Journal of Information Technology and Computer Science
Journal Homepage: https://nicomarcinternationalpublishers.com/index.php/jitcs/index

JITCS
NICOMARC INTERNATIONAL PUBLISHERS

| RESEARCH ARTICLE

The Role of Artificial Intelligence in Cyber Security Defense

Peter Okebukola Soyinka

University of Ibadan, Ibadan, Nigeria

Corresponding Author: Peter Okebukola Soyinka, **E-mail**: petersoyinka@gmail.com

| ABSTRACT

With the recent surge in the adoption of digital technology and network systems, there have been increased complexities and frequencies in cyber threats, demanding responsive and smart defense mechanisms. Artificial Intelligence (AI) technology has been identified as a revolutionary paradigm in the domain of cybersecurity defense, providing superior intelligence for threat protection, prevention, and reaction compared to rule-based methods. This review brief will explore the recent trends in the use of AI for improving cybersecurity defenses. It will selectively summarize the recent literature on important technology used in cybersecurity defense, such as machine learning, deep learning, NLP, and behavioral analysis. Machine learning and deep learning have been widely used in developing intrusion detection systems, malware analysis tools, phishing attacks, anomaly analysis, and automated incident response. AI-powered tools provide superior accuracy in detecting sophisticated attacks such as zero-day attacks and advanced persistent threats in real-time through the analysis of complex patterns in massive amounts of security data. Additionally, the integration of AI with big data analytics in cloud infrastructure has provided better scalability in modern cybersecurity frameworks.Despite these benefits, the integration of AI technology in the realm of cybersecurity defense exhibits some challenges. These challenges include data quality, bias, explainability, and adversarial attack issues, relating to the trustworthiness and transparency of AI-powered defense systems. Furthermore, there is the problem of ethics, privacy concerns, and the lack of professional experts to facilitate proper integration. The dual-use aspect of AI is well emphasized, wherein the same technology that is beneficial to the defense system can be abused by cyber attackers to create sophisticated threats. In summary, AI technology is an important element that can boost the system of cybersecurity defense. AI technology is beneficial since it offers proactive, adaptive, and autonomous defense systems that can be efficient only through proper data governance, explainability, and human supervision.

| KEYWORDS

Artificial Intelligence (AI), Cybersecurity Defense, Machine Learning, Intrusion Detection Systems, Threat Detection and Prevention, Adversarial Attacks, Automated Security Response

| ARTICLE INFORMATION

ACCEPTED: 19 November 2025 **PUBLISHED:** 03 January 2026

1. Introduction

The accelerated development of digital technology means that people, businesses, and states can now function and connect in ways that were previously unimaginable (Li, 2018; Das & Sandhane, 2021). However, this digital revolution also provides more opportunities for cyber attackers, leading to increasing levels of cyberspace threats (Khan et al., 2025; Banik & Dandyala, 2023). Traditional defense mechanisms, largely dependent on manual rule-based systems, are no longer sufficient against modern threats, which include zero-day attacks, ransomware, phishing, and advanced persistent threats (Bonfanti, 2022; Truong et al., 2020). With the increasing intelligence of cyber attackers, there is a growing demand for smarter cyber defense tools (Tyugu, 2011; Timilehin, 2023).

Artificial Intelligence (AI) has emerged as a robust solution to the shortcomings of conventional cybersecurity mechanisms. AI can be defined as the ability of computer systems to perform tasks typically requiring human intelligence, such as learning, decision-making, and perception (Das & Sandhane, 2021; Jun et al., 2021). In cybersecurity defense, AI applications can handle large volumes of varied data and respond to security incidents in real time, representing a paradigm shift in defense strategies (Lysenko et al., 2024; De Azambuja et al., 2023).

Significant improvements in machine learning and deep learning have further enhanced AI capabilities. Machine learning algorithms enable continuous learning from past and current security events to detect anomalies and attacks that may evade traditional systems (Li, 2018; Khan et al., 2025). Deep learning algorithms have proven effective in identifying and categorizing malware and phishing attacks by extracting abstract features from raw data (Banik & Dandyala, 2023; Jia et al., 2023). Natural language processing techniques have also been applied to extract useful information from text-based files such as emails and security reports (Bonfanti, 2022; Jun et al., 2021).

The adoption of cloud computing, IoT devices, and big data has accelerated the deployment of AI in cybersecurity, generating massive, complex datasets beyond the capabilities of human analysis (De Azambuja et al., 2023; Morel, 2011). AI-enabled solutions provide the scale and speed needed to secure dynamic infrastructures and are increasingly integrated into security information and event management systems, endpoint protection, and threat intelligence platforms (Lysenko et al., 2024; Jia et al., 2023).

Despite its potential, AI in cybersecurity faces challenges such as data quality, model interpretability, algorithmic bias, and vulnerability to adversarial attacks (Taddeo et al., 2019; Bonfanti, 2022). Additionally, the dual-use nature of AI highlights the risk of malicious exploitation, making its study in cyber defense highly significant (Truong et al., 2020; Timilehin, 2023).

2. Literature Review

2.1 Artificial Intelligence in Modern Cybersecurity Frameworks

Existing literature highlights artificial intelligence as a core component of modern cybersecurity frameworks, addressing the limitations of traditional, rule-based security systems (Das & Sandhane, 2021; Li, 2018). Early cybersecurity approaches relied heavily on predefined signatures and manual analysis, which proved ineffective against rapidly evolving threats (Tyugu, 2011; Bonfanti, 2022). Recent studies emphasize how AI-driven systems enable adaptive security by learning from historical and real-time data to detect malicious activities (Jun et al., 2021; Khan et al., 2025). Researchers consistently report that AI enhances detection accuracy and reduces response time, particularly in large-scale and complex network environments (Banik & Dandyala, 2023; Lysenko et al., 2024). The integration of AI into security architectures has shifted cybersecurity from a reactive model toward a more proactive and predictive defense strategy (De Azambuja et al., 2023; Truong et al., 2020).

2.3 Machine Learning Techniques for Threat and Intrusion Detection

A significant body of research focuses on the application of machine learning algorithms in threat and intrusion detection (Li, 2018; Khan et al., 2025). Supervised learning techniques have been widely used for malware classification and spam detection, while unsupervised and semi-supervised methods are effective in anomaly detection and identifying unknown attacks (Das & Sandhane, 2021; Jun et al., 2021). Literature demonstrates that machine learning models can uncover subtle patterns in network traffic and system behavior that may indicate intrusions or advanced persistent threats (Banik & Dandyala, 2023; Lysenko et al., 2024). Comparative studies suggest that machine learning-based intrusion detection systems outperform traditional signature-based systems, particularly in detecting zero-day attacks and evolving malware variants (Truong et al., 2020; Bonfanti, 2022).

2.4 Deep Learning Applications in Malware and Phishing Detection

Recent literature underscores the growing use of deep learning techniques in cybersecurity defense (Jia et al., 2023; De Azambuja et al., 2023). Deep neural networks, including convolutional and recurrent neural networks, have shown strong performance in malware detection, phishing identification, and botnet analysis (Li, 2018; Bonfanti, 2022). Researchers note that deep learning models can automatically extract complex features from raw data, reducing reliance on manual feature engineering (Khan et al., 2025; Jun et al., 2021). Studies also highlight improvements in detection rates and robustness when deep learning is applied to large and diverse datasets (Banik & Dandyala, 2023; Lysenko et al., 2024). However, the literature acknowledges that deep learning models require substantial computational resources and high-quality data for optimal performance (Morel, 2011; Tyugu, 2011).

2.5 Behavioral Analytics and Anomaly Detection

Behavioral analytics has emerged as a key AI-driven approach in cybersecurity defense, focusing on understanding normal user and system behavior to detect anomalies (Jun et al., 2021; Das & Sandhane, 2021). Literature indicates that behavioral-based models are particularly effective in identifying insider threats and stealthy attacks that evade traditional detection mechanisms (Banik & Dandyala, 2023; Timilehin, 2023). By continuously learning baseline behaviors, AI systems can flag deviations that may signal compromised accounts or malicious activity (Lysenko et al., 2024; Khan et al., 2025). Researchers emphasize that behavioral analytics complements other AI-based security tools, enhancing overall situational awareness and threat detection capabilities (De Azambuja et al., 2023; Truong et al., 2020).

2.6 Automation and AI-Driven Incident Response

The role of AI in automating incident response has been widely discussed in recent studies (Jia et al., 2023; Das & Sandhane, 2021). Literature reveals that AI-powered security orchestration and automated response systems reduce the burden on human analysts by prioritizing alerts and executing predefined mitigation actions (Bonfanti, 2022; Lysenko et al., 2024). Automated incident response improves containment speed and minimizes potential damage from cyber incidents (Morel, 2011; Jun et al., 2021). However, researchers caution that excessive automation without human oversight may lead to false positives or unintended disruptions, highlighting the need for balanced human–AI collaboration (Timilehin, 2023; Khan et al., 2025).

2.7 Challenges and Ethical Considerations in AI-Based Cybersecurity

Despite the advantages of AI in cybersecurity defense, the literature identifies several challenges and ethical concerns. Issues such as data bias, lack of model explainability, and vulnerability to adversarial attacks raise questions about trust and accountability (Taddeo et al., 2019; Truong et al., 2020). Additionally, privacy concerns arise from the extensive data collection required for AI training (Li, 2018; Jun et al., 2021). Scholars also warn of the dual-use nature of AI, as attackers increasingly exploit AI technologies to develop more sophisticated cyber threats (Bonfanti, 2022; Khan et al., 2025). These challenges underscore the importance of robust governance frameworks and ethical guidelines (Timilehin, 2023; Das & Sandhane, 2021).

2.8 Future Directions of AI in Cybersecurity Defense

The literature suggests that future research should focus on developing explainable and resilient AI models to enhance trust and transparency in cybersecurity systems (Lysenko et al., 2024; Taddeo et al., 2019). Emerging trends include the integration of AI with threat intelligence sharing, edge computing, and zero-trust architectures (Jia et al., 2023; De Azambuja et al., 2023). Researchers advocate for interdisciplinary approaches combining technical innovation, policy development, and workforce training to maximize the effectiveness of AI-driven cybersecurity defense (Timilehin, 2023; Truong et al., 2020). Overall, the literature affirms that AI will continue to play a critical role in shaping the future of cybersecurity defense (Khan et al., 2025; Bonfanti, 2022).

3. Method

For this review, a systematic literature review technique has been applied to discuss the use of artificial intelligence in the defense capability of cybersecurity. A thorough search of peer-reviewed journals, proceedings of various conferences, and reputable electronic libraries like IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar has also been carried out. Keywords including "Artificial Intelligence in cybersecurity," "machine learning in threat detection," "deep learning in cybersecurity," "intrusion detection by AI," and "automated incident response" were utilized to search relevant literature that has been published within the last ten years.

Articles were reviewed to ascertain relevance to the discussion at hand, publishing quality, and value to comprehension of AI in cybersecurity defense engagements. Study types included quantitative and/or qualitative research encompassing theory development and research studies across a broad spectrum of engagements including case studies. Information abstracted encompassed development and application of AI technology. The review was done in an organized manner involving data extraction, analysis, and theming. Studies included in the analysis can be divided in accordance with AI approaches (machine learning, deep learning, BA) as well as application fields (malware analysis, intrusion detection, IR). Study outcomes were carefully reviewed for patterns, trends, and gaps in existing literature in order to form a balanced outlook on the role of AI in defense strategies.

4. Results and Discussion

Available literature on AI technology within the realm of cybersecurity defense showcases the revolutionary change it has caused, particularly in the detection, prevention, and response to threats (Das & Sandhane, 2021; Li, 2018). Traditional signature-based and rule-driven solutions struggle to keep pace with sophisticated cyber threats, such as ransomware, phishing, and zero-

day malware, while AI offers machine learning (ML), deep learning (DL), and behavioral analytics (BA) solutions capable of processing massive amounts of security data in real time (Khan et al., 2025; Banik & Dandyala, 2023).

Machine learning is the most widely applied AI method in cyber defense. Supervised learning algorithms, including decision trees, support vector machines, and random forests, are used for malware analysis, phishing detection, and network traffic monitoring (Das & Sandhane, 2021; Jun et al., 2021). Unsupervised and semi-supervised learning techniques are particularly effective for anomaly detection and identifying unknown threats (Li, 2018; Truong et al., 2020). Existing studies indicate that ML-based solutions outperform conventional signature-matching approaches in efficiency and accuracy (Banik & Dandyala, 2023; Lysenko et al., 2024).

Deep learning methods, especially convolutional neural networks (CNNs) and recurrent neural networks (RNNs), enhance the ability to detect complex and evolving threats (Jia et al., 2023; De Azambuja et al., 2023). These models automatically extract features from raw data, improving detection rates for malware, phishing, and botnet attacks compared to traditional ML models (Li, 2018; Bonfanti, 2022). However, DL implementation presents challenges due to high computational requirements and the need for extensive labeled datasets (Morel, 2011; Tyugu, 2011).

Behavioral analytics leverages AI to monitor normal system and user behavior, identifying deviations that indicate potential malicious activity (Jun et al., 2021; Das & Sandhane, 2021). Such approaches are particularly useful for insider threats and low-level attacks that evade conventional defenses (Banik & Dandyala, 2023; Timilehin, 2023). By establishing behavioral baselines, AI can flag anomalies in real time, complementing ML and DL models and enhancing situational awareness (Lysenko et al., 2024; Khan et al., 2025).

AI is also widely employed in automating incident response. AI systems can prioritize alerts, implement mitigation procedures, and autonomously isolate compromised systems (Jia et al., 2023; Das & Sandhane, 2021). Research shows that autonomous AI response solutions reduce mean time to detect (MTTD) and mean time to respond (MTTR), minimizing potential damage (Morel, 2011; Jun et al., 2021). However, excessive automation without human oversight can cause false positives or operational issues, highlighting the importance of balancing AI and human interaction (Bonfanti, 2022; Timilehin, 2023).

Despite its advantages, AI faces several challenges in cybersecurity. Data quality and accessibility are critical for effective implementation, and the lack of explainability in DL models hampers trust and accountability (Taddeo et al., 2019; Truong et al., 2020). Adversarial attacks, which manipulate AI inputs to deceive models, have emerged as a significant concern (Li, 2018; Jun et al., 2021). Ethical and privacy implications, especially regarding user monitoring, are also prominent (Khan et al., 2025; Bonfanti, 2022). Furthermore, the dual-use nature of AI allows malicious actors to exploit similar technologies for advanced attacks (Truong et al., 2020; Timilehin, 2023).

Emerging trends in AI for cybersecurity include integration with threat intelligence platforms, edge computing, and zero-trust architectures to improve real-time threat detection and mitigation (Jia et al., 2023; De Azambuja et al., 2023). Explainable AI (XAI) is gaining importance to increase transparency and trust in AI decision-making (Lysenko et al., 2024; Taddeo et al., 2019). Collaborative approaches combining human intelligence and AI have been advocated to enhance defense capabilities (Das & Sandhane, 2021; Timilehin, 2023).

In summary, the literature confirms that AI has emerged as a key pillar of modern cybersecurity defense. Machine learning, deep learning, behavioral analytics, and automated incident response collectively enhance detection, response, and resilience. However, challenges associated with data dependency, explainability, adversarial attacks, and ethics must be managed to fully realize the potential of AI-powered cybersecurity solutions (Khan et al., 2025; Bonfanti, 2022).

5. Conclusion

Increasing complexities and rising incidents of cyber threats make it imperative to develop sophisticated defense mechanisms that can respond effectively to rapidly changing cyber attack patterns and strategies. This review clearly establishes that artificial intelligence has emerged as a key ingredient in the present-day defense mechanisms of cyber security and provides a far better solution in this context compared to existing rule-based and signature-driven mechanisms of cyber defense. AI-based processes and solutions like machine learning algorithms, deep learning processes, behavioral analytics tools, and autonomous incident response tools always provide a better solution in detecting cyber threats and generating rapid responses to block them efficiently. Machine learning algorithms can identify existing and new threats by examining the patterns in large amounts of data in a short span of time; on the other hand, deep learning algorithms can provide even more accurate results by automatically

extracting relevant features based on complex data patterns. In addition, the use of AI in automatic response solutions increases the efficiency of operations by ensuring fewer manual responses to security events, thus facilitating fast containment and mitigation of the incident. It has been evident that the use of these solutions reduces the mean time to detect (MTTD) and mean time to respond (MTTR) to security threats, thus limiting potential losses from the operations. However, the review of the use of AI in cybersecurity operations also points out important challenges in the application of the technology. In terms of what is to come, a successful integration of AI into cybersecurity defense efforts is going to demand a certain amount of technical innovation, ethical framing, and human oversight. The latest trends being witnessed within this sector include explainable AI, AI-powered threat intelligence, and zero trust frameworks, which hold a lot of promises regarding enhancing cybersecurity frameworks. In order to tap into AI's full potential while managing risks, AI can only act as a transformative force within cybersecurity defense, ensuring a proactive, adaptive, and resilient defense of digital infrastructure against threats.

References

[1] Banik, S., & Dandyala, S. S. M. (2023). The role of artificial intelligence in cybersecurity opportunities and threats. *International Journal of Advanced Engineering Technologies and Innovations, 1*(04), 420–440.

[2] Bonfanti, M. E. (2022). *Artificial intelligence and the offence-defence balance in cyber security*. Cyber Security: Socio-Technological Uncertainty and Political Fragmentation (pp. 64–79). London: Routledge.

[3] Das, R., & Sandhane, R. (2021, July). Artificial intelligence in cyber security. In *Journal of Physics: Conference Series* (Vol. 1964, No. 4, p. 042072). IOP Publishing.

[4] De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics, 12*(8), 1920.

[5] Jia, Y., Gu, Z., Du, L., Long, Y., Wang, Y., Li, J., & Zhang, Y. (2023). Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the MDATA model. *Knowledge-Based Systems, 276*, 110781.

[6] Jun, Y., Craig, A., Shafik, W., & Sharif, L. (2021). Artificial intelligence application in cybersecurity and cyberdefense. *Wireless Communications and Mobile Computing, 2021*(1), 3329581.

[7] Khan, M. I., Arif, A., Khan, A. R. A., Anjum, N., & Arif, H. (2025). The dual role of artificial intelligence in cybersecurity: Enhancing defense and navigating challenges. *International Journal of Innovative Research in Computer Science and Technology, 13*, 62–67.

[8] Li, J. H. (2018). Cyber security meets artificial intelligence: A survey. *Frontiers of Information Technology & Electronic Engineering, 19*(12), 1462–1474.

[9] Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs, 69*, 43–51.

[10] Morel, B. (2011, October). Artificial intelligence and the future of cybersecurity. In *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence* (pp. 93–98).

[11] Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence, 1*(12), 557–560.

[12] Timilehin, O. (2023). *Defending the digital horizon: Artificial intelligence in cybersecurity warfare*.

[13] Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry, 12*(3), 410.

[14] Tyugu, E. (2011, June). Artificial intelligence in cyber defense. In *2011 3rd International Conference on Cyber Conflict* (pp. 1–11). IEEE.