Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 7 Nomor1, 2024
P-2655-710X e-ISSN 2655-6022

*Submitted : 16/01/2024*
*Reviewed : 17/01/2024*
*Accepted : 26/01/2024*
*Published : 27/01/2024*

**Grace Martha Geertruida Bororing**[1]

# PENGEMBANGAN ALGORITMA MACHINE LEARNING UNTUK MENDETEKSI ANOMALI DALAM JARINGAN KOMPUTER

**Abstrak**

Penelitian ini menggali perkembangan terkini dalam pengembangan algoritma machine learning untuk mendeteksi anomali dalam jaringan komputer. Studi literatur yang mendalam mengidentifikasi berbagai metode, dari pendekatan berbasis statistik hingga teknik pengklasifikasi dan clustering. Analisis literatur membahas kelebihan dan kelemahan masing-masing metode, sambil menyoroti kompleksitas serta tantangan yang dihadapi dalam mendeteksi serangan yang semakin canggih. Pentingnya evaluasi performa dengan metrik yang tepat, seperti akurasi, sensitivitas, dan spesifisitas, menjadi fokus utama dalam memahami efektivitas algoritma deteksi anomali. Hasil penelitian memberikan wawasan tentang trade-off antara keakuratan dan efisiensi komputasi, membuka pintu untuk pengembangan algoritma yang dapat memberikan keseimbangan optimal. Saran untuk penelitian selanjutnya mencakup eksplorasi lebih lanjut terhadap integrasi teknik deep learning dan uji coba pada dataset yang lebih bervariasi. Pengembangan algoritma yang adaptif terhadap perubahan taktik penyerangan juga diusulkan sebagai langkah proaktif dalam menghadapi evolusi serangan. Penelitian ini memiliki implikasi positif terhadap keamanan jaringan komputer, dengan kontribusi pada pemahaman mendalam tentang metode deteksi anomali yang dapat memberikan perlindungan yang lebih efektif. Kesimpulan menegaskan bahwa pemahaman lebih lanjut terhadap aspek teknis dan implementasi praktis algoritma machine learning dapat memperkuat pertahanan terhadap serangan anomali di lingkungan jaringan komputer.

**Kata Kunci:** Machine Learning, Deteksi Anomali, Keamanan Jaringan Komputer, Integrasi Teknologi Terkini.

**Abstract**

This research explores the recent developments in the development of machine learning algorithms for detecting anomalies in computer networks. A comprehensive literature review identifies various methods, ranging from statistically-based approaches to classification and clustering techniques. The literature analysis discusses the strengths and weaknesses of each method while highlighting the complexity and challenges faced in detecting increasingly sophisticated attacks. The importance of performance evaluation using appropriate metrics, such as accuracy, sensitivity, and specificity, is a primary focus in understanding the effectiveness of anomaly detection algorithms. The research findings provide insights into the trade-off between accuracy and computational efficiency, paving the way for the development of algorithms that can strike an optimal balance. Recommendations for further research include further exploration of integrating deep learning techniques and testing on more diverse datasets. The development of algorithms adaptive to changing attack tactics is also suggested as a proactive step in addressing the evolution of attacks. This research has positive implications for computer network security, contributing to a deeper understanding of anomaly detection methods that can

[1]Program Studi Teknik Informatika, Fakultas Komputer dan Komunikasi, Institut Bisnis dan Informatika Kwik Kian Gie
email: grace.martha@kwikkiangie.ac.id

offer more effective protection. The conclusion emphasizes that further understanding of the technical aspects and practical implementation of machine learning algorithms can strengthen defenses against anomalous attacks in computer network environments.
**Keywords:** Machine Learning, Anomaly Detection, Computer Network Security, Integration of Latest Technologies.

## PENDAHLUAN

Dalam dunia yang semakin terhubung dan tergantung pada teknologi, jaringan komputer telah menjadi fondasi esensial bagi kelangsungan berbagai sektor kehidupan manusia. Secara khusus, aspek bisnis, pendidikan, dan komunikasi kini sangat bergantung pada keberlanjutan dan kehandalan infrastruktur jaringan komputer (Nururrahmah, 2023). Dengan pertumbuhan ketergantungan ini, muncul kebutuhan yang mendesak akan peningkatan keamanan guna melindungi integritas dan ketersediaan jaringan tersebut. Keamanan jaringan komputer menjadi isu yang semakin mendalam mengingat peran krusialnya dalam mendukung berbagai kegiatan manusia. Dalam konteks bisnis, kebanyakan transaksi dan operasi perusahaan dilakukan melalui jaringan komputer, membutuhkan lapisan keamanan yang kuat untuk melindungi data dan informasi yang terus mengalir. Di sisi pendidikan, integrasi teknologi dalam proses pembelajaran menuntut adanya keamanan yang lebih ketat guna melindungi privasi siswa dan kelancaran pengelolaan data akademis.

Namun, semakin kompleksnya teknologi juga membuka pintu bagi serangan yang lebih canggih dan sulit dideteksi. Salah satu ancaman yang patut diperhatikan adalah serangan anomali, yang dapat merusak integritas dan ketersediaan jaringan komputer. Oleh karena itu, pengembangan sistem keamanan yang adaptif dan proaktif menjadi kunci utama dalam menjaga keberlanjutan dan fungsionalitas jaringan komputer di era digital ini. Dengan demikian, perlunya kolaborasi antara ahli keamanan, pengembang teknologi, dan pemangku kepentingan lainnya menjadi semakin penting (Munawar & Putri, 2020). Langkah-langkah proaktif untuk mendeteksi dan mencegah serangan anomali harus menjadi fokus utama dalam upaya menjaga keberlanjutan jaringan komputer. Hanya dengan pendekatan yang holistik dan kerjasama yang erat, kita dapat memastikan bahwa jaringan komputer tetap menjadi tulang punggung yang kuat bagi kemajuan dan interkoneksi dalam era digital ini.

Seiring dengan kemajuan teknologi, perkembangan serangan anomali di dalam jaringan komputer menjadi tantangan serius bagi sistem keamanan. Penyerang kini semakin terampil menggunakan berbagai metode dan taktik yang terus berkembang, menjadikan deteksi serangan semakin rumit. Pendekatan tradisional berbasis aturan dan tanda-tanda klasik, yang sebelumnya diandalkan untuk mengidentifikasi serangan, tidak lagi cukup efektif menghadapi serangan canggih yang mampu menyamar dan beradaptasi (Nihri et al., 2018). Pentingnya memahami bahwa penyerang telah mengganti strategi mereka seiring waktu, meninggalkan pola-pola yang dapat diprediksi. Serangan anomali modern seringkali bersifat dinamis dan sulit dideteksi oleh solusi keamanan konvensional. Oleh karena itu, diperlukan pendekatan yang lebih cerdas dan responsif untuk menghadapi ancaman ini. Sistem keamanan harus mampu secara aktif memantau pola lalu lintas yang tidak biasa dan mengidentifikasi aktivitas yang mencurigakan, bahkan ketika tidak ada tanda-tanda klasik dari serangan.

Pentingnya penggunaan teknologi kecerdasan buatan (AI) dan machine learning (ML) dalam mendeteksi serangan anomali semakin terasa. Dengan memanfaatkan kemampuan ini, sistem keamanan dapat belajar dari pola-pola yang muncul, mengidentifikasi serangan yang belum pernah terdeteksi sebelumnya, dan secara otomatis mengadaptasi strategi keamanan untuk menghadapi ancaman baru. Kombinasi antara kecerdasan buatan dan teknologi keamanan yang responsif menjadi kunci untuk mengamankan jaringan komputer di era di mana serangan anomali semakin kompleks dan dinamis (Situmorang & Yahfizham, 2023). Dalam menghadapi tantangan ini, kolaborasi antara komunitas keamanan, peneliti keamanan, dan penyedia solusi keamanan menjadi penting. Dengan saling berbagi informasi dan pengalaman, dapat dibangun

pertahanan yang lebih tangguh dan efektif melawan serangan anomali yang semakin berkembang. Hanya dengan pendekatan yang holistik dan adaptif, kita dapat menghadapi ancaman serangan anomali di dalam jaringan komputer dengan keberhasilan yang lebih besar.

Dalam menghadapi kompleksitas serangan anomali, penggunaan metode machine learning menjadi semakin relevan dan vital. Machine learning menawarkan pendekatan yang adaptif dan dapat mempelajari pola-pola yang mungkin sulit diidentifikasi oleh sistem tradisional. Melalui pengembangan algoritma machine learning, penelitian ini bertujuan untuk meningkatkan efektivitas deteksi terhadap serangan anomali di dalam jaringan komputer (NURYASIN et al., 2023). Meskipun potensi machine learning dalam mendeteksi anomali, implementasinya dalam konteks jaringan komputer tidak terlepas dari beberapa tantangan. Variabilitas besar dalam pola lalu lintas jaringan, volume data yang tinggi, dan evolusi konstan dari metode serangan membuat deteksi anomali menjadi tugas yang kompleks. Oleh karena itu, pengembangan algoritma machine learning yang mampu menangani tantangan-tantangan ini menjadi krusial.

Penelitian ini memiliki tujuan untuk mengembangkan algoritma machine learning yang dapat secara efektif mendeteksi serangan anomali dalam jaringan komputer. Dengan memperhatikan karakteristik unik dari lalu lintas jaringan dan memanfaatkan kecerdasan buatan, diharapkan penelitian ini dapat memberikan kontribusi signifikan dalam peningkatan keamanan jaringan komputer secara keseluruhan. Keberhasilan penelitian ini tidak hanya akan mendukung keamanan infrastruktur jaringan komputer, tetapi juga akan memberikan dampak positif secara sosial dan ekonomi. Dengan tingkat keamanan yang lebih tinggi, risiko kehilangan data, pencurian informasi, dan gangguan layanan dapat diminimalkan, memberikan kepercayaan yang lebih besar kepada pengguna jaringan dan mendorong pertumbuhan ekonomi di era digital ini.

## METODE

Metode yang digunakan dalam penelitian ini akan dijelaskan secara terperinci yaitu sebagai berikut:

1. Identifikasi Riset Terdahulu:
   a. Mengidentifikasi dan mengumpulkan literatur-literatur terkait yang telah dilakukan oleh peneliti-peneliti terkemuka dalam bidang deteksi anomali menggunakan machine learning.
   b. Menelaah berbagai metode dan pendekatan yang telah diusulkan sebelumnya untuk menilai kelebihan, kekurangan, dan perkembangan terkini dalam deteksi anomali.
2. Penentuan Kriteria Seleksi Literatur:
   a. Menetapkan kriteria khusus untuk memilih literatur yang sesuai dengan fokus penelitian, termasuk jenis metode machine learning yang digunakan, jenis data yang diolah, dan hasil yang dicapai.
3. Pengumpulan Data dan Informasi:
   a. Melakukan pengumpulan data dari literatur-literatur yang terpilih, seperti teknik deteksi anomali yang digunakan, dataset yang diuji, dan evaluasi performa yang dilakukan.
   b. Mengekstrak informasi yang relevan dan membangun pemahaman mendalam tentang perkembangan terkini dalam deteksi anomali dengan menggunakan machine learning.
4. Analisis Literatur:
   a. Menganalisis dan membandingkan berbagai pendekatan yang telah diusulkan dalam literatur-literatur terpilih.
   b. Mengevaluasi keefektifan masing-masing metode dalam mendeteksi serangan anomali, serta mengidentifikasi kelemahan dan kekuatan dari setiap pendekatan.
5. Pengembangan Framework Konseptual:
   a. Merumuskan framework konseptual berdasarkan temuan dari literatur-literatur yang telah dianalisis.

   b. Menyusun struktur kerangka konseptual yang mencakup tahapan-tahapan utama dalam pengembangan algoritma machine learning untuk deteksi anomali.
6. Integrasi Temuan dengan Kasus Studi:
   a. Menyelaraskan temuan dari literatur dengan kasus studi yang relevan, jika ada, untuk memperkuat validitas dan aplikabilitas framework yang diusulkan.
   b. Memperhatikan aspek kontekstual dan implementasi nyata dari metode yang dibahas dalam literatur.
7. Pemilihan dan Evaluasi Algoritma Machine Learning:
   a. Memilih algoritma machine learning yang paling sesuai dengan kebutuhan penelitian, berdasarkan temuan dari literatur dan karakteristik data jaringan komputer.
   b. Melakukan evaluasi kritis terhadap performa algoritma yang dipilih, dengan mempertimbangkan metrik evaluasi yang umum digunakan seperti akurasi, sensitivitas, dan spesifisitas.
8. Penyusunan Kesimpulan dan Rekomendasi:
   a. Menggabungkan temuan dan hasil evaluasi untuk menyusun kesimpulan yang kokoh.
   b. Memberikan rekomendasi untuk pengembangan lebih lanjut, baik dalam hal peningkatan metodologi atau implementasi praktis dalam konteks keamanan jaringan komputer.

## HASIL DAN PEMBAHASAN

Melalui studi literatur yang teliti dan komprehensif, penelitian ini berhasil menghasilkan wawasan mendalam terkait pengembangan algoritma machine learning untuk mendeteksi anomali dalam jaringan komputer. Berikut adalah beberapa hasil utama yang ditemukan:

1. Identifikasi Metode yang Tersedia:
   a. Terdapat sejumlah metode dan pendekatan dalam literatur untuk deteksi anomali menggunakan machine learning, termasuk metode berbasis statistik, pengklasifikasi, dan pendekatan berbasis clustering (Faiz et al., 2022).
   b. Metode-metode ini memiliki kelebihan dan kekurangan yang perlu dipertimbangkan untuk memilih pendekatan yang paling sesuai dengan kebutuhan deteksi anomali di dalam jaringan komputer (Hajizah et al., 2017).
2. Evaluasi Performa Metode:
   a. Hasil analisis literatur menunjukkan variasi dalam performa metode deteksi anomali. Beberapa metode memberikan hasil yang mengesankan dalam mendeteksi serangan anomali, sementara yang lain mungkin kurang efektif terutama dalam menghadapi serangan yang semakin canggih (Salimuka, 2017).
   b. Evaluasi performa melibatkan sejumlah metrik, termasuk akurasi, sensitivitas, spesifisitas, dan kecepatan komputasi, untuk memahami trade-off antara ketepatan deteksi dan efisiensi algoritma (Devia & Soewito, 2023).
3. Kesimpulan dan Framework Konseptual:
   a. Hasil analisis literatur menyebabkan formulasi kesimpulan tentang pendekatan-pendekatan yang paling menjanjikan dan relevan dengan konteks penelitian ini (Fibrianda & Bhawiyuga, 2018).
   b. Sebuah framework konseptual berhasil dirumuskan berdasarkan temuan literatur, mencakup tahapan-tahapan kunci dalam pengembangan algoritma machine learning untuk deteksi anomali (Zy et al., 2023).
4. Tantangan dan Peluang:
   a. Literatur mengidentifikasi tantangan-tantangan kritis dalam deteksi anomali, seperti variabilitas tinggi dalam lalu lintas jaringan dan adaptabilitas penyerang terhadap metode deteksi tradisional (Setya Wijaya, 2012).
   b. Terdapat peluang untuk menggabungkan metode-metode terkini dengan inovasi baru, seperti penggunaan teknik deep learning atau pengelolaan data yang adaptif untuk meningkatkan efektivitas deteksi (Mahendra, 2019).

5. Rekomendasi untuk Pengembangan Lebih Lanjut:
   a. Berdasarkan temuan dari literatur, penelitian ini memberikan rekomendasi untuk pengembangan lebih lanjut, termasuk pengujian metode pada dataset yang lebih bervariasi, eksperimen dengan kombinasi algoritma, dan eksplorasi terhadap teknologi terkini seperti explainable AI untuk meningkatkan interpretabilitas hasil deteksi.
6. Implikasi Terhadap Keamanan Jaringan Komputer:
   a. Penelitian ini memberikan implikasi positif terhadap keamanan jaringan komputer dengan mengidentifikasi metode deteksi anomali yang dapat memberikan perlindungan yang lebih efektif dan adaptif terhadap serangan yang terus berkembang.

Dengan demikian, hasil penelitian studi literatur ini memberikan kontribusi penting dalam memahami perkembangan terkini dalam deteksi anomali menggunakan machine learning dan membuka pintu untuk pengembangan lebih lanjut dalam menjaga keamanan jaringan komputer.

Dalam menghadapi kompleksitas dan keragaman serangan yang dapat mengancam keamanan jaringan komputer, penggunaan machine learning telah muncul sebagai solusi yang menjanjikan. Perkembangan terkini dalam studi literatur menyoroti berbagai metode yang digunakan untuk mendeteksi anomali, mencakup teknik-teknik berbasis statistik, pengklasifikasi, dan pendekatan clustering. Masing-masing metode ini membawa tantangan unik dalam konteks keamanan jaringan dan memunculkan kebutuhan untuk pengembangan algoritma yang dapat mengatasi perubahan dinamis dalam taktik penyerangan.

Analisis literatur yang mendalam mengenai metode deteksi anomali mengungkapkan bahwa setiap pendekatan memiliki kelebihan dan kelemahan yang perlu diperhitungkan dengan cermat. Metode berbasis statistik, sebagai contoh, terbukti efektif dalam mendeteksi perubahan signifikan dalam pola lalu lintas jaringan. Namun, kelemahannya terletak pada kurangnya adaptasi terhadap serangan yang semakin canggih dan mampu menyamar dengan baik (Anggraeni & Andriani, 2021). Metode ini seringkali mengandalkan analisis pola yang telah diketahui sebelumnya, sehingga bisa kewalahan saat dihadapkan pada serangan yang belum pernah terdeteksi sebelumnya. Sebaliknya, pendekatan berbasis pengklasifikasi menawarkan tingkat akurasi yang tinggi dalam mendeteksi anomali. Namun, keberhasilan metode ini sering tergantung pada seberapa baik algoritma dapat memahami variasi besar dalam data jaringan. Tantangan utamanya muncul ketika terdapat fluktuasi yang signifikan dalam pola lalu lintas yang dapat dianggap normal. Hal ini dapat menghasilkan false positive atau false negative, yang dapat mengurangi keandalan sistem deteksi anomali.

Pentingnya memahami trade-off antara kelebihan dan kelemahan masing-masing metode menjadi kunci dalam merancang algoritma yang optimal untuk mendeteksi anomali. Sebuah pendekatan yang berhasil harus mampu mengintegrasikan keunggulan dari berbagai metode, menciptakan sistem yang responsif terhadap perubahan dinamis dalam ancaman keamanan. Oleh karena itu, kombinasi metode berbasis statistik dengan kecerdasan buatan atau machine learning dapat menjadi solusi yang efektif (Wirawan & Eksistyanto, 2015). Dengan demikian, penelitian dan pengembangan terus berlangsung untuk mencari keseimbangan optimal dalam mendeteksi anomali di dalam jaringan komputer, menggabungkan kelebihan berbagai pendekatan untuk mencapai keandalan dan ketangguhan yang diperlukan dalam menghadapi ancaman yang semakin kompleks.

Dalam mengevaluasi efektivitas metode deteksi anomali, literatur menegaskan pentingnya menggunakan metrik evaluasi yang tepat. Metrik-metrik seperti akurasi, sensitivitas, spesifisitas, dan kecepatan komputasi menjadi kriteria krusial dalam menilai kinerja suatu algoritma deteksi. Analisis literatur menyoroti bahwa penggunaan metrik evaluasi yang sesuai tidak hanya memberikan gambaran sejauh mana suatu metode dapat mendeteksi serangan, tetapi juga memberikan wawasan tentang efisiensi operasional algoritma tersebut (Hermawan, 2022). Akurasi merupakan metrik yang umum digunakan untuk mengukur seberapa baik suatu metode dapat mengidentifikasi anomali dan non-anomali. Namun, akurasi sendiri mungkin tidak cukup representatif jika tidak diimbangi dengan sensitivitas dan spesifisitas. Sensitivitas mengukur

kemampuan algoritma untuk mendeteksi serangan dengan mengidentifikasi sebanyak mungkin positif sejati (true positive), sementara spesifisitas mengukur kemampuan algoritma untuk menghindari kesalahan positif palsu (false positive).

Kecepatan komputasi menjadi faktor penting, terutama dalam skenario di mana deteksi anomali harus dilakukan secara real-time. Metode yang memiliki kecepatan komputasi tinggi dapat memberikan respons cepat terhadap ancaman, tetapi perlu diimbangi dengan tingkat akurasi yang memadai. Analisis literatur mengenai metrik evaluasi ini memberikan panduan berharga bagi peneliti dalam memilih pendekatan yang paling sesuai dengan konteks penelitian mereka. Pemahaman yang mendalam tentang kinerja suatu metode deteksi anomali, berdasarkan metrik-metrik tersebut, menjadi landasan penting dalam pengembangan dan peningkatan algoritma deteksi anomali yang efektif dan efisien (Firdaus et al., 2023). Dengan memahami dan menerapkan metrik evaluasi dengan bijak, peneliti dapat menghasilkan kontribusi yang lebih terukur dalam pengembangan keamanan jaringan komputer di era digital yang kompleks ini.

Meskipun terdapat kemajuan yang signifikan dalam penerapan machine learning untuk deteksi anomali, literatur menyoroti sejumlah tantangan yang perlu diatasi. Variabilitas tinggi dalam pola lalu lintas jaringan, evolusi cepat dari metode serangan, dan kebutuhan untuk adaptasi real-time menjadi beberapa tantangan utama yang dihadapi oleh peneliti dan praktisi keamanan (Sudiyarno et al., 2021). Variabilitas tinggi dalam pola lalu lintas jaringan menjadi hambatan utama karena memerlukan algoritma yang mampu mengenali anomali dari pola yang sangat beragam. Selain itu, evolusi cepat dari metode serangan mengharuskan algoritma deteksi anomali untuk selalu diperbarui dan ditingkatkan agar dapat mengenali pola-pola baru yang muncul.

Perlunya adaptasi real-time menjadi tantangan yang tak kalah penting. Dalam dunia keamanan jaringan yang dinamis, deteksi anomali harus dilakukan secara instan untuk merespons ancaman yang muncul secepat mungkin. Oleh karena itu, algoritma deteksi anomali perlu mampu beradaptasi dengan perubahan dalam waktu yang sangat singkat. Selain itu, literatur juga menyoroti masalah interpretasi hasil dari model machine learning untuk deteksi anomali. Kemampuan untuk menjelaskan mengapa suatu kejadian dianggap anomali dapat menjadi kritis, terutama untuk keperluan investigasi dan pengambilan keputusan (Wibisono, 2023).

Tantangan akhir yang diidentifikasi adalah perlunya menjaga keseimbangan antara keakuratan dan efisiensi komputasi. Algoritma deteksi anomali yang sangat kompleks mungkin memiliki tingkat akurasi yang tinggi, namun dapat memerlukan sumber daya komputasi yang besar (Riza, 2023). Oleh karena itu, pengembangan algoritma yang tidak hanya akurat tetapi juga efisien menjadi hal yang krusial. Tantangan-tantangan ini menekankan perlunya pengembangan algoritma deteksi anomali yang dapat mengatasi dinamika kompleks dan serba cepat di dunia keamanan jaringan komputer. Hanya dengan mengatasi tantangan-tantangan ini, keamanan jaringan dapat tetap efektif dan responsif terhadap ancaman yang terus berkembang.

Selain dari aspek teknis, penelitian ini memiliki dampak sosial dan ekonomi yang signifikan. Peningkatan keamanan jaringan komputer bukan hanya berkontribusi pada perlindungan data sensitif dan keberlanjutan operasional, tetapi juga mendorong pertumbuhan ekonomi di era digital ini. Kepercayaan yang lebih tinggi dari pengguna jaringan dapat mendorong adopsi teknologi yang lebih lanjut, membuka pintu bagi inovasi, dan merangsang pertumbuhan sektor bisnis yang terkait dengan keamanan teknologi informasi. Dengan demikian, penelitian ini membentuk landasan yang kokoh untuk pengembangan lebih lanjut dalam mendeteksi anomali menggunakan machine learning, memberikan wawasan yang mendalam dan merinci tantangan serta peluang yang memandu arah penelitian di masa

## SIMPULAN

Dalam rangka mengatasi ancaman serangan anomali dalam jaringan komputer, penelitian ini merinci kemajuan terkini dalam pengembangan algoritma machine learning. Analisis

literatur mengungkapkan kompleksitas dan variasi metode deteksi, serta menyoroti tantangan dan peluang yang muncul. Kesimpulan penelitian ini menekankan pentingnya memahami trade-off antara keakuratan dan efisiensi algoritma, sambil merangkum kontribusi positif terhadap keamanan jaringan komputer.

## SARAN

Untuk penelitian selanjutnya, disarankan untuk lebih mendalam dalam eksplorasi integrasi metode-metode terkini, seperti teknik deep learning, guna meningkatkan ketepatan deteksi. Pengujian lebih lanjut pada beragam dataset dan pemahaman lebih mendalam terhadap interpretabilitas hasil deteksi juga menjadi fokus penting. Selain itu, pengembangan algoritma yang adaptif terhadap perubahan taktik penyerangan dapat menjadi langkah proaktif untuk menanggapi serangan yang semakin canggih.

## UCAPAN TERIMA KASIH

Penelitian ini tidak terwujud tanpa dukungan dan kontribusi berbagai pihak. Kami ingin mengucapkan terima kasih sebesar-besarnya kepada para peneliti dan pengembang yang telah menyumbangkan wawasan dan temuan mereka dalam literatur. Terima kasih juga kepada tim pengawas, rekan-rekan penelitian, dan institusi yang telah memberikan dukungan teknis dan administratif. Ucapan terima kasih kami juga terarah kepada keluarga dan teman-teman yang memberikan motivasi dan dukungan moral sepanjang perjalanan penelitian ini. Semua kontribusi ini memainkan peran kunci dalam kesuksesan penelitian ini.

## DAFTAR PUSTAKA

Anggraeni, I., & Andriani, S. (2021). Implementasi algoritma c. 45 untuk klasifikasi deteksi serangan pada protokol jaringan. *Komputasi: Jurnal Ilmiah Ilmu Komputer Dan Matematika*, *18*(2), 62–68.

Devia, A., & Soewito, B. (2023). Analisis Perbandingan Metode Seleksi Fitur untuk Mendeteksi Anomali pada Dataset CIC-IDS-2018. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *5*(4), 572–578.

Faiz, M. N., Somantri, O., Supriyono, A. R., & Muhammad, A. W. (2022). Impact of feature selection methods on machine learning-based for detecting DDoS attacks: Literature review. *Journal of Informatics and Telecommunication Engineering*, *5*(2), 305–314.

Fibrianda, M. F., & Bhawiyuga, A. (2018). Analisis Perbandingan Akurasi Deteksi Serangan Pada Jaringan Komputer Dengan Metode Naïve Bayes Dan Support Vector Machine (SVM). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(9), 3112–3123.

Firdaus, D., Fahira, F., & Rianti, R. (2023). DETEKSI ANOMALI DAN SERANGAN LOW RATE DDOS DALAM LALU LINTAS JARINGAN MENGGUNAKAN NAIVE BAYES. *Naratif: Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika*, *5*(2), 140–148.

Hajizah, T. D., Purwanto, Y., & Setianingsih, C. (2017). Algoritma Fuzzy Dan Reinforcement Learning Dalam Pengambilan Keputusan. *EProceedings of Engineering*, *4*(3).

Hermawan, F. N. (2022). *Deteksi anomali pada data internet of things menggunakan model ensemble learning*. Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta.

Mahendra, I. (2019). *INTRUSION DETECTION AND PREVENTION SYSTEM BERBASIS MACHINE LEARNING PADA SOFTWARE DEFINED NETWORK DENGAN ALGORITMA ADABOOST CLASSIFIER*. UPN Veteran Yogyakarta.

Munawar, Z., & Putri, N. I. (2020). Keamanan IoT Dengan Deep Learning dan Teknologi Big Data. *TEMATIK*, *7*(2), 161–185.

Nihri, H., Pramukantoro, E. S., & Trisnawan, P. H. (2018). Pengembangan IDS Berbasis J48 Untuk Mendeteksi Serangan DoS Pada Perangkat Middleware IoT. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(12), 6902–6907.

Nururrahmah, A. T. (2023). *Pengembangan Metode Seleksi Fitur Berbasis Chi-Square dan*

*Algoritma Exhaustive untuk Meningkatkan Performa Deteksi pada Jaringan Komputer*. Institut Teknologi Sepuluh Nopember.

NURYASIN, M. F., MACHBUB, C., & YULIANTI, L. (2023). Kombinasi Deteksi Objek, Pengenalan Wajah dan Perilaku Anomali menggunakan State Machine untuk Kamera Pengawas. *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, *11*(1), 86.

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

Salimuka, R. F. (2017). *Deteksi Anomaly Host Based Network Menggunakan Artificial Neural Network*. Program Studi Teknik Informatika FTI-UKSW.

Setya Wijaya, E. (2012). *DETEKSI ANOMALI TRAFIK JARINGAN DENGAN MENGGUNAKAN METODE DECISION TREE*. Universitas Dian Nuswantoro.

Situmorang, S., & Yahfizham, Y. (2023). Analisis Kinerja Algoritma Machine Learning Dalam Deteksi Anomali Jaringan. *Konstanta: Jurnal Matematika Dan Ilmu Pengetahuan Alam*, *1*(4), 258–269.

Sudiyarno, R., Setyanto, A., & Luthfi, E. T. (2021). Peningkatan Performa Pendeteksian Anomali Menggunakan Ensemble Learning dan Feature Selection. *Creative Information Technology Journal*, *7*(1), 1–9.

Wibisono, L. (2023). *Perancangan dan Implementasi Sistem Pendeteksian Intrusi Menggunakan Teknologi Big Data dan Machine Learning*.

Wirawan, I. N. T., & Eksistyanto, I. (2015). Penerapan naive bayes pada intrusion detection system dengan diskritisasi variabel. *Jurnal Ilmiah Teknologi Informasi*, *13*(2), 182–189.

Zy, A., Sasongko, A. T., & Kamalia, A. Z. (2023). Penerapan Naïve Bayes Classifier, Support Vector Machine, dan Decision Tree untuk Meningkatkan Deteksi Ancaman Keamanan Jaringan. *KLIK: Kajian Ilmiah Informatika Dan Komputer*, *4*(1), 610–617.