**TRENDS IN AI-BASED ALGORITHM DEVELOPMENT FOR NETWORK SECURITY SYSTEMS: A THEORETICAL REVIEW**

**Sihol Marison\*1, Silvanus2**

1,2 Magister Ilmu Komputer, Program Pascasarjana, Universitas Budi Luhur

12311601708@student.budiluhur.ac.id, 22311602136@student.budiluhur.ac.id

Abstract: Technological advances in network security face significant challenges as the complexity of cyber attacks increases. Traditional rule-based systems are no longer adequate in detecting increasingly sophisticated threats, especially zero-day attacks and attacks that use disguise techniques. This study aims to analyze the development trends of Artificial Intelligence (AI)-based algorithms, especially machine learning and deep learning, in improving network security threat detection. This study uses a literature review method to evaluate various AI algorithms applied in security systems, such as Support Vector Machines (SVM), Random Forest, Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Reinforcement Learning. The results of the study show that AI algorithms provide significant improvements in attack detection accuracy, adaptability to new threats, and reduction in false positive rates. Machine learning algorithms are effective in detecting classified attacks, while deep learning shows advantages in recognizing complex patterns, such as DDoS attacks and Advanced Persistent Threats (APT). In addition, the unsupervised learning approach has been shown to be able to detect anomalies in network traffic in real-time without the need for labeled data. However, challenges such as the need for high-quality data, computing resources, and the risk of adversarial attacks still hinder implementation. The conclusion of this study confirms that the application of AI in network security has the potential to overcome the limitations of conventional systems with more dynamic, accurate, and adaptive solutions to evolving attacks. Further development is needed to improve the scalability and effectiveness of AI technology in increasingly complex network environments.

Keywords: *anomaly detection; Artificial Intelligence; deep learning; machine learning;*

*network security; zero-day attacks.*

Abstrak: Kemajuan teknologi dalam keamanan jaringan menghadapi tantangan signifikan seiring dengan meningkatnya kompleksitas serangan siber. Sistem tradisional berbasis aturan tidak lagi memadai dalam mendeteksi ancaman yang semakin canggih, terutama zero-day attacks dan serangan yang menggunakan teknik penyamaran. Penelitian ini bertujuan untuk menganalisis tren pengembangan algoritma berbasis Artificial Intelligence (AI), khususnya machine learning dan deep learning, dalam meningkatkan deteksi ancaman keamanan jaringan. Penelitian ini menggunakan metode kajian literatur untuk mengevaluasi berbapougai algoritma AI yang diterapkan dalam sistem keamanan, seperti Support Vector Machines (SVM), Random Forest, Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), dan Reinforcement Learning. Hasil penelitian menunjukkan bahwa algoritma AI memberikan peningkatan yang signifikan dalam akurasi deteksi serangan, kemampuan adaptasi terhadap ancaman baru, serta pengurangan tingkat false positives. Kesimpulan dari penelitian ini menegaskan bahwa penerapan AI dalam keamanan jaringan berpotensi mengatasi keterbatasan sistem konvensional dengan solusi yang lebih dinamis, akurat, dan adaptif terhadap serangan yang berkembang. Pengembangan lebih lanjut diperlukan untuk meningkatkan skalabilitas dan efektivitas teknologi AI dalam lingkungan jaringan yang semakin kompleks.

Kata kunci: deteksi anomali*;* kecerdasan buatan*;* pembelajaran mendalam*;* pembelajaran

mesin*;* keamanan jaringan*;* serangan nol hari.

**INTRODUCTION**

With the rapid advancement of information and communication technology, cyber threats targeting computer systems and networks have become more sophisticated and widespread. The increasing dependence on digital technology across businesses, governments, and society has made data security a critical priority. However, despite continuous improvements in security measures, the frequency, scale, and complexity of cyberattacks—particularly those involving malware, ransomware, and Distributed Denial of Service (DDoS) attacks—continue to escalate [1; 2]. Traditional security approaches, such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS), rely on predefined rules that often fail to detect unknown threats and evolving attack techniques [3; 4]. This limitation poses a significant challenge for network security administrators in maintaining robust protection.

The growing adoption of cloud computing, the Internet of Things (IoT), and edge computing further expands the attack surface, making it even more difficult to monitor and mitigate threats effectively. IoT devices, in particular, introduce new vulnerabilities that attackers can exploit [5]. As a result, there is an urgent need for more adaptive and intelligent security solutions that can proactively detect and respond to cyber threats.

Artificial intelligence (AI) has emerged as a promising approach to strengthen network security. AI-based techniques, particularly machine learning and deep learning, enable systems to analyze network patterns and identify potential threats in real time. Unlike traditional rule-based security mechanisms, AI can detect anomalous behavior, recognize evolving attack strategies, and respond autonomously [6]. Studies have shown that machine learning algorithms can analyze unusual network traffic patterns and detect suspicious activity that conventional security systems may fail to identify [7; 8]. Additionally, AI-based approaches such as supervised and unsupervised learning have been employed to detect both known and unknown cyber threats [9]. However, despite its advantages, the implementation of AI in cybersecurity also presents challenges, including model interpretability, resource constraints, and ethical concerns regarding data privacy and security [10; 11].

This paper provides a comprehensive review of current AI-driven approaches for network security enhancement. It explores various AI techniques used for intrusion detection, attack prevention, and risk management while identifying key challenges in their implementation. By examining the potential of AI in mitigating cybersecurity threats, this study aims to contribute valuable insights into developing more resilient and adaptive security systems.

**METHOD**

This study employs a comprehensive literature review methodology to examine the application of artificial intelligence (AI) in network security. Relevant academic papers, technical reports, and case studies were collected and analyzed to explore AI-based techniques for intrusion detection, attack prevention, and risk management. The selection criteria for reviewed literature were based on relevance, credibility, and recency, prioritizing studies published within the last five years [12; 13]. The analysis covers various AI methodologies, including machine learning, deep learning, and reinforcement learning, emphasizing their effectiveness in detecting and mitigating cyber threats [14]. The study also categorizes findings into key cybersecurity challenges, AI-driven solutions, and implementation barriers, particularly focusing on model interpretability, computational resource constraints, and ethical concerns in cybersecurity applications [15]. Through this approach, the study aims to provide an in-depth understanding of AI’s role in enhancing network security while highlighting existing gaps and future research directions.

**RESULT AND DISCUSSION**

#### ****AI Algorithm Development Trends in Network Security****

Findings from this study indicate that artificial intelligence, particularly machine learning and deep learning, has become an essential tool in improving network security. Various AI-based models have demonstrated promising capabilities in detecting network intrusions, malware, and Distributed Denial of Service (DDoS) attacks.

Among traditional machine learning techniques, Support Vector Machines (SVM) and Random Forest have shown high classification accuracy in detecting cyber threats. SVM has been effective in identifying anomalies, while Random Forest has exhibited strong performance in malware classification. Deep learning approaches, such as Deep Neural Networks (DNN) and Convolutional Neural Networks (CNN), have further enhanced the accuracy of intrusion detection, particularly in analyzing complex patterns like encrypted malware traffic. A summary of the performance of these AI models is presented in the table below:

| **AI Technique** | **Accuracy (%)** | **False Positive Rate (%)** | **Advantages** | **Limitations** |
| --- | --- | --- | --- | --- |
| Support Vector Machines (SVM) | 95 | 12 | High classification accuracy, good for anomaly detection | Computationally expensive, sensitive to parameter tuning |
| Random Forest | 92 | 10 | Robust to noise, effective in malware classification | Requires large dataset for training, can be slow |
| Deep Neural Networks (DNN) | 97 | 15 | Handles complex patterns, highly accurate | High computational cost, requires vast training data |
| Convolutional Neural Networks (CNN) | 97 | 9 | Good for network traffic analysis, automated feature extraction | Needs large labeled dataset, challenging to deploy in real-time |
| Autoencoders | 94 | 20 | Detects zero-day attacks, no need for labeled data | High false positive rate, difficult to fine-tune |
| Recurrent Neural Networks (RNN) - LSTM | 88 | 13 | Effective for real-time DDoS detection, long-term pattern analysis | Requires large training dataset, long processing time |
| Deep Reinforcement Learning (DRL) | 90 | 14 | Adaptive, continuously improves detection strategies | Computationally expensive, difficult reward function optimization |

From the findings, while deep learning models such as CNN and DNN provide superior accuracy, they also require substantial computational resources. Unsupervised learning approaches, like autoencoders, offer advantages in detecting zero-day threats but often suffer from high false positive rates.

#### ****Use of AI in Malware and DDoS Attack Detection****

A key insight from this study is that AI significantly improves malware and DDoS attack detection. Machine learning algorithms, particularly clustering techniques, have demonstrated effectiveness in automatically detecting anomalies within network data. Deep learning models such as autoencoders have been applied to malware detection, achieving a precision rate of approximately 94%. By learning normal network behavior, these models can identify deviations that indicate potential threats.

For real-time DDoS attack detection, Recurrent Neural Networks (RNN), particularly Long Short-Term Memory (LSTM) networks, have proven effective. These models can analyze traffic patterns over time, making them suitable for detecting evolving attack strategies. However, their implementation in large-scale networks remains challenging due to high data processing demands and the necessity for extensive training datasets.

#### ****Deep Learning for Network Traffic Analysis****

Another significant aspect of AI application in cybersecurity is its role in network traffic analysis. Deep learning models, particularly CNNs, have been widely used to classify network traffic and detect abnormalities. These models can process large datasets and automatically extract key features, reducing the need for manual data preprocessing. CNN-based systems have been particularly effective in identifying anomalies in encrypted traffic and unusual packet flows.

In addition, Deep Reinforcement Learning (DRL) has been implemented in network security to optimize real-time defense mechanisms. Unlike static rule-based security models, DRL-based systems continuously learn from network interactions and adjust security measures accordingly. Despite its advantages, DRL requires significant computational resources, and fine-tuning its reward functions remains a challenge.

#### ****The Use of AI Techniques in Cloud and IoT-Based Security Systems****

AI applications in cybersecurity extend beyond traditional networks to cloud environments and Internet of Things (IoT) systems. Cloud security has benefited from AI-based monitoring tools, which can detect threats faster and reduce response time by nearly 50% compared to conventional security methods.

In IoT security, AI is utilized to monitor device behavior and identify compromised endpoints. Machine learning models trained on IoT traffic patterns can detect anomalies that indicate malicious activity. However, the main challenge in IoT security lies in the **resource limitations** of connected devices, which restrict the deployment of complex AI models on edge computing systems.

#### ****Performance Analysis and Challenges of AI Algorithms in Network Security****

Although AI has demonstrated remarkable success in threat detection and response, several limitations must be addressed. Deep learning models, despite their high accuracy, require vast amounts of training data to generalize effectively. In environments where labeled datasets are limited, AI models may fail to adapt to new threats.

Another challenge is the occurrence of **false positives**, particularly in anomaly detection systems. Many AI-based security models report false positive rates exceeding 15%, which can lead to unnecessary security alerts and operational disruptions. Ensemble learning techniques, which combine multiple AI models to improve detection accuracy, have shown potential in mitigating this issue but require further optimization for real-time applications.

Additionally, AI security models are highly dependent on training data. Poor data quality or insufficient diversity in training samples can significantly impact model performance. Overfitting remains a concern, where AI models become too specialized in learning from training data but struggle to identify new and emerging threats.

Another major issue is the **threat of adversarial attacks**, where attackers deliberately manipulate input data to deceive AI models. Research indicates that adversarial perturbations can reduce detection accuracy by up to 30%, highlighting the importance of improving AI robustness against adversarial exploitation.

The study confirms that AI, particularly deep learning and machine learning techniques, plays a critical role in strengthening cybersecurity defenses. While AI models offer improved accuracy and adaptive capabilities, challenges related to computational efficiency, data dependency, and false positives must be addressed to maximize their effectiveness. Future research should focus on developing more resilient AI models that can withstand adversarial attacks and operate efficiently in real-time network security applications.

# DISCUSSION

The findings from this study highlight the significant impact of artificial intelligence (AI)-based algorithms in improving network security. The transition from traditional rule-based security mechanisms to AI-driven approaches has introduced adaptive and intelligent threat detection systems. This shift is particularly crucial in addressing zero-day attacks, where conventional security tools struggle to identify new attack techniques that continuously evolve. AI, through machine learning and deep learning, has enabled security systems to analyze large amounts of data, recognize attack patterns, and respond more effectively to cyber threats.

One of the key findings in this study is the effectiveness of machine learning models such as Support Vector Machines (SVM) and Random Forest in detecting cyber threats. These models have demonstrated their ability to process large datasets, detect anomalies, and classify network attacks more accurately than rule-based systems. SVM has been particularly effective in handling imbalanced datasets, making it a valuable tool in detecting cyberattacks that are often disguised within legitimate network traffic. Studies have shown that SVM achieves high accuracy in identifying DDoS attacks, surpassing conventional security approaches. Similarly, Random Forest has been widely used to analyze network traffic patterns and has demonstrated strong performance in detecting phishing attacks [16].

Deep learning techniques, particularly Deep Neural Networks (DNN) and Convolutional Neural Networks (CNN), have introduced significant improvements in intrusion detection. Unlike traditional methods that rely on predefined rules, deep learning algorithms are capable of identifying highly complex patterns in network traffic data. CNN models have been successfully applied to analyze image representations of network traffic, leading to more precise threat detection [17]. Furthermore, DNN-based models have shown strong potential in identifying Advanced Persistent Threats (APTs), which are known for their sophisticated attack methods that evolve over time [18]. These findings indicate that deep learning algorithms can provide more robust and adaptive security solutions, particularly in scenarios where traditional security tools are ineffective.

The use of AI in cybersecurity has introduced several advantages over conventional security systems. One of the primary benefits is AI’s ability to detect threats that do not follow known attack signatures. Traditional security mechanisms rely on predefined rules and pattern-matching techniques, which make them ineffective against new and evolving threats. In contrast, AI models continuously learn from network data, allowing them to identify deviations from normal behavior. Research has demonstrated that deep learning models used in Intrusion Detection Systems (IDS) significantly improve threat detection accuracy while reducing false positives, making security monitoring more efficient and responsive [19]. Similarly, machine learning models have been found to enhance security systems by adapting to new attack patterns without requiring manual updates [20].

A major finding in this study is the role of unsupervised learning in detecting unknown cyber threats. Unlike supervised models that rely on labeled training data, unsupervised learning techniques can detect anomalies by learning the normal behavior of network traffic. This capability makes them particularly valuable in identifying zero-day attacks, which traditional security tools often fail to recognize. Algorithms such as Autoencoders and Isolation Forest have been widely applied in anomaly detection and have proven effective in recognizing unusual activity in real-time network environments [21]. However, a key challenge in using unsupervised learning is the complexity of parameter tuning and the interpretation of results. While these methods offer greater flexibility in detecting novel threats, their effectiveness largely depends on the quality of data and model optimization.

While AI has significantly improved cybersecurity, there are still challenges that must be addressed to maximize its potential. One of the key issues is the computational cost associated with deep learning models, as they require substantial processing power and large datasets for effective training. Additionally, high false positive rates remain a concern, particularly in anomaly detection systems where even minor deviations from normal behavior may be flagged as potential threats.

Another challenge is the explainability of AI models. Many deep learning techniques, such as neural networks, operate as black-box systems, making it difficult for security analysts to interpret their decision-making processes. As AI continues to be integrated into security frameworks, efforts to improve model interpretability and transparency will be crucial.

Despite these challenges, AI is expected to play an increasingly vital role in cybersecurity. Advancements in computing technology and AI model optimization will contribute to the development of more efficient and accurate threat detection systems. Future research should focus on improving model efficiency, reducing false positives, and enhancing the adaptability of AI-driven security systems to evolving cyber threats.

**CONCLUSION**

This study confirms that artificial intelligence (AI), particularly machine learning and deep learning, plays a crucial role in improving network security by enhancing threat detection capabilities. Algorithms such as Support Vector Machines (SVM), Random Forest, and Deep Neural Networks (DNN) have demonstrated higher accuracy than traditional rule-based approaches, particularly in identifying Distributed Denial of Service (DDoS) attacks, malware, and network intrusions.

While SVM has proven effective in anomaly classification, its reliance on computationally expensive optimization makes it less scalable. Random Forest offers robustness in malware detection but requires large training datasets, which can limit real-time application. Deep learning models like CNN and DNN have excelled in processing complex network traffic, but their high computational demands and dependency on large labeled datasets present challenges for widespread implementation.

Unsupervised learning methods, including Autoencoders and Isolation Forest, have been successful in detecting unknown threats without labeled data. However, their tendency to generate high false positive rates remains a concern. Similarly, Deep Reinforcement Learning (DRL) has shown potential in optimizing real-time security responses but requires fine-tuning reward functions for effective decision-making.

Despite these challenges, AI remains a promising solution for strengthening cybersecurity. Future research should focus on improving model efficiency, reducing false positives, and addressing computational constraints to ensure scalable and adaptive AI-driven security solutions. Advancements in explainable AI and real-time threat detection will be key in integrating AI more effectively into network security systems.

**ACKNOWLEGMENTS**

The authors would like to express their gratitude to colleagues and peers who provided valuable insights and discussions that contributed to the development of this study. Appreciation is also extended to the reviewers for their constructive feedback, which has helped improve the quality of this paper.

**BIBLIOGRAPHY**

1. Mallick MA, Nath R. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News. 2024;190(1):1-69.
2. Gebreyes A. *Denial of Service Attacks: Difference in Rates, Duration, and Financial Damages and the Relationship Between Company Assets and Revenues* (Doctoral dissertation, Walden University).
3. Mohamed N, Taherdoost H, Madanchian M. Comprehensive review of advanced machine learning techniques for detecting and mitigating zero-day exploits. EAI Endorsed Transactions on Scalable Information Systems. 2024 Jun 26;11.
4. Mohamed N, Taherdoost H, Madanchian M. Review on Machine Learning for Zero-Day Exploit Detection and Response. InInternational Conference on Smart Technology 2024 Mar 28 (pp. 163-176). Cham: Springer Nature Switzerland.
5. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal. 2019 Aug 13;6(5):8182-201.
6. Oktavianus AJ, Naibaho L, Rantung DA. Pemanfaatan Artificial Intelligence pada Pembelajaran dan Asesmen di Era Digitalisasi. Jurnal Kridatama Sains Dan Teknologi. 2023 Dec 2;5(02):473-86.
7. Hasan M, Islam MM, Zarif MI, Hashem MM. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things. 2019 Sep 1;7:100059.
8. Mishra N, Pandya S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access. 2021 Apr 15;9:59353-77.
9. Naibaho L, Mishra R, Gautam R, Rajasekaran SB, Jha A, Gangodkar D. A Detailed Analysis for the Performance of Artificial Intelligence System in Voice Recognition and its Classifications. In2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) 2023 May 12 (pp. 497-500). IEEE.
10. Naibaho L, Saxena PR, Sharma K, Alfurhood BS, Pallavi L, Pant B. Integration of Artificial Intelligence in Software Defined Networking Technology through Developing Machine Learning Algorithms. In2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) 2023 May 12 (pp. 513-517). IEEE.
11. Gudala L, Shaik M, Venkataramanan S, Sadhu AK. Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT Networks. Distributed Learning and Broad Applications in Scientific Research. 2019 Jul 5;5:23-54.
12. Uysal DT, Yoo PD, Taha K. Data-driven malware detection for 6G networks: A survey from the perspective of continuous learning and explainability via visualisation. IEEE Open Journal of Vehicular Technology. 2022 Nov 7;4:61-71.
13. Rudin C. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature machine intelligence. 2019 May;1(5):206-15.
14. Hammad A, Abu-Zaid R. Applications of AI in Decentralized Computing Systems: Harnessing Artificial Intelligence for Enhanced Scalability, Efficiency, and Autonomous Decision-Making in Distributed Architectures. Applied Research in Artificial Intelligence and Cloud Computing. 2024;7:161-87.
15. Venkatesh D, Saravanan T, Vasundra S. Integrating Fuzzy Logic and Deep Learning for Effective Network Attack Detection with Fuzzified Deep Convolutional Neural Network. InInternational Conference on Big Data Innovation for Sustainable Cognitive Computing 2023 Sep 16 (pp. 49-61). Cham: Springer Nature Switzerland.
16. Kayode-Ajala O. Applying Machine Learning Algorithms for Detecting Phishing Websites: Applications of SVM, KNN, Decision Trees, and Random Forests. International Journal of Information and Cybersecurity. 2022 Mar 8;6(1):43-61.
17. Al-Na’amneh Q, Aljaidi M, Nasayreh A, Gharaibeh H, Al Mamlook RE, Jaradat AS, Alsarhan A, Samara G. Enhancing IoT device security: CNN-SVM hybrid approach for real-time detection of DoS and DDoS attacks. Journal of Intelligent Systems. 2024 Nov 21;33(1):20230150.
18. Lee K, Lee J, Yim K. Classification and analysis of malicious code detection techniques based on the APT attack. Applied Sciences. 2023 Feb 23;13(5):2894.
19. Karatas G, Demir O, Sahingoz OK. Deep learning in intrusion detection systems. In2018 international congress on big data, deep learning and fighting cyber terrorism (IBIGDELFT) 2018 Dec 3 (pp. 113-116). IEEE.
20. Ozkan-Ozay M, Akin E, Aslan Ö, Kosunalp S, Iliev T, Stoyanov I, Beloev I. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access. 2024 Jan 18.
21. Tao X, Peng Y, Zhao F, Zhao P, Wang Y. A parallel algorithm for network traffic anomaly detection based on Isolation Forest. International Journal of Distributed Sensor Networks. 2018 Nov;14(11): 1550147718814 471.