JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XI No 2, Maret 2025, hlm. 329 – 336 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/10.33330/jurteksi.v11i2.3699
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

AI-BASED ALGORITHMS FOR NETWORK SECURITY: TRENDS, PERFORMANCE, AND CHALLENGES

Sihol Marison[1*], Silvanus[1], Rudi Rusdiah[1]
[1]Master of Computer Science, Universitas Budi Luhur
email :*2311601708@student.budiluhur.ac.id

Abstract: The advancement of network security faces growing challenges as cyberattacks become more sophisticated. Traditional rule-based systems struggle with zero-day attacks and obfuscation techniques. This study examines the development trends of AI-based algo-rithms, particularly machine learning and deep learning, in threat detection. A literature review evaluates AI-driven approaches, including support vector machines, random for-est, deep neural networks, convolutional neural networks, and reinforcement learning. Findings show that AI enhances detection accuracy, adaptability, and reduces false posi-tives. Machine learning efficiently classifies known attacks, while deep learning excels in identifying complex patterns such as distributed denial-of-service and advanced persis-tent threats. Unsupervised learning improves anomaly detection without labeled data. However, AI models require high-quality data, substantial computational resources, and remain vulnerable to adversarial attacks. Despite these challenges, AI provides a dynam-ic and adaptive security solution, surpassing traditional systems. Future research should enhance AI scalability and resilience for evolving cybersecurity threats.

Keywords: anomaly detection; artificial intelligence; deep learning; machine learning; network security

Abstrak: Perkembangan keamanan jaringan menghadapi tantangan yang semakin besar seiring meningkatnya kompleksitas serangan siber. Sistem berbasis aturan tradisional kesulitan mendeteksi zero-day attack dan teknik penyamaran. Penelitian ini mengkaji tren pengembangan algoritma berbasis *AI*, khususnya machine learning dan deep learning, dalam deteksi ancaman. Literature review mengevaluasi pendekatan berbasis AI, termasuk support vector machines, random forest, deep neural networks, convolutional neural networks, dan reinforcement learning. Hasil penelitian menunjukkan bahwa AI meningkatkan akurasi deteksi, adaptabilitas terhadap ancaman baru, serta mengurangi false positive. Machine learning efektif mengklasifikasikan serangan yang telah diketahui, sementara deep learning unggul dalam mengenali pola kompleks seperti distributed denial-of-service dan advanced persistent threats. Unsupervised learning meningkatkan deteksi anomali tanpa memerlukan data berlabel. Namun, AI masih bergantung pada data berkualitas tinggi, sumber daya komputasi besar, dan rentan terhadap adversarial attack. Meskipun demikian, AI menawarkan solusi keamanan yang lebih dinamis dan adaptif dibandingkan sistem tradisional. Penelitian selanjutnya perlu difokuskan pada peningkatan skalabilitas dan ketahanan AI dalam menghadapi ancaman siber yang terus berkembang.

Kata kunci: deteksi anomali; jaringan keamanan; kecerdasan buatan; pembelajaran dalam; pembelajaran mesin

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XI No 2, Maret 2025, hlm. 329 – 336 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/10.33330/jurteksi.v11i2.3699
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

INTRODUCTION

The rapid advancement of information and communication technology has significantly impacted network security, making cyber threats such as malware, ransomware, and distributed denial-of-service attacks increasingly sophisticated and harder to detect [1]. Traditional security mechanisms, including firewalls, intrusion detection systems, and intrusion prevention systems, rely on rule-based approaches that struggle to identify zero-day attacks and evolving threats [2]. Therefore, more adaptive security strategies are essential to effectively counter emerging cyber risks.

Recent advancements in artificial intelligence (AI) have significantly enhanced threat detection and response efficiency. Machine learning and deep learning enable security systems to analyze network traffic, detect anomalies, and identify unknown attacks [3]. These technologies are widely applied in intrusion detection systems, cyberattack prevention, and proactive risk mitigation. Network intrusion detection plays a crucial role in cybersecurity defense by identifying and preventing malicious activities in computer networks. As cyber threats grow in complexity and variety, traditional rule-based methods struggle to recognize new attack strategies. Machine learning (ML) and deep learning (DL) models, capable of processing large volumes of network traffic data, can autonomously detect patterns and irregularities. This has led to a growing interest in applying these advanced models for more effective network intrusion detection. [4].

Several studies have explored AI-based approaches to strengthen network security. Research by Kamenova et al. [5] demonstrated that support vector machines improve anomaly detection accuracy, although parameter optimization remains a challenge. Similarly, deep learning models have shown superior performance in detecting zero-day attacks compared to rule-based methods, yet they require extensive datasets and often exhibit high false positive rates [6].

An LSTM network is added after the encoder to memorize feature representations of normal data [7]. Additionally, deep reinforcement learning has demonstrated potential in adaptive security frameworks, allowing dynamic threat mitigation, though reward function optimization remains a challenge. The researchers begin by presenting the fundamental concepts and frameworks of Domain Adaptation (DA) in Reinforcement Learning (RL), followed by a review of the current DA methods applied within RL. Their main objective was to address the gap in existing literature regarding DA in RL. To accomplish this, they conducted a comprehensive evaluation of state-of-the-art DA techniques. Their goal was to provide valuable insights into DA in RL and contribute to advancing knowledge in this field. [8].

Despite these advancements, AI-based security systems still face limitations, including high computational demands, false positive rates, and model interpretability issues [9]. To address these challenges, this study provides a comprehensive review of AI-driven network security algorithms. By analyzing intrusion detection techniques, attack prevention strategies, and adaptive risk mitigation approaches, this research aims to contribute insights toward the development of more efficient and scalable cybersecurity frameworks. By examining extensive datasets from network activity, user behavior, and past incidents,

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XI No 2, Maret 2025, hlm. 329 – 336 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/10.33330/jurteksi.v11i2.3699
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

organizations can recognize patterns and irregularities that indicate possible risks. [10].

METHOD

This study employs a systematic literature review (SLR) and comparative analysis to examine AI-based network security algorithms. Software-Defined Networking (SDN) offers an innovative network architecture by combining centralized control with the flexibility of network programming [11]. Creating a document from a voice recording is no longer a difficult task. It can be easily and quickly accomplished using a program called Voice Recognition [12]. New methods for evaluating software architecture reliability, deploying ERP systems, and developing information systems for analyzing viral infection data [13].

Findings are categorized into three key areas: (1) emerging trends in AI-driven network security, (2) comparative performance analysis of AI-based algorithms, and (3) implementation challenges, such as model interpretability, computational demands, and adversarial attack risks. This approach provides a structured understanding of AI's impact on network security while identifying research gaps and future directions.

RESULT AND DISCUSSION

The application of artificial intelligence in network security has advanced significantly, enabling more adaptive threat detection mechanisms. An Intrusion Detection System (IDS) helps protect the network by analyzing incoming traffic to detect and prevent unauthorized access, ensuring the network's confidentiality, integrity, and availability [14].

Among traditional machine learning methods, support vector machines and random forest have demonstrated high classification accuracy in detecting cyber threats. Support vector machines effectively identify anomalies in network behavior, while random forest is robust in malware classification. Meanwhile, deep learning models, such as deep neural networks and convolutional neural networks, have further improved intrusion detection accuracy by recognizing complex patterns, including encrypted malware traffic [15].

models such as deep neural networks and convolutional neural networks achieve 97% accuracy, but require substantial computational resources. Autoencoders are effective for detecting zero-day attacks without labeled data but have high false positive rates. Meanwhile, recurrent neural networks, particularly long short-term memory models, are effective in real-time DDoS detection but face challenges due to high processing demands. Deep reinforcement learning shows adaptability in optimizing network security strategies, but requires extensive reward function tuning for effective deployment [16].

Table 1. Comparative Analysis of AI Techniques for Cybersecurity Threat Detection

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XI No 2, Maret 2025, hlm. 329 – 336 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/10.33330/jurteksi.v11i2.3699
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

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

The application of AI in detecting malware and DDoS attacks has significantly improved cybersecurity. Machine learning techniques, particularly clustering methods, have proven effective in detecting network anomalies. Deep learning models, such as autoencoders, achieve 94% precision in malware detection by learning normal network behavior and identifying deviations that signal potential threats [17].

For real-time DDoS detection, recurrent neural networks and long short-term memory models effectively analyze evolving traffic patterns. With the rise of internet-connected devices now reaching into the tens of billions. Cybercriminals are increasingly leveraging Distributed Denial-of-Service (DDoS) attacks to compromise systems. This project seeks to develop a cutting-edge intrusion detection system utilizing deep learning, specifically designed for the Internet of Things (IoT), as traditional machine learning methods fall short in identifying these threats in real-world scenarios. The proposed approach effectively aims to detect and neutralize DDoS attacks within the unique environment of connected devices. [18].

Deep learning also plays a key role in network traffic analysis. Convolutional neural networks efficiently classify network traffic and detect anomalies by processing large datasets and automatically extracting key features. Their effectiveness in detecting encrypted traffic anomalies has been well-documented [19]. Additionally, deep reinforcement learning adapts security measures based on evolving threats, but requires significant computational power and reward function optimization to ensure efficiency. Our attention is directed towards the

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XI No 2, Maret 2025, hlm. 329 – 336 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/10.33330/jurteksi.v11i2.3699
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

shortcomings of conventional reward functions, which frequently struggle to address complex tasks in continuous state spaces. To overcome these challenges, we suggest incorporating active preference learning to create reward functions that align with human preferences. This method capitalizes on an individual's subjective preferences to direct the learning process of the agent, allowing for the development of reward functions that better reflect human desires. By using mutual information, we generate informative queries and utilize the insights gained to balance the agent's uncertainty with the human's ability to respond, prompting the agent to ask clear and insightful questions. [20].

Beyond traditional network security, AI enhances security in cloud environments and Internet of Things (IoT) systems. In cloud security, AI-driven monitoring tools reduce response time by nearly 50% compared to conventional methods. In IoT security, machine learning models analyze device behavior and network traffic to detect malicious activity. Advancements in artificial intelligence, mobile communication, and sensor technologies have expanded vehicle design requirements beyond just driving functionality [21].

Despite AI-driven advancements in cybersecurity, several challenges remain. artificial neural networks (ANN), machine learning (ML), deep learning (DL), and ensemble learning (EL)—allow algorithms to autonomously analyze data and make predictions or decisions without requiring explicit programming [22].

Another issue is the high false positive rate, particularly in anomaly detection systems, where rates often exceed 15%, leading to excessive security alerts and operational disruptions. Identifying and addressing faults early is essential for the optimal performance of these systems and for reaching the low temperature goals set for 4th generation district heating networks. Particularly, techniques for detecting faults and anomalies in district heating substations are gaining significant attention [23]. Additionally, AI models are vulnerable to adversarial attacks, where manipulated input data deceives detection systems, potentially reducing accuracy by up to 30%**.** Ongoing research in adversarial machine learning focuses on developing robust AI models through adversarial training and improved model resilience.

CONCLUSION

This study confirms that artificial intelligence (AI), particularly machine learning and deep learning, enhances network security by improving threat detection. Algorithms such as support vector machines, random forest, convolutional neural networks, and deep neural networks outperform traditional rule-based methods in detecting distributed denial-of-service attacks, malware, and network intrusions. Despite their effectiveness, AI models face challenges such as high computational demands, reliance on large labeled datasets, and false positive rates. Unsupervised learning techniques like autoencoders and isolation forest detect unknown threats without labeled data but often generate high false positives. Similarly, deep reinforcement learning improves adaptive security responses but requires complex reward function tuning.

AI remains a promising solution for cybersecurity, but further research is needed to improve efficiency, reduce false positives, and enhance scalability. The development of explainable AI and

real-time threat detection will be key to integrating AI more effectively into network security systems

BIBLIOGRAPHY

[1] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, "A Survey on ML Techniques for Multi-Platform Malware Detection: Securing PC, Mobile Devices, IoT, and Cloud Environments," *Sensors*, vol. 25, no. 4, 2025, doi: 10.3390/s25041153.

[2] E. Owusu *et al.*, "Online Network DoS/DDoS Detection: Sampling, Change Point Detection, and Machine Learning Methods," *IEEE Commun. Surv. Tutorials*, no. December, 2024, doi: 10.1109/COMST.2024.3488580.

[3] M. Almehdhar *et al.*, "Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems for Intelligent Vehicle Networks," *IEEE Open J. Veh. Technol.*, vol. 5, pp. 869–906, 2024, doi: 10.1109/OJVT.2024.3422253.

[4] M. Liu *et al.*, "Enhancing Cyber-Resiliency of DER-based SmartGrid: A Survey," pp. 1–32, 2023, doi: 10.1109/TSG.2024.3373008.

[5] I. Kamenova, M. Chanev, P. Dimitrov, L. Filchev, B. Bonchev, and L. Zhu, "Crop Type Mapping and Winter Wheat Yield Prediction Utilizing," 2024.

[6] L. Zeng, Q. Liu, S. Shen, and X. Liu, "Improved Double Deep Q Network-Based Task Scheduling Algorithm in Edge Computing for Makespan Optimization," *Tsinghua Sci. Technol.*, vol. 29, no. 3, pp. 806–817, 2024, doi: 10.26599/TST.2023.9010058.

[7] W. Huang, B. Zhang, K. Zhang, H. Gao, and R. Wan, "Improved AutoEncoder with LSTM module and KL divergence," vol. 14, no. 8, pp. 1–12, 2024, [Online]. Available: http://arxiv.org/abs/2404.19247

[8] A. Farhadi, M. Mirzarezaee, A. Sharifi, and M. Teshnehlab, "Domain adaptation in reinforcement learning: a comprehensive and systematic study," *Front. Inf. Technol. Electron. Eng.*, vol. 25, no. 11, pp. 1446–1465, 2024, doi: 10.1631/FITEE.2300668.

[9] O. Friha, M. A. Ferrag, B. Kantarci, B. Cakmak, A. Ozgun, and N. Ghoualmi-Zine, "LLM-Based Edge Intelligence: A Comprehensive Survey on Architectures, Applications, Security and Trustworthiness," *IEEE Open J. Commun. Soc.*, vol. 5, no. September, pp. 1–1, 2024, doi: 10.1109/ojcoms.2024.3456549.

[10] Kingsley David Onyewuchi Ofoegbu, Olajide Soji Osundare, Chidiebere Somadina Ike, Ololade Gilbert Fakeyede, and Adebimpe Bolatito Ige, "Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols," *Comput. Sci. IT Res. J.*, vol. 5, no. 8, pp. 2083–2106, 2024, doi: 10.51594/csitrj.v5i8.1493.

[11] M. Latah and L. Toker, "Artificial intelligence enabled software-defined networking: A comprehensive overview," *IET Networks*, vol. 8, no. 2, pp. 79–99,

2019, doi: 10.1049/iet-net.2018.5082.

[12] F. Adnan, I. Amelia, and S. 'Umar Shiddiq, "Implementasi Voice Recognition Berbasis Machine Learning," *Implementasi Voice Recognit. Berbas. Mach. Learn.*, vol. 11, no. 1, pp. 24–29, 2022.

[13] S. O. Semerikov and A. M. Striuk, "Embracing Emerging Technologies: Insights from the 6th Workshop for Young Scientists in Computer Science & Software Engineering," *CEUR Workshop Proc.*, vol. 3662, pp. 1–36, 2024.

[14] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, pp. 1–29, 2021, doi: 10.1002/ett.4150.

[15] I. Khan, Junaid Khan, S. H. Bangash, Waqas Ahmad, A. I. Khan, and K. Hameed, "Intrusion Detection Using Machine Learning and Deep Learning Models on Cyber Security Attacks," *VFAST Trans. Softw. Eng.*, vol. 12, no. 2, pp. 95–113, 2024, doi: 10.21015/vtse.v12i2.1817.

[16] W. Ju *et al.*, "A Comprehensive Survey on Deep Graph Representation Learning," *Neural Networks*, vol. 173, pp. 287–356, 2024, doi: 10.1016/j.neunet.2024.106207.

[17] C. Ma *et al.*, "Trusted AI in Multiagent Systems: An Overview of Privacy and Security for Distributed Learning," *Proc. IEEE*, vol. 111, no. 9, pp. 1097–1132, 2023, doi: 10.1109/JPROC.2023.3306773.

[18] J. Veeramreddy, C. K. R. Vardhireddy, H. Thangella, K. Sarangula, R. Tamidilapati, and B. Pydala, *Hybrid Deep Learning Model for Detecting DDoS Attacks in IoT Networks*, no. Icciet. Atlantis Press International BV, 2024. doi: 10.2991/978-94-6463-471-6_42.

[19] N. Saran and N. Kesswani, "A comparative study of supervised Machine Learning classifiers for Intrusion Detection in Internet of Things," *Procedia Comput. Sci.*, vol. 218, no. January 2023, pp. 2049–2057, 2022, doi: 10.1016/j.procs.2023.01.181.

[20] L. Ge, X. Zhou, and Y. Li, "Designing Reward Functions Using Active Preference Learning for Reinforcement Learning in Autonomous Driving Navigation," *Appl. Sci.*, vol. 14, no. 11, 2024, doi: 10.3390/app14114845.

[21] B. Lin, K. Lin, C. Lin, Y. Lu, Z. Huang, and X. Chen, "Computation offloading strategy based on deep reinforcement learning for connected and autonomous vehicle in vehicular edge computing," *J. Cloud Comput.*, vol. 10, no. 1, 2021, doi: 10.1186/s13677-021-00246-6.

[22] E. Yaghoubi, E. Yaghoubi, A. Khamees, and A. H. Vakili, *A systematic review and meta-analysis of artificial neural network, machine learning, deep learning, and ensemble learning approaches in field of geotechnical engineering*, vol. 36, no. 21. Springer London, 2024. doi: 10.1007/s00521-024-09893-7.

[23] M. Neumayer, D. Stecher, S.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. XI No 2, Maret 2025, hlm. 329 – 336 ISSN 2550-0201 (Online)
DOI: http://dx.doi.org/10.33330/jurteksi.v11i2.3699
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Grimm, A. Maier, D. Bücker, and J. Schmidt, "Fault and anomaly detection in district heating substations: A survey on methodology and data sets," *Energy*, vol. 276, no. December 2022, p. 127569, 2023, doi: 10.1016/j.energy.2023.127569.