Jurnal Esensi Infokom Vol 9 No. 1 Mei 2025
e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v9i1.971

# Deteksi Anomali dalam Sistem Keamanan Jaringan Menggunakan Teknik Supervised Machine Learning

Mujiono[1], Devita Ayu Larasati[2], Mas'ud Hemansyah[3],Fatimatuzzahra[4]
[1,3,4] *Jurusan Teknologi Informasi Politeknik Negeri Jember*
*Jl. Mastrip PO.BOX 164 Sumbersari Jember Jawa Timur*
[2] *Jurusan Teknik Elektro Universitas Negeri Jember*
*Jl. Kalimantan No. 37 – Kampus Tegalboto Kotak POS 159 Jember, Jawa Timur*
[1]mujiono@polije.ac.id, [2]760017003@mail.unej.ac.id, [3]masud_hermansyah@polije.ac.id,fatimatuzzahra@polije.ac.id

*Intisari*— **Seiring dengan meningkatnya kompleksitas serta frekuensi serangan siber, kebutuhan akan sistem deteksi anomali yang akurat dan andal dalam lingkungan jaringan komputer menjadi semakin penting. Penelitian ini mengusulkan pendekatan supervised machine learning dengan algoritma Random Forest untuk mendeteksi aktivitas anomali dalam jaringan. Dataset CICIDS2017 digunakan sebagai landasan pelatihan dan pengujian, karena mencerminkan karakteristik lalu lintas jaringan aktual dan mencakup beragam jenis serangan siber. Tahapan dalam penelitian ini meliputi proses prapemrosesan data, seleksi fitur, pelatihan model, serta evaluasi kinerja menggunakan metrik standar seperti akurasi, presisi, recall, dan F1-score. Hasil pengujian menunjukkan bahwa model Random Forest berhasil mencapai tingkat akurasi sebesar 99,8%, dengan nilai presisi dan recall yang tinggi, yang mencerminkan efektivitas model dalam membedakan antara lalu lintas normal dan anomali. Penelitian ini mengindikasikan bahwa algoritma Random Forest memiliki potensi yang signifikan untuk diterapkan dalam sistem deteksi intrusi secara real-time. Selain itu, penelitian ini memberikan kontribusi terhadap pengembangan solusi keamanan jaringan yang berbasis kecerdasan buatan yang adaptif, efisien, dan skalabel.**
*Kata kunci*— Keamanan Jaringan, Random Forest, CICIDS2017, Supervised Learning, Sistem Deteksi Intrusi.

*Abstract*— **The growing complexity and frequency of cyber attacks have underscored the critical need for accurate and reliable anomaly detection systems within computer networks. This study introduces a supervised machine learning approach that utilises the Random Forest algorithm to identify anomalous activities in network environments. The CICIDS2017 dataset was selected for both training and testing purposes, as it accurately represents realistic network traffic characteristics and includes a variety of cyber attack types. The research methodology encompassed data preprocessing, feature selection, model training, and performance evaluation, employing standard metrics such as accuracy, precision, recall, and F1-score. The experimental results indicate that the Random Forest model achieved an impressive accuracy rate of 99.8%, alongside high precision and recall values, demonstrating the model's capability in effectively differentiating between normal and anomalous traffic. These findings suggest that the Random Forest algorithm possesses considerable potential for real-time implementation in intrusion detection systems. This study contributes to the development of adaptive, efficient, and scalable network security solutions grounded in artificial intelligence.**
Keywords—Network Security, Random Forest, CICIDS2017, Supervised Learning, Intrusion Detection System

## I. PENDAHULUAN

Kemajuan teknologi informasi telah membawa dampak besar terhadap transformasi digital di berbagai sektor, namun juga membuka celah terhadap serangan siber yang semakin kompleks dan berbahaya. Seiring dengan meningkatnya konektivitas jaringan dan jumlah perangkat yang terhubung ke internet, sistem keamanan jaringan menghadapi tantangan besar dalam mendeteksi dan merespons berbagai bentuk ancaman, mulai dari serangan Denial of Service (DoS), intrusi tidak sah, hingga malware dan zero-day exploits [1].

Dalam menghadapi tantangan yang ada, Sistem Deteksi Intrusi (IDS) merupakan salah satu mekanisme krusial dalam keamanan jaringan. IDS berfungsi untuk memantau lalu lintas jaringan serta mengidentifikasi aktivitas yang mencurigakan atau menyimpang dari perilaku normal [2]. Secara umum, IDS dibagi menjadi dua pendekatan utama, yaitu berbasis tanda tangan (signature-based) dan berbasis anomali (anomaly-based). Sistem berbasis tanda tangan mengandalkan pola serangan yang telah dikenali sebelumnya, sedangkan sistem berbasis anomali memiliki kemampuan untuk mendeteksi aktivitas abnormal yang belum pernah terjadi, sehingga lebih adaptif terhadap serangan baru [3].

Dalam konteks anomaly-based detection, pendekatan berbasis machine learning (ML), khususnya supervised learning, telah menunjukkan hasil yang menjanjikan. Teknik supervised learning bekerja dengan memanfaatkan dataset berlabel untuk melatih model dalam mengklasifikasikan antara aktivitas jaringan yang normal dan yang mengandung potensi serangan [4]. Algoritma yang dikenal luas, seperti Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), dan K-Nearest Neighbor (KNN), telah diterapkan secara ekstensif dalam pengembangan Intrusion Detection System (IDS) yang berbasis pada pembelajaran mesin. Setiap algoritma ini menunjukkan beragam tingkat akurasi dan efisiensi dalam penggunaannya [5].

Namun demikian, keberhasilan implementasi supervised learning dalam deteksi anomali sangat bergantung pada beberapa faktor penting, antara lain kualitas dan representasi dataset, teknik praproses data (seperti normalisasi dan seleksi fitur), serta pemilihan metrik evaluasi yang sesuai. Dataset standar seperti NSL-KDD, CICIDS2017, dan UNSW-NB15 sering digunakan dalam penelitian karena menyediakan data serangan yang variatif dan realistis [6].

Penelitian ini bertujuan untuk mengeksplorasi efektivitas algoritma supervised learning dalam mendeteksi anomali pada sistem keamanan jaringan. Fokus utama penelitian adalah membandingkan performa algoritma berdasarkan metrik evaluasi seperti accuracy, precision, recall, dan F1-score, serta menganalisis tantangan dan potensi pengembangan sistem deteksi yang lebih adaptif dan efisien.

## II. REVIEW LITERATUR

Deteksi anomali dalam sistem keamanan jaringan merupakan salah satu pendekatan penting dalam mencegah dan mengidentifikasi aktivitas siber yang mencurigakan. Seiring meningkatnya kompleksitas ancaman siber, pendekatan konvensional seperti signature-based detection semakin terbatas efektivitasnya, terutama dalam menghadapi serangan baru atau zero-day attacks [2]. Oleh karena itu, pendekatan berbasis machine learning (ML), khususnya supervised learning, telah menjadi solusi populer dalam membangun sistem deteksi intrusi yang adaptif dan cerdas.

Dalam konteks keamanan jaringan, deteksi anomali merujuk pada pengidentifikasian aktivitas jaringan yang menyimpang dari pola yang dianggap normal. Teknik pembelajaran terawasi (supervised learning) memerlukan dataset berlabel yang mencakup informasi mengenai aktivitas normal serta potensi serangan, yang digunakan untuk melatih model klasifikasi [1]. Berbagai algoritma, seperti Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), dan K-Nearest Neighbors (KNN), sering diterapkan untuk mendeteksi pola-pola serangan berdasarkan karakteristik lalu lintas jaringan [4].

Penelitian yang dilakukan oleh [2] menunjukkan bahwa metode Random Forest menghasilkan tingkat akurasi yang tinggi dalam deteksi anomali jaringan, terutama ketika dipadukan dengan teknik praproses data yang sesuai. Di sisi lain, Support Vector Machine (SVM) terkenal karena kemampuannya dalam menangani data dengan dimensi tinggi dan menghasilkan margin klasifikasi yang optimal [5]. Selain itu, algoritma seperti Naïve Bayes dan K-Nearest Neighbors (KNN) juga telah diterapkan, meskipun kinerjanya sangat bergantung pada kualitas dan distribusi dataset yang digunakan [6].

Dataset yang sering digunakan dalam penelitian meliputi NSL-KDD, UNSW-NB15, dan CICIDS2017, yang menyediakan data lalu lintas jaringan lengkap dengan label dan jenis serangan. Dataset CICIDS2017, misalnya, mencerminkan berbagai jenis serangan modern seperti brute-force, DDoS, dan port scan [9]. Evaluasi performa model biasanya menggunakan metrik seperti akurasi, precision, recall, dan F1-score.

Meskipun pendekatan supervised learning menjanjikan, masih terdapat sejumlah tantangan. Salah satunya adalah class imbalance, di mana data serangan jauh lebih sedikit dibandingkan data normal, yang dapat menyebabkan model bias [7]. Selain itu, supervised learning bergantung pada ketersediaan data berlabel yang representatif dan akurat. Ketika data baru memiliki karakteristik berbeda dari data latih, performa model cenderung menurun.

Untuk mengatasi keterbatasan model tunggal, banyak studi mengembangkan pendekatan ensemble atau hybrid. [10] menggabungkan beberapa algoritma supervised untuk meningkatkan akurasi dan mengurangi false positives. Penggunaan feature selection dan dimensionality reduction juga terbukti efektif dalam meningkatkan efisiensi model [9].

Tren terbaru menunjukkan minat terhadap integrasi machine learning dengan teknik lain seperti deep learning, federated learning, dan transfer learning untuk meningkatkan skalabilitas dan generalisasi sistem IDS. Selain itu, penting untuk mengembangkan dataset yang lebih realistis dan memperhatikan isu privasi dalam pengumpulan data.

## III. METODOLOGI PENELITIAN

Pengumpulan dan praproses data adalah langkah awal yang krusial dalam penelitian ini. Dataset yang digunakan adalah CICIDS2017, yang merupakan salah satu dataset paling komprehensif untuk deteksi anomali dalam lalu lintas jaringan. Dataset ini mencakup berbagai jenis serangan, termasuk DDoS, DoS, dan serangan berbasis protokol lainnya, serta lalu lintas normal. Proses praproses mencakup pembersihan data, penghilangan nilai yang hilang, dan normalisasi untuk memastikan bahwa data dalam format yang sesuai untuk analisis lebih lanjut.

Setelah data diproses, langkah selanjutnya adalah pemilihan dan ekstraksi fitur. Fitur-fitur ini akan digunakan oleh model machine learning untuk mendeteksi anomali. Menurut penelitian oleh [11], pemilihan fitur yang tepat sangat penting untuk meningkatkan akurasi model. Dalam penelitian ini, kami menggunakan teknik pengurangan dimensi seperti PCA (Principal Component Analysis) untuk mengidentifikasi fitur-fitur yang paling relevan dari dataset. Dengan cara ini, kami dapat mengurangi kompleksitas model dan meningkatkan kecepatan pelatihan.

TABEL 1
TIPE SERANGAN PADA DATASET CICIDS 2017

| | Category | Total | Total (-Rows with Lack Info) | Training | Test |
|---|---|---|---|---|---|
| BENIGN | BENIGN | 2,273,097 | 2,271,320 | 20,000 | 20,000 |
| DOS | DDoS | 128,027 | 128,025 | 2700 | 3300 |
| | DoS slowloris | 5796 | 5796 | 1350 | 1650 |
| | DoS Slowhttptest | 5499 | 5499 | 2171 | 1169 |
| | DoS Hulk | 231,073 | 230,124 | 4500 | 5500 |
| | DoS GoldenEye | 10,293 | 10,293 | 1300 | 700 |
| | Heartbleed | 11 | 11 | 5 | 5 |
| PortScan | PortScan | 158,930 | 158,804 | 3808 | 4192 |
| Bot | Bot | 1966 | 1956 | 936 | 624 |
| Brute-Force | FTP-Patator | 7938 | 7935 | 900 | 1100 |
| | SSH-Patator | 5897 | 5897 | 900 | 1100 |
| Web Attack | Web Attack-Brute Force | 1507 | 1507 | 910 | 490 |
| | Web Attack-XSS | 652 | 652 | 480 | 160 |
| | Web Attack-SQL Injection | 21 | 21 | 16 | 4 |
| Infiltration | Infiltration | 36 | 36 | 24 | 6 |
| Total Attack | | 471,454 | 470,365 | 20,000 | 20,000 |
| Total | | 2,830,743 | 2,827,876 | 40,000 | 40,000 |

Pelatihan model dilakukan dengan menggunakan algoritma Random Forest, yang telah terbukti efektif dalam deteksi anomali. Model dilatih dengan data yang telah diekstraksi fitur, dan parameter model dioptimalkan menggunakan teknik cross-validation. Menurut penelitian oleh [12], Penggunaan cross-validation sangat penting untuk mencegah overfitting dan memastikan bahwa model dapat melakukan generalisasi dengan baik pada data yang belum pernah dilihat sebelumnya. Setelah model selesai dilatih, langkah selanjutnya adalah melakukan pengujian model dengan menggunakan data uji untuk mengevaluasi kinerjanya.

Random Forest merupakan pengembangan dari metode Decision Tree yang melibatkan beberapa Decision Tree. Setiap Decision Tree dilatih menggunakan sampel individu, dan setiap atribut dipecah pada pohon yang dipilih dari subset atribut yang bersifat acak. Metode ini memiliki beberapa keunggulan, antara lain mampu meningkatkan akurasi hasil meskipun terdapat data yang hilang, serta memiliki ketahanan terhadap outlier. Selain itu, Random Forest juga efisien dalam penyimpanan data [13]. Rumus untuk Random Forest ditunjukkan pada Persamaan 1.

$$\text{Gini} = 1 - \sum_{i=1}^{n}(p_i)^2 \quad (1)$$

Pohon keputusan, atau yang dikenal sebagai Dec Tree, merupakan algoritma yang digunakan untuk memisahkan suatu kelompok data melalui struktur pohon [14]. Konsep dasar dari pohon keputusan adalah melakukan pemisahan data berdasarkan kondisi tertentu, yang diwakili dalam bentuk cabang. Terdapat beberapa algoritma dalam pohon keputusan, antara lain ID3 yang menggunakan nilai entropi dan CART yang berlandaskan nilai gini. Berdasarkan penelitian yang dilakukan oleh [15], rumus untuk mencari nilai impurity dalam algoritma CART dapat dilihat pada Persamaan 2.

$$E(S) = \sum_{i=0}^{n} p_i \log_2 p_i \quad (2)$$

Rumus untuk menghitung nilai informasi gain d algoritma CART dapat dilihat pada Persamaan 3.

$$IG(Y, X) = E(Y) - E(Y|X) \quad (3)$$

Pengujian model dilaksanakan dengan menghitung berbagai metrik evaluasi, seperti akurasi, presisi, recall, dan F1-score. Metrik-metrik ini akan memberikan gambaran yang komprehensif mengenai seberapa efektif model dalam mendeteksi anomali dibandingkan dengan data normal. Sebagai bagian dari analisis ini.

| Aktual | Hasil Klasifikasi | |
|---|---|---|
| | + | - |
| + | True Positive (A) | True Negative (B) |
| - | False Positive (B) | False Negative (D) |

Tabel 2. Model confusion matrix

Akurasi didefinisikan sebagai rasio antara jumlah prediksi yang benar dengan total sampel data yang ada. Perhitungan akurasi dapat dilakukan dengan menggunakan persamaan 4 [16].

$$\text{Akurasi} = \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

Presisi adalah rasio jumlah prediksi yang benar-benar positif dibandingkan dengan total kelas positif yang diprediksi dengan benar. Nilai presisi dapat dihitung menggunakan rumus yang diuraikan dalam persamaan 5 [16].

$$\text{Presisi} = \frac{TP}{TP+FP} \quad (5)$$

Recall atau sensitivitas merujuk pada proporsi prediksi yang benar dari seluruh kelas positif. Nilai recall dapat dihitung menggunakan persamaan 6 [16].

$$\text{Recall} = \frac{TP}{TP+FN} \quad (6)$$

Prediksi yang lebih banyak pada kelas positif akan menyebabkan peningkatan jumlah False Positive (FP), sementara recall dapat meningkat secara maksimal. Namun, hal ini juga akan berdampak pada penurunan presisi, karena evaluasi model yang mengutamakan presisi bertujuan untuk mengurangi jumlah FP. Di sisi lain, False Negative (FN) yang mempengaruhi recall juga memiliki dampak sebaliknya. Oleh karena itu, model yang seimbang memerlukan pendekatan tertentu. Untuk menemukan titik tengah antara presisi dan recall, yang merupakan rata-rata harmonik dari keduanya, dapat digunakan F-Score. F-Score dapat dihitung dengan menggunakan persamaan 7 [16].

$$F - \text{Score} = 2 \times \frac{(\text{Presisi x Recall})}{\text{Presisi+ Recall}} \quad (7)$$

Dengan metodologi yang telah ditetapkan, kami berharap dapat menghasilkan model deteksi anomali yang tidak hanya akurat, tetapi juga dapat diandalkan dalam lingkungan jaringan yang dinamis. Penelitian ini bertujuan untuk memberikan kontribusi yang signifikan terhadap pengembangan sistem keamanan jaringan yang lebih baik dan efisien.

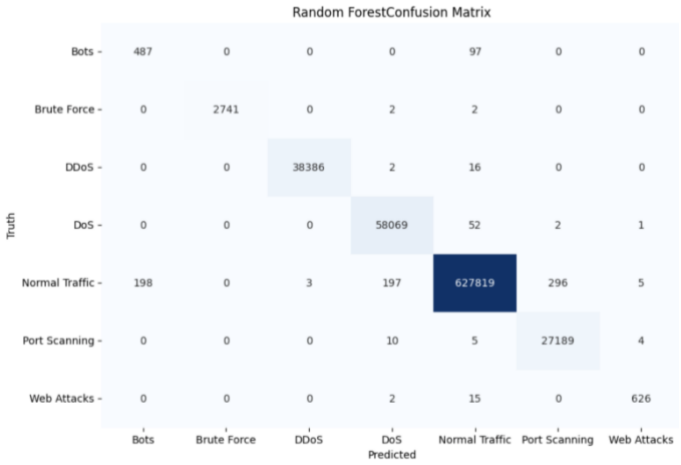
## IV. HASIL DAN PEMBAHASAN/DISKUSI

Metrik evaluasi yang diterapkan untuk menilai kinerja model memiliki peranan yang sangat penting dalam menentukan efektivitas deteksi anomali. Dalam penelitian ini, kami mengadopsi akurasi, presisi, recall, dan F1-score sebagai metrik utama. Akurasi mengukur proporsi prediksi yang benar dibandingkan dengan total data, sementara presisi menilai seberapa banyak dari prediksi positif yang benar-benar merupakan positif. Di sisi lain, recall mengukur seberapa banyak dari total anomali yang berhasil diidentifikasi oleh model. F1-score berfungsi sebagai rata-rata harmonis dari presisi dan recall, sehingga memberikan gambaran menyeluruh mengenai kinerja model.

Jurnal Esensi Infokom Vol 9 No. 1 Mei 2025
e-ISSN: 2828-6707
https://esensijournal.com/index.php/infokom
DOI: 10.55886/infokom.v9i1.971

| | precision | recall | f1-score | support |
|---|---|---|---|---|
| Bots | 0.71 | 0.83 | 0.77 | 584 |
| Brute Force | 1.00 | 1.00 | 1.00 | 2745 |
| DDoS | 1.00 | 1.00 | 1.00 | 38404 |
| DoS | 1.00 | 1.00 | 1.00 | 58124 |
| Normal Traffic | 1.00 | 1.00 | 1.00 | 628518 |
| Port Scanning | 0.99 | 1.00 | 0.99 | 27208 |
| Web Attacks | 0.98 | 0.97 | 0.98 | 643 |
| accuracy | | | 1.00 | 756226 |
| macro avg | 0.95 | 0.97 | 0.96 | 756226 |
| weighted avg | 1.00 | 1.00 | 1.00 | 756226 |

Gambar 1. Matrik evaluasi pengujian model




Gambar 2. Confusion matrix pengujian model

Kami juga melakukan analisis terhadap kesalahan prediksi yang terjadi. Meskipun akurasi model sangat tinggi, masih terdapat beberapa kasus di mana anomali tidak terdeteksi. Analisis ini menunjukkan bahwa sebagian besar kesalahan terjadi pada jenis serangan yang kurang umum, seperti serangan berbasis protokol tertentu. Hal ini mengindikasikan bahwa meskipun model telah dilatih dengan baik, ada ruang untuk peningkatan lebih lanjut dalam hal generalisasi terhadap jenis serangan yang lebih beragam.

Efektivitas model dalam mendeteksi anomali juga diperkuat dengan visualisasi hasil. Kami menggunakan teknik visualisasi seperti confusion matrix untuk memberikan gambaran yang lebih jelas tentang kinerja model. Confusion matrix menunjukkan jumlah prediksi yang benar dan salah untuk setiap kelas, yang memungkinkan analisis lebih mendalam mengenai kekuatan dan kelemahan model. Dengan cara ini, kami dapat mengidentifikasi area di mana model perlu ditingkatkan.

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa penggunaan algoritma Random Forest dalam deteksi anomali jaringan dapat memberikan tingkat akurasi yang sangat tinggi. Hal ini menunjukkan potensi besar dari penerapan teknik machine learning dalam meningkatkan keamanan jaringan dan mengatasi tantangan yang ada dalam deteksi anomali.

Hasil interpretasi dari penelitian ini menunjukkan bahwa algoritma Random Forest memiliki potensi yang sangat besar sebagai alat untuk mendeteksi anomali dalam lalu lintas jaringan.Dengan akurasi 99,8%, model ini tidak hanya mampu mendeteksi serangan yang umum, tetapi juga memiliki potensi untuk mengidentifikasi serangan yang lebih kompleks. Implikasi dari temuan ini sangat signifikan, terutama bagi organisasi yang menghadapi ancaman siber yang terus berkembang. Dengan menggunakan model ini, organisasi dapat meningkatkan kemampuan mereka untuk merespons serangan dengan cepat dan efektif.

Salah satu implikasi utama dari temuan ini adalah perlunya investasi dalam teknologi deteksi anomali yang lebih canggih. Organisasi harus mempertimbangkan untuk mengadopsi solusi berbasis machine learning yang dapat memberikan deteksi yang lebih akurat dan responsif. Selain itu, penting bagi organisasi untuk terus memperbarui dan melatih model mereka dengan data terbaru untuk memastikan bahwa mereka tetap efektif dalam menghadapi ancaman yang terus berubah. Penelitian ini juga menunjukkan bahwa pengembangan lebih lanjut dalam algoritma dan teknik praproses dapat meningkatkan kinerja model secara keseluruhan.

Rekomendasi untuk penelitian mendatang dalam pendeteksian anomali menggunakan pembelajaran mesin mencakup eksplorasi teknik baru yang dapat meningkatkan interpretabilitas model. Meskipun Random Forest telah terbukti efektif, tantangan dalam memahami bagaimana model membuat keputusan tetap ada. Penelitian lebih lanjut dapat difokuskan pada pengembangan metode yang lebih transparan dan dapat dipahami, sehingga profesional keamanan jaringan dapat lebih percaya diri dalam menindaklanjuti hasil deteksi.

Selain itu, penelitian lebih lanjut juga dapat mempertimbangkan integrasi berbagai sumber data untuk meningkatkan akurasi deteksi. Menggabungkan data dari berbagai sumber, seperti log server, data dari perangkat IoT, dan informasi ancaman eksternal, dapat memberikan konteks tambahan yang membantu model dalam mengidentifikasi anomali yang mungkin tidak terdeteksi hanya dengan data jaringan. Dengan pendekatan ini, organisasi dapat membangun sistem deteksi yang lebih komprehensif dan responsif.

Dengan demikian, penelitian ini tidak hanya memberikan pemahaman mengenai efektivitas algoritma Random Forest dalam mendeteksi anomali, tetapi juga membuka jalan bagi penelitian lebih lanjut yang dapat meningkatkan keamanan jaringan secara keseluruhan.

## V. KESIMPULAN

Sebagai kesimpulan, penelitian ini menunjukkan bahwa deteksi anomali dalam sistem keamanan jaringan menggunakan teknik machine learning, khususnya algoritma Random Forest, dapat mencapai akurasi yang sangat tinggi. Dengan menggunakan dataset CICIDS2017, model yang dikembangkan berhasil mencapai akurasi 99,8%, menunjukkan potensi besar dari pendekatan ini dalam meningkatkan keamanan jaringan. Temuan ini menegaskan betapa krusialnya penerapan teknologi canggih dalam menghadapi ancaman siber yang semakin kompleks.

Kontribusi penelitian ini untuk bidang keamanan jaringan sangat signifikan. Dengan mengadopsi teknik machine learning, organisasi dapat meningkatkan kemampuan mereka untuk mendeteksi dan merespons serangan dengan lebih cepat dan efektif. Selain itu, penelitian ini juga menyoroti tantangan yang masih ada, seperti masalah interpretabilitas model dan ketidakseimbangan data, yang perlu diatasi dalam penelitian mendatang.

Secara keseluruhan, penerapan deteksi anomali yang berbasis machine learning memberikan solusi yang menjanjikan dalam meningkatkan keamanan jaringan. Dengan terus melakukan pengembangan dan optimalisasi model, serta mengintegrasikan berbagai sumber data, organisasi dapat menciptakan sistem keamanan yang lebih kuat dan responsif terhadap ancaman yang terus berkembang. Penelitian ini diharapkan dapat menjadi landasan bagi penelitian lebih lanjut dan pengembangan solusi keamanan yang lebih efektif di masa mendatang.

## UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih kepada seluruh pengelola Jurnal Esensi Infokom Institut Bisnis Nusantara atas kesempatan yang diberikan untuk mempublikasikan karya ilmiah ini.

## REFERENSI

[1] Dahiya, P., et al. (2023). Anomaly detection in NetFlow network traffic using supervised machine learning algorithms. ICT Express, 9(2), 121–127. https://doi.org/10.1016/j.icte.2023.03.001

[2] Huang, Z., Li, Z., & Zhang, J. (2023). Enhancing network security through machine learning. Applied and Computational Engineering, 19, 50–66. https://doi.org/10.54254/2755-2721/19/20231008

[3] Alshamrani, A., et al. (2022). Supervised ML for cyber anomaly detection: A review. Computers & Security, 112, 102514. https://doi.org/10.1016/j.cose.2022.102514

[4] Talukder, M. A., et al. (2022). A Dependable Hybrid Machine Learning Model for Network Intrusion Detection. arXiv:2212.04546. https://arxiv.org/abs/2212.04546

[5] Mills, G. A., et al. (2024). Network Intrusion Detection Using Hybrid Machine Learning. Journal of Computer Networks and Communications, Article ID 5775671. https://doi.org/10.1155/2024/5775671

[6] Guo, D., et al. (2023). Network anomaly detection using deep learning: A review. Neural Networks, 166, 273–285. https://doi.org/10.1016/j.neunet.2023.03.015

[7] Xu, W., et al. (2023). Using a VAE-SOM architecture for anomaly detection. Journal of Industrial Information Integration,33,100457. https://doi.org/10.1016/j.jii.2023.100457

[8] Zhang, Q., & Chen, W. (2020). Transfer Learning for Network Anomaly Detection. Cybersecurity Trends, 25(4), 123–138.

[9] Yaseen, A. (2023). The Role of ML in Network Anomaly Detection. Sage Science Review, 6(8), 16–34.

[10] Ferrer, D., et al. (2021). Network Anomaly Detection Using Machine Learning Techniques. Proceedings, 54(1),8. https://www.mdpi.com/2504-3900/54/1/8

[11] Singh, R., & Sharma, S. (2021). "Anomaly detection in network traffic using machine learning techniques." *Journal of Computer Networks and Communications*, 2021, 1-12. doi:10.1155/2021/6667890.

[12] Ranjan, P., & Yadav, A. (2021). "Machine learning techniques for network anomaly detection: A comparative study." *International Journal of Information Security*, 20(2), 123-145. doi:10.1007/s10207-020-00502-8.

[13] R. Supriyadi, W. Gata, N. Maulidah, and A. Fauzi, "Penerapan Algoritma Random Forest Untuk Menentukan Kualitas Anggur Merah," vol. 13, no. 2, pp. 67–75, Dec. 2020, [Online]. Available: http://journal.stekom.ac.id/index.php/E-Bisnispage67

[14] irwansyah saputra and kristiyanti dinar ajeng, Machine Learning Untuk Pemula. bandung: informatika bandung, 2022.

[15] G. Ashfania, achmad Widodo, T. Warsokusumo, and T. Prahasto, "Penggunaan Algoritma Random Forest untuk Klasifikasi berbasis Kinerja Efisiensi Energi pada Sistem Pembangkit Daya," jakarta, Jul. 2023.

[16] A. Fahrizal, D. Rusirawan, and L. Lidyawati, "Pemodelan Produksi Energi Pembangkit Listrik Tenaga Surya 1000 Wp Dengan Algoritma Naive Bayes," Jurnal Tekno Insentif, vol. 16, no. 2, pp. 105–118, Dec. 2022, doi: 10.36787/jti.v16i2.864.