensional (Ilarizky & Prihantono, 2024; Soedjito, 2025). Selain itu, Farizi dan Nizam (2025) menegaskan bahwa penerapan deep learning dalam sistem deteksi intrusi mampu meningkatkan efektivitas mitigasi serangan zero-day yang sulit dideteksi oleh pendekatan tradisional.

Perkembangan lebih lanjut terlihat pada pemanfaatan arsitektur deep learning yang lebih kompleks, seperti Transformer-based model, terutama pada lingkungan jaringan berbasis IoT dan infrastruktur kritis. Penelitian oleh Fransiska dan Azhari (2025) menunjukkan bahwa Transformer memiliki keunggulan dalam menangkap dependensi jangka panjang pada data jaringan, sehingga berpotensi meningkatkan kemampuan deteksi dini serangan siber. Namun demikian, implementasi model-model tersebut umumnya masih terbatas pada skenario tertentu, seperti IoT medis atau infrastruktur spesifik, serta lebih berfokus pada pencapaian akurasi tanpa analisis komprehensif terhadap kinerja algoritma dari berbagai aspek evaluasi.

Di sisi lain, beberapa penelitian juga menyoroti pentingnya evaluasi kinerja algoritma secara menyeluruh, tidak hanya berdasarkan akurasi, tetapi juga metrik lain seperti precision, recall, F1-score, dan kemampuan generalisasi model terhadap berbagai jenis serangan. Gevindo dan Hendrik (2025) melalui systematic literature review mengungkapkan bahwa sebagian besar penelitian deteksi serangan siber masih terfragmentasi, baik dari sisi pemilihan algoritma, dataset, maupun pendekatan evaluasi. Penelitian lain oleh Mujiono et al. (2025) serta Sari et al. (2024) menunjukkan bahwa pendekatan supervised learning dan deep learning memiliki potensi besar, tetapi masih memerlukan kajian komparatif yang lebih sistematis untuk menentukan efektivitas algoritma dalam konteks deteksi dini serangan siber.

Berdasarkan uraian tersebut, research gap dalam penelitian ini terletak pada belum adanya kajian studi literatur yang secara komprehensif mengevaluasi kinerja berbagai algoritma deep learning untuk deteksi dini serangan siber pada jaringan komputer dengan pendekatan evaluasi yang terstruktur dan terintegrasi. Sebagian besar penelitian sebelumnya cenderung fokus pada implementasi satu model atau satu konteks jaringan tertentu, tanpa membandingkan kelebihan, keterbatasan, dan efektivitas algoritma deep learning secara menyeluruh. Oleh karena itu, novelty penelitian ini terletak pada penyajian evaluasi kinerja algoritma deep learning melalui metode studi literatur yang sistematis, dengan menekankan analisis komparatif antararsitektur, konteks penerapan, serta metrik evaluasi yang digunakan. Penelitian

Copyright © 2025, Jurnal Pengabdian Masyarakat dan Riset Pendidikan
ISSN 2963-7856 (print), ISSN 2961-9890 (online)

ini diharapkan mampu memberikan gambaran utuh mengenai tren, tantangan, dan peluang pengembangan algoritma deep learning sebagai solusi deteksi dini serangan siber pada jaringan komputer.

METODE

Penelitian ini menggunakan metode studi literatur dengan tujuan untuk mengevaluasi kinerja algoritma deep learning dalam deteksi dini serangan siber pada jaringan komputer. Metode ini dipilih karena mampu memberikan pemahaman komprehensif terhadap perkembangan penelitian, tren algoritma, serta hasil evaluasi yang telah dilakukan oleh peneliti sebelumnya.

1. Penentuan Topik dan Rumusan Masalah

Tahap awal penelitian dimulai dengan penentuan topik yang berfokus pada evaluasi kinerja algoritma deep learning dalam mendeteksi serangan siber pada jaringan komputer. Selanjutnya, dirumuskan permasalahan penelitian yang berkaitan dengan efektivitas, keunggulan, dan keterbatasan berbagai algoritma deep learning dalam konteks deteksi dini serangan siber.

2. Penelusuran dan Pengumpulan Literatur

Pada tahap ini dilakukan penelusuran artikel ilmiah melalui sumber-sumber akademik yang kredibel, seperti Google Scholar dan repositori jurnal nasional. Kata kunci yang digunakan meliputi *deep learning*, *intrusion detection system*, *cyber attack detection*, dan *network security*. Literatur yang dikumpulkan dibatasi pada artikel yang relevan, memiliki keterkaitan langsung dengan topik penelitian, serta diterbitkan dalam kurun waktu terbaru.

3. Seleksi dan Kriteria Inklusi Literatur

Literatur yang telah dikumpulkan kemudian diseleksi berdasarkan kriteria inklusi, yaitu penelitian yang membahas penerapan algoritma deep learning atau machine learning dalam deteksi serangan siber, menyajikan hasil evaluasi kinerja algoritma, serta menggunakan dataset jaringan komputer atau IoT. Artikel yang tidak relevan dengan fokus penelitian atau tidak menyajikan hasil evaluasi yang jelas dikeluarkan dari analisis.

4. Analisis dan Klasifikasi Literatur

Artikel terpilih dianalisis secara mendalam untuk mengidentifikasi jenis algoritma deep learning yang digunakan, konteks penerapan, dataset, serta metrik evaluasi kinerja seperti akurasi, precision, recall, dan F1-score. Selanjutnya, literatur diklasifikasikan berdasarkan pendekatan algoritma dan tujuan deteksi serangan untuk memudahkan proses perbandingan.

5. Evaluasi Kinerja Algoritma Deep Learning

Pada tahap ini dilakukan evaluasi kinerja algoritma deep learning berdasarkan hasil analisis literatur yang telah diklasifikasikan. Evaluasi difokuskan pada perbandingan performa antaralgoritma, keunggulan dan keterbatasan masing-masing pendekatan, serta efektivitasnya dalam mendeteksi serangan siber secara dini pada jaringan komputer.

6. Sintesis Temuan dan Penarikan Kesimpulan

Tahap akhir penelitian dilakukan dengan mensintesis seluruh temuan dari hasil evaluasi literatur untuk memperoleh gambaran komprehensif mengenai kinerja algoritma deep learning. Hasil sintesis digunakan untuk menarik kesimpulan, mengidentifikasi research gap, serta merumuskan kontribusi dan rekomendasi penelitian lanjutan di bidang deteksi dini serangan siber.

HASIL DAN PEMBAHASAN

Hasil

Bagian hasil penelitian ini menyajikan temuan-temuan utama yang diperoleh dari studi literatur terhadap berbagai penelitian terdahulu yang relevan dengan topik evaluasi kinerja algoritma deep learning dalam deteksi dini serangan siber pada jaringan komputer. Penyajian hasil difokuskan pada ringkasan kinerja masing-masing penelitian, meliputi efektivitas algoritma yang digunakan, kemampuan deteksi serangan, serta keunggulan dan keterbatasan pendekatan yang diterapkan. Hasil penelitian disusun secara sistematis berdasarkan setiap studi yang dianalisis untuk memberikan gambaran komprehensif mengenai perkembangan dan tren penggunaan deep learning dalam sistem keamanan jaringan.

1. Farizi dan Nizam (2025)

Hasil penelitian menunjukkan bahwa penerapan algoritma deep learning dalam sistem deteksi intrusi mampu meningkatkan kemampuan mitigasi serangan zero-day pada jaringan komputer. Model deep learning yang digunakan terbukti lebih adaptif dalam mengenali pola serangan baru dibandingkan metode konvensional. Evaluasi kinerja menunjukkan peningkatan yang signifikan pada metrik akurasi dan recall, sehingga sistem deteksi yang diusulkan efektif dalam mendukung deteksi dini serangan siber yang belum memiliki pola serangan sebelumnya.

2. Fransiska dan Azhari (2025)

Penelitian ini menunjukkan bahwa penerapan model Transformer-based deep learning memberikan kinerja yang unggul dalam mendeteksi serangan siber pada infrastruktur kritis berbasis IoT. Hasil evaluasi mengindikasikan bahwa arsitektur Transformer mampu menangkap dependensi jangka panjang pada data lalu lintas jaringan, sehingga meningkatkan akurasi dan stabilitas sistem deteksi. Temuan ini memperlihatkan bahwa deep learning dengan arsitektur modern sangat sesuai untuk lingkungan jaringan yang kompleks dan dinamis.

3. Ilarizky dan Prihantono (2024)

Hasil analisis performa pada modifikasi arsitektur VGGNet-16 menunjukkan bahwa model deep learning berbasis Convolutional Neural Network (CNN) mampu meningkatkan akurasi deteksi serangan siber dibandingkan dengan model standar. Penelitian ini menegaskan bahwa kemampuan ekstraksi fitur otomatis pada deep learning memberikan keunggulan dalam mengenali pola serangan yang kompleks, meskipun masih terdapat tantangan terkait efisiensi komputasi dan optimasi model.

4. Soedjito (2025)

Penelitian ini mengungkapkan bahwa algoritma deep learning memiliki kinerja yang tinggi dalam klasifikasi intrusi jaringan komputer. Hasil evaluasi menunjukkan nilai akurasi dan F1-score yang lebih baik dibandingkan pendekatan machine learning tradisional. Selain itu, deep learning dinilai lebih konsisten dalam mendeteksi berbagai jenis serangan, khususnya pada data jaringan yang memiliki karakteristik nonlinier dan berdimensi tinggi.

5. Gevindo dan Hendrik (2025)

Hasil systematic literature review menunjukkan adanya tren peningkatan kinerja sistem deteksi serangan siber dengan menggunakan algoritma deep learning. Namun demikian, penelitian ini juga menemukan bahwa hasil evaluasi kinerja masih bervariasi, yang dipengaruhi oleh perbedaan dataset, metode evaluasi, dan konteks penerapan. Temuan ini menegaskan pentingnya evaluasi kinerja algoritma deep learning secara komprehensif dan terstandarisasi untuk memperoleh hasil yang lebih objektif dan dapat dibandingkan.

Pembahasan

Hasil studi literatur menunjukkan bahwa penggunaan algoritma deep learning dalam deteksi dini serangan siber pada jaringan komputer merupakan pendekatan yang semakin relevan seiring dengan meningkatnya kompleksitas dan dinamika ancaman siber. Berbagai penelitian terdahulu menegaskan bahwa serangan modern, termasuk zero-day attack dan anomali lalu lintas jaringan, sulit dideteksi menggunakan metode konvensional berbasis aturan atau signature. Dalam konteks ini, deep learning menawarkan kemampuan adaptif melalui proses pembelajaran otomatis dari data jaringan yang kompleks dan berdimensi tinggi, sehingga mampu meningkatkan efektivitas sistem deteksi intrusi (Farizi & Nizam, 2025; Sinaga & Irmayani, 2024).

Secara umum, hasil pembahasan menunjukkan bahwa algoritma deep learning memiliki keunggulan dibandingkan pendekatan machine learning tradisional dalam mengenali pola serangan siber yang bersifat nonlinier dan tersembunyi. Penelitian oleh Ilarizky dan Prihantono (2024) serta Soedjito (2025) membuktikan bahwa arsitektur deep learning seperti CNN dan modifikasinya mampu mengekstraksi fitur penting dari data jaringan tanpa ketergantungan pada rekayasa fitur manual. Keunggulan ini berdampak langsung pada peningkatan kinerja deteksi, khususnya pada metrik akurasi dan F1-score, yang menunjukkan kemampuan model dalam mengklasifikasikan lalu lintas normal dan berbahaya secara lebih konsisten.

Lebih lanjut, penerapan deep learning pada berbagai konteks jaringan menunjukkan fleksibilitas dan potensi pengembangan yang luas. Fransiska dan Azhari (2025) mengungkapkan bahwa model Transformer-based deep learning memiliki kemampuan superior dalam mendeteksi serangan siber pada infrastruktur kritis berbasis IoT. Hal ini disebabkan oleh kemampuan Transformer dalam menangkap dependensi jangka panjang pada data sekuensial, yang sangat relevan dengan karakteristik lalu lintas

Copyright © 2025, Jurnal Pengabdian Masyarakat dan Riset Pendidikan
ISSN 2963-7856 (print), ISSN 2961-9890 (online)

jaringan IoT yang kompleks dan berkelanjutan. Temuan ini sejalan dengan penelitian Firdaus et al. (2025) pada jaringan IoT medis, yang menegaskan pentingnya kecerdasan buatan dalam menjaga keamanan sistem yang bersifat sensitif dan kritis.

Meskipun demikian, studi literatur juga menunjukkan bahwa pendekatan machine learning konvensional masih memiliki kontribusi penting dalam deteksi serangan siber, terutama pada skenario tertentu. Penelitian oleh Siswanto dan Latifah (2024), Uzlah et al. (2024), serta Inayah dan Ramli (2024) menunjukkan bahwa algoritma Random Forest dan XGBoost mampu memberikan performa yang cukup baik dalam mendeteksi serangan, khususnya ketika dikombinasikan dengan pengelolaan dataset yang tepat. Namun, keterbatasan utama dari pendekatan ini terletak pada ketergantungan terhadap kualitas fitur dan kesulitan dalam menangani serangan baru yang tidak memiliki pola historis yang jelas, sehingga kinerjanya cenderung lebih rendah dibandingkan deep learning pada skenario serangan kompleks.

Dari sisi evaluasi kinerja, hasil pembahasan mengindikasikan bahwa sebagian besar penelitian masih berfokus pada metrik akurasi sebagai indikator utama keberhasilan sistem deteksi. Padahal, penelitian oleh Inayah dan Ramli (2024) serta Mujiono et al. (2025) menekankan pentingnya penggunaan metrik evaluasi yang lebih komprehensif, seperti precision, recall, dan F1-score, terutama pada dataset yang tidak seimbang. Kondisi unbalanced dataset sering ditemukan pada data serangan siber, sehingga evaluasi kinerja yang tidak mempertimbangkan aspek ini berpotensi menghasilkan kesimpulan yang bias terhadap performa algoritma.

Selain itu, hasil kajian oleh Gevindo dan Hendrik (2025) melalui systematic literature review menyoroti adanya variasi yang signifikan dalam hasil evaluasi kinerja algoritma deep learning antar penelitian. Variasi ini dipengaruhi oleh perbedaan dataset, arsitektur model, teknik praproses data, serta konteks penerapan jaringan. Temuan ini mengindikasikan bahwa meskipun deep learning memiliki potensi besar, efektivitasnya tidak dapat digeneralisasi secara langsung tanpa mempertimbangkan faktor-faktor tersebut. Oleh karena itu, diperlukan pendekatan evaluasi yang lebih terstandarisasi untuk memperoleh gambaran kinerja algoritma yang lebih objektif dan dapat dibandingkan.

Secara keseluruhan, pembahasan ini menunjukkan bahwa deep learning merupakan pendekatan yang menjanjikan untuk deteksi dini serangan siber pada jaringan komputer, terutama dalam menghadapi ancaman yang kompleks dan dinamis. Namun demikian, tantangan masih ditemukan dalam aspek pemilihan arsitektur yang tepat, efisiensi komputasi, serta konsistensi evaluasi kinerja. Dengan mengintegrasikan temuan dari berbagai penelitian terdahulu, studi literatur ini memberikan pemahaman yang komprehensif mengenai posisi dan peran algoritma deep learning dalam sistem keamanan jaringan, sekaligus membuka peluang bagi penelitian lanjutan yang lebih terarah dan terstandarisasi.

SIMPULAN

Berdasarkan hasil studi literatur, dapat disimpulkan bahwa algoritma deep learning memiliki kinerja yang unggul dalam mendeteksi dini serangan siber pada jaringan komputer dibandingkan pendekatan konvensional dan machine learning tradisional. Kemampuan deep learning dalam mengekstraksi fitur secara otomatis serta mengenali pola serangan yang kompleks dan dinamis menjadikannya solusi yang efektif untuk meningkatkan sistem keamanan jaringan. Namun demikian, variasi hasil kinerja antar penelitian menunjukkan bahwa efektivitas algoritma deep learning sangat dipengaruhi oleh pemilihan arsitektur, karakteristik dataset, serta metode evaluasi yang digunakan.

SARAN

Penelitian selanjutnya disarankan untuk melakukan evaluasi kinerja algoritma deep learning secara lebih terstandarisasi dengan menggunakan dataset yang beragam dan metrik evaluasi yang komprehensif. Selain itu, pengembangan model yang mempertimbangkan efisiensi komputasi dan kemampuan generalisasi terhadap serangan baru perlu menjadi fokus utama agar sistem deteksi dini serangan siber dapat diterapkan secara optimal pada lingkungan jaringan nyata.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan dan kontribusi dalam pelaksanaan penelitian ini, baik melalui penyediaan referensi ilmiah, masukan akademik, maupun dukungan moril, sehingga penelitian ini dapat diselesaikan dengan baik.

DAFTAR PUSTAKA

Farizi, A., & Nizam, M. K. (2025). *Sistem deteksi intrusi berbasis deep learning untuk mitigasi serangan zero-day pada jaringan komputer*. Karapan Network Journal, 2(1), 45–58.

Firdaus, D., Afin, A., & Sumardi, I. (2025). *Deteksi serangan pada jaringan Internet of Things medis menggunakan machine learning dengan algoritma XGBoost*. Cyber Security dan Forensik Digital Journal, UIN Sunan Kalijaga. https://ejournal.uin-suka.ac.id/saintek/cybersecurity/article/view/5036

Fransiska, H., & Azhari, A. (2025). *Penerapan Transformer-based Deep Learning untuk deteksi dini serangan siber pada infrastruktur kritis berbasis IoT*. RIGGS: Journal of Artificial Intelligence and Cybersecurity, 7(1). https://journal.ilmudata.co.id/index.php/RIGGS/article/view/1118

Gevindo, A., & Hendrik, B. (2025). *Machine learning untuk mendeteksi serangan anomali dalam jaringan komputer: Systematic literature review*. JATI (Jurnal Mahasiswa Teknik Informatika). https://mail.ejournal.itn.ac.id/index.php/jati/article/download/13746/7624

Ilarizky, A., & Prihantono, Y. (2024). *Analisis performa pada modifikasi VGGNet-16 untuk deteksi serangan siber: Pendekatan deep learning*. Jurnal Ilmu-Ilmu Komputer, Universitas Borobudur. https://ejournal.borobudur.ac.id/index.php/08/article/view/1596

Inayah, K., & Ramli, K. (2024). *Analisis kinerja intrusion detection system berbasis algoritma Random Forest menggunakan dataset unbalanced Honeynet BSSN*. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIik), Universitas Brawijaya. https://jtiik.ub.ac.id/index.php/jtiik/article/view/8911

Mujiono, M., Larasati, D. A., & Hemansyah, M. (2025). *Deteksi anomali dalam sistem keamanan jaringan menggunakan teknik supervised machine learning*. Esensi Journal of Computer Systems, 4(2). http://esensijournal.com/index.php/infokom/article/view/221

Sari, D. P., Halim, Z., Irlon, I., & Waseso, B. (2024). *Implementasi machine learning untuk deteksi intrusi pada jaringan komputer*. Jurnal Minfo Polgan. https://www.jurnal.polgan.ac.id/index.php/jmp/article/view/14074

Sinaga, N. H., & Irmayani, D. (2024). *Mengoptimalkan keamanan jaringan memanfaatkan kecerdasan buatan untuk meningkatkan deteksi dan respon ancaman*. Jurnal Ilmu Komputer dan Komunikasi, 5(3). https://ejournal.sisfokomtek.org/index.php/jikom/article/view/3582

Siswanto, I., & Latifah, U. W. (2024). *Implementasi algoritma Random Forest untuk deteksi serangan siber pada jaringan komputer*. Science Informatics Journal, Universitas Bina Sarana Informatika. https://ejurnal.ibisa.ac.id/index.php/ji/article/view/439/386

Soedjito, V. W. (2025). *Klasifikasi intrusi jaringan menggunakan algoritma deep learning*. Universitas Atma Jaya Yogyakarta Repository. https://repository.uajy.ac.id/id/eprint/35368/

Uzlah, L. I., Saputra, R. A., & Isnawaty, I. (2024). *Deteksi serangan siber pada jaringan komputer menggunakan metode Random Forest*. JATI (Jurnal Mahasiswa Teknik Informatika). https://www.ejournal.itn.ac.id/index.php/jati/article/download/8891/5436

Copyright © 2025, Jurnal Pengabdian Masyarakat dan Riset Pendidikan
ISSN 2963-7856 (print), ISSN 2961-9890 (online)