International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 112 – 115, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1009

Advances in Cybersecurity: A Literature Review

Amrani Hassan
Technical University of Mombasa
Mombasa, Kenya

Kennedy Hadullo
Technical University of Mombasa
Mombasa, Kenya

Kelvin Tole
Technical University of Mombasa
Mombasa, Kenya

Abstract: The rapid proliferation of digital infrastructures, including cloud computing, the Internet of Things (IoT), and artificial intelligence (AI), has transformed the landscape of cybersecurity, introducing both new opportunities and heightened risks. This paper presents a comprehensive literature review of cybersecurity advancements between 2020 and 2024, focusing on the integration of AI and machine learning to address evolving threats. Thirty academic studies were analyzed to explore key themes, including the role of AI in threat detection, the security challenges posed by IoT, and the impact of generative AI technologies. AI and machine learning have demonstrated remarkable potential in improving cybersecurity frameworks, particularly through predictive models that enhance threat detection and reduce false positives. Generative AI, while presenting significant opportunities for defence, also poses new risks such as phishing, social engineering, and automated hacking, requiring sophisticated mitigation strategies. Similarly, the growing reliance on IoT devices, especially in industrial systems, has introduced vulnerabilities in communication and management protocols, which AI-driven solutions like federated learning aim to address by providing decentralized cybersecurity without compromising privacy. In addition, emerging trends such as cyber threat intelligence (CTI) mining have positioned organizations to adopt proactive defence strategies by identifying threats in real time. Despite these advancements, significant challenges remain, particularly around the ethical implementation of AI in cybersecurity and the need for standardized frameworks capable of addressing both current and future threats. The findings of this review emphasize the critical role of AI in shaping the future of cybersecurity while highlighting the importance of robust ethical standards and regulatory frameworks to mitigate the risks associated with advanced technologies like AI and IoT. Future research should prioritize the development of AI-driven cybersecurity solutions that are both effective and ethically sound.

Keywords: Cybersecurity, Artificial Intelligence (AI), Internet of Things (IoT), Generative AI, Threat Detection, Federated Learning

1. INTRODUCTION

Cybersecurity has become an increasingly crucial area of research and practice, especially given the rapid growth in digital infrastructures, cloud computing, IoT, and artificial intelligence (AI). Between 2020 and 2024, cybersecurity research has addressed challenges such as data breaches, ransomware attacks, AI-driven cyberattacks, and the risks posed by the Internet of Things (IoT). This review examines thirty academic studies published during this period, analyzing key contributions related to machine learning, AI, generative AI, IoT, and cybersecurity frameworks.

The rapid advancement of digital technologies such as cloud computing, the Internet of Things (IoT), and artificial intelligence (AI) has significantly increased the complexity of cybersecurity threats. Despite ongoing improvements in cybersecurity measures, the evolution of cyberattacks, including AI-driven threats and vulnerabilities in IoT systems, continues to outpace traditional security protocols. This growing gap between security measures and emerging threats poses a serious risk to individuals, businesses, and critical infrastructures. Thus, there is a pressing need to explore advanced methods, including the integration of AI and machine learning, to bolster cybersecurity frameworks effectively.

2. RESEARCH OBJECTIVES

The primary objective of this research is to critically review recent advancements in cybersecurity, focusing on the integration of AI and machine learning to enhance security protocols. The study aims to:

1. Assess the role of AI and machine learning in threat detection and mitigation.

2. Explore the risks and opportunities presented by generative AI in cybersecurity.

3. Analyze security challenges related to IoT devices and industrial systems.

To guide the investigation, the following research questions are posed:

1. How do AI and machine learning contribute to improving cybersecurity measures, particularly in threat detection?

2. What are the security risks posed by generative AI technologies, and how can these be mitigated?

3. What vulnerabilities exist in IoT systems, and how can AI-based solutions enhance IoT cybersecurity?

3. LITERATURE REVIEW

3.1 The Role of AI and Machine Learning in Cybersecurity

The use of machine learning and deep learning techniques in cybersecurity has gained significant attention. Mijwil (2023) highlights the potential of AI in safeguarding systems against unauthorized access by predicting the behavior of malicious software. The introduction of AI-driven automation in threat intelligence processes has also been a significant development, as highlighted by (Shah & Parast, 2024), who explored the use of GPT-4o models in threat report generation. These techniques offer sophisticated tools for threat detection and prevention in cybersecurity practices. Kaur et al., (2023) extend this discussion by exploring AI's role in enhancing security protocols, emphasizing its ability to detect and respond to security threats more efficiently than traditional methods. Furthermore, (Ferrari et al., 2024) discuss

the application of AI in cybersecurity education, highlighting its role in developing robust threat detection skills. Metta et al., (2024) underscore the importance of generative AI in both enhancing cybersecurity capabilities and introducing new challenges for threat detection.

3.2 Impact of Generative AI on Cybersecurity

The rise of generative AI, exemplified by models like ChatGPT, poses both opportunities and risks. Gupta et al., (2023) discuss how adversaries exploit vulnerabilities in generative AI to conduct social engineering attacks, phishing, and automated hacking. The transformative role of generative AI in enhancing threat detection and cyber resilience is further discussed by (Usman et al., 2024), who detail AI's capacity to automate complex cyber-attacks. Despite these risks, generative AI also offers significant defense potential, from threat intelligence automation to secure code generation. Similarly, (Sebastian, 2023) explores how AI-based chatbots, such as ChatGPT, pose potential cyber risks, highlighting examples where malicious actors have exploited vulnerabilities in these systems. Broklyn et al., (2024) argue that while generative AI can be leveraged for defensive measures like automated threat detection, it also introduces new vulnerabilities. Meanwhile, (Ramakrishnan & Chittibala, 2024) examined the convergence of Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and AI technologies, highlighting their role in proactive cybersecurity frameworks.

3.3 Cybersecurity in IoT and Industrial Systems

IoT devices have significantly expanded the attack surface, leading to novel cybersecurity challenges. A recent study by (Mekala et al., 2023) highlights the critical need for IoT-specific cybersecurity measures, especially in industrial IoT (IIoT) environments. The increasing reliance on IoT devices has introduced new cybersecurity challenges. Tariq et al., (2023) provide a comprehensive review of IoT-related security concerns, identifying key vulnerabilities in connectivity and management protocols. The integration of IoT in industrial environments, combined with AI, has provided significant potential for improving threat detection. Additionally, (Lone et al., 2023) discuss how IoT integration with AI can both enhance security and introduce new attack vectors, requiring sophisticated countermeasures. Federated learning, as discussed by (Ghimire & Rawat, 2022), is a promising decentralized model to enhance IoT cybersecurity, enabling better threat detection without compromising privacy. Furthermore, (Wang, 2023) discusses robust federated learning approaches for IoT security, focusing on anomaly detection to secure decentralized IoT networks. In addition, the Edge-IIoTset dataset introduced by (Ferrag et al., 2022) has become a critical resource for intrusion detection systems utilizing centralized and federated learning modes. Zhu et al., (2023) emphasize the integration of federated learning and blockchain to enhance the security of IoT networks without compromising data privacy.

3.4 AI-Driven Cyber Defense and Threat Intelligence

Deep learning approaches have proven effective in detecting cyberattacks on complex systems such as cyber-physical systems (CPSs). Zhang et al., (2021) demonstrate that AI models significantly improve the detection of cyber threats, particularly within CPS environments. Furthermore, the deployment of machine learning techniques, such as support vector machines (SVMs) and neural networks, has shown promising results in reducing false positives and improving the overall accuracy of threat detection systems. Additionally, (Albshaier et al., 2024) explore ransomware detection frameworks, stressing the need for proactive AI-driven approaches to mitigate ransomware attacks. Advanced AI algorithms are being utilized to bolster proactive defense mechanisms. Studies emphasize that the fusion of AI with cybersecurity frameworks significantly enhances resilience against cyber threats. For instance, (Sarker, 2024) discusses how AI-driven decision-making tools are transforming threat intelligence and response strategies, as well as (Hummelholm, 2023) discusses the convergence of AI and quantum-safe cybersecurity measures, especially in edge networks, highlighting the need for scalable and robust cybersecurity frameworks. Additionally, AI-based solutions, such as federated learning, are becoming crucial in identifying and countering complex cyber threats in real-time (Nyre-Yu et al., 2022).

3.5 Digital Transformation and Cybersecurity

The digital transformation of organizations has increased cybersecurity risks, particularly with the integration of new technologies such as blockchain, AI, and big data (Saeed et al., 2023) discuss the cybersecurity challenges posed by digital transformation and emphasize the importance of a staged cybersecurity readiness framework. This approach ensures that organizations can proactively address emerging threats while maintaining business resilience. A study by (Manea, 2023) underscores the crucial role of cybersecurity in enabling digital transformation, emphasizing that robust cyber defenses are critical for protecting sensitive information and ensuring operational resilience. Li, (2024) discusses the implications of digital transformation on supply chain resilience, emphasizing the need for enhanced cybersecurity measures to mitigate risks associated with the digitization of supply chains. This sentiment is echoed by (Harshada Umesh Salvi & Supriya Santosh Surve, 2023), who explore emerging trends in cybersecurity technologies to address challenges posed by digital transformation, proposing innovative frameworks for digital security.

3.6 Emerging Trends in Cybersecurity Research

Cyber threat intelligence (CTI) has emerged as a critical area for proactive cybersecurity defense. Sun et al., (2023) explore how CTI mining uncovers valuable insights into cyber threats, enabling organizations to improve their security postures. Similarly, (Ren et al., 2022) propose a cybersecurity knowledge graph for advanced persistent threat (APT) attribution, demonstrating its ability to enhance proactive threat detection. Taskeen & Garai, (2024) provide a comprehensive overview of emerging cybersecurity trends, suggesting a shift towards holistic frameworks that integrate AI for proactive threat detection. Akhtar & Rawol, (2024) explore the dual-edged impact of AI in cybersecurity, emphasizing both its potential in enhancing defense mechanisms and its vulnerability to exploitation by cyber adversaries. Srivastava et al., (2022) highlight the growing relevance of Explainable AI (xAI) in cybersecurity, advocating for transparent AI models to build trust and efficacy in automated defense systems. Furthermore, (Prathyush & Kumar, 2022) provide insights into the latest

cybersecurity techniques, focusing on AI-driven solutions to address challenges in IoT security.

4. RESEARCH METHODOLOGY

This study employs a systematic literature review to assess current advancements in cybersecurity research between 2020 This study, adopted the systematic literature review techniques developed by (Kitchenham et al., 2003) and (Torres-Carrión et al., 2018).The systematic approach encompassing the following key steps: Research questions, definition, design of search strategy, selection of studies, evaluation of quality, extraction and synthesis of data. The review focuses on academic articles that discuss AI, machine learning, IoT, and cybersecurity frameworks. A total of thirty academic studies were analyzed to identify key trends, challenges, and technological innovations. The selected studies were sourced from reputable journals and conferences in the fields of computer science and cybersecurity. The search criteria used keywords; "AI in Cybersecurity", "AI and Cybersecurity" "Role of AI in Cybersecurity", "Role of Machine Learning in Cybersecurity", "Security risks Gen AI". The results were grouped into themes for analysis. By evaluating the findings of these studies, the research aims to provide a comprehensive understanding of how AI and related technologies are shaping the future of cybersecurity.

5. RESULTS AND DISCUSSION

The literature review reveals that AI and machine learning are critical in enhancing cybersecurity, particularly in detecting and mitigating sophisticated cyber threats. Several studies demonstrate that AI-driven models, such as deep learning and support vector machines (SVMs), have significantly improved threat detection accuracy, especially in complex environments like cyber-physical systems (CPSs). However, the rise of generative AI technologies poses new risks, such as automated phishing attacks and the exploitation of AI vulnerabilities by adversaries. At the same time, generative AI holds potential for automating threat intelligence and generating secure code.

In the context of IoT, the increasing number of connected devices has introduced new vulnerabilities, particularly in industrial systems. AI-based solutions, such as federated learning, offer promising decentralized approaches to IoT security, allowing for better threat detection while preserving data privacy. Emerging trends such as cyber threat intelligence (CTI) mining further underscore the shift toward proactive defense strategies in cybersecurity, enabling organizations to identify and respond to threats before they cause significant damage.

Despite these advancements, the research highlights several gaps, particularly in the ethical implementation of AI-driven cybersecurity measures and the need for standardized frameworks that address both current and future cyber threats.

6. CONCLUSION

The period from 2020 to 2024 witnessed significant advancements in cybersecurity, driven largely by innovations in AI, machine learning, and IoT security. The reviewed studies emphasize the importance of integrating AI-driven solutions into cybersecurity frameworks, enabling faster threat detection and mitigation. However, the risks posed by new technologies, such as generative AI, underscore the need for robust security measures and ethical guidelines. Future research should focus on improving AI-based security measures, enhancing IoT security, and addressing the evolving nature of cyber threats.

7. REFERENCES

[1] Akhtar, Z. B., & Rawol, A. T. (2024). Harnessing artificial intelligence (AI) for cybersecurity: Challenges, opportunities, risks, future directions. Computing and Artificial Intelligence, 2(2), 1485. https://doi.org/10.59400/cai.v2i2.1485

[2] Albshaier, L., Almarri, S., & Rahman, M. M. H. (2024). Earlier Decision on Detection of Ransomware Identification: A Comprehensive Systematic Literature Review. Information, 15(8), 484. https://doi.org/10.3390/info15080484

[3] Broklyn, P., Shad, R., & Egon, A. (2024). The Evolving Thread Landscape Pf Ai-Powered Cyberattacks:A Multi-Faceted Approach to Defense And Mitigate; SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4904878

[4] Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. IEEE Access, 10, 40281–40306. https://doi.org/10.1109/ACCESS.2022.3165809

[5] Ferrari, E. P., Wong, A., & Khmelevsky, Y. (2024). Cybersecurity Education within a Computing Science Program—A Literature Review. The 26th Western Canadian Conference on Computing Education, 1–5. WCCCE '24: The 26th Western Canadian Conference on Computing Education. https://doi.org/10.1145/3660650.3660666

[6] G. Prem Prathyush & G. Pavan Durga Kumar. (2022). A Study of Cybersecurity and its Role in Information Technology along with the Emerging Trends and Latest Technologies. International Journal of Advanced Research in Science, Communication and Technology, 854–858. https://doi.org/10.48175/IJARSCT-7576

[7] Ghimire, B., & Rawat, D. B. (2022). Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. IEEE Internet of Things Journal, 9(11), 8229–8249. https://doi.org/10.1109/JIOT.2022.3150363

[8] Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy. IEEE Access, 11, 80218–80245. https://doi.org/10.1109/ACCESS.2023.3300381

[9] Harshada Umesh Salvi & Supriya Santosh Surve. (2023). Emerging Trends and Future Prospects of Cybersecurity Technologies: Addressing Challenges and Opportunities. International Journal of Scientific Research in Science and Technology, 399–406. https://doi.org/10.32628/IJSRST52310432

[10] Hummelholm, A. (2023). AI-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks. European Conference on Cyber Warfare and Security, 22(1), 696–702. https://doi.org/10.34190/eccws.22.1.1211

[11] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[12] Kitchenham, B., Fry, J., & Linkman, S. (2003). The case against cross-over designs in software engineering.

Eleventh Annual International Workshop on Software Technology and Engineering Practice, 65–67. https://ieeexplore.ieee.org/abstract/document/1372135/

[13] Li, R. (2024). The Impact and Challenges of Digital Transformation on Supply Chain Resilience in Physical Enterprises. Advances in Economics, Management and Political Sciences, 122(1), None-None. https://doi.org/10.54254/2754-1169/122/20242311

[14] Lone, A. N., Mustajab, S., & Alam, M. (2023). A comprehensive study on cybersecurity challenges and opportunities in the IOT world. SECURITY AND PRIVACY, 6(6), e318. https://doi.org/10.1002/spy2.318

[15] Mekala, S. H., Baig, Z., Anwar, A., & Zeadally, S. (2023). Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. Computer Communications, 208, 294–320. https://doi.org/10.1016/j.comcom.2023.06.020

[16] Metta, S., Chang, I., Parker, J., Roman, M. P., & Ehuan, A. F. (2024). Generative AI in Cybersecurity. https://doi.org/10.48550/ARXIV.2405.01674

[17] Mijwil, M., & Aljanabi, M. (2023). Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime. Iraqi Journal For Computer Science and Mathematics, 4(1), 65–70. http://journal.esj.edu.iq/index.php/IJCM/article/view/538

[18] Mijwil, M., Salem, I. E., & Ismaeel, M. M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. Iraqi Journal For Computer Science and Mathematics, 4(1), 87–101. https://www.iasj.net/iasj/download/e2b912a802ead428

[19] Nyre-Yu, M., Morris, E., Smith, M., Moss, B., & Smutz, C. (2022). Explainable AI in Cybersecurity Operations: Lessons Learned from xAI Tool Deployment. Proceedings 2022 Symposium on Usable Security. Symposium on Usable Security. https://doi.org/10.14722/usec.2022.23014

[20] Ramakrishnan, S., & Chittibala, D. R. (2024). Enhancing Cyber Resilience: Convergence of SIEM, SOAR, and AI in 2024. International Journal of Computing and Engineering, 5(2), 36–44. https://doi.org/10.47941/ijce.1754

[21] Ren, Y., Xiao, Y., Zhou, Y., Zhang, Z., & Tian, Z. (2022). CSKG4APT: A Cybersecurity Knowledge Graph for Advanced Persistent Threat Organization Attribution. IEEE Transactions on Knowledge and Data Engineering, 1–15. https://doi.org/10.1109/TKDE.2022.3175719

[22] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666

[23] Sarcea (Manea), O. A. (2023). How digital transformation and cyber security affect companies' performance? 530–540. Strategica. https://doi.org/10.25019/STR/2023.039

[24] Sarker, I. H. (2024). AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability. https://doi.org/10.1007/978-3-031-54497-2

[25] Sebastian, G. (2023). Do ChatGPT and Other AI Chatbots Pose a Cybersecurity Risk? - An Exploratory Study. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4363843

[26] Shah, S., & Parast, F. K. (2024, October 26). AI-Driven Cyber Threat Intelligence Automation. https://www.semanticscholar.org/paper/AI-Driven-Cyber-Threat-Intelligence-Automation-Shah-Parast/3a62acda417f2b5c886083f375a1ec9ac4457019

[27] Srivastava, G., Jhaveri, R. H., Bhattacharya, S., Pandya, S., Rajeswari, Maddikunta, P. K. R., Yenduri, G., Hall, J. G., Alazab, M., & Gadekallu, T. R. (2022). XAI for Cybersecurity: State of the Art, Challenges, Open Issues and Future Directions. https://doi.org/10.48550/ARXIV.2206.03585

[28] Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives. IEEE Communications Surveys & Tutorials, 25(3), 1748–1774. https://doi.org/10.1109/COMST.2023.3273282

[29] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors, 23(8), 4117. https://doi.org/10.3390/s23084117

[30] Taskeen, & Garai, S. (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. Blockchain in Healthcare Today, 7(1). https://doi.org/10.30953/bhty.v7.302

[31] Torres-Carrión, P. V., González-González, C. S., Aciar, S., & Rodríguez-Morales, G. (2018). Methodology for systematic literature review applied to engineering and education. 2018 IEEE Global Engineering Education Conference (EDUCON), 1364–1373. https://doi.org/10.1109/EDUCON.2018.8363388

[32] Usman, Y., Upadhyay, A., Gyawali, P., & Chataut, R. (2024). Is Generative AI the Next Tactical Cyber Weapon For Threat Actors? Unforeseen Implications of AI Generated Cyber Attacks. https://doi.org/10.48550/ARXIV.2408.12806

[33] Wang, H. (2023). Robust and Efficient Federated Learning for IoT Security. https://www.semanticscholar.org/paper/Robust-and-Efficient-Federated-Learning-for-IoT-Wang/b1f2134e64adc2b66348ef1eec184c1a238da532

[34] Zhang, J., Pan, L., Han, Q.-L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep learning based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA Journal of Automatica Sinica, 9(3), 377–391. https://ieeexplore.ieee.org/abstract/document/9536650/

[35] Zhu, L., Hu, S., Zhu, X., Meng, C., & Huang, M. (2023). Enhancing the Security and Privacy in the IoT Supply Chain Using Blockchain and Federated Learning with Trusted Execution Environment. Mathematics, 11(17), 3759. https://doi.org/10.3390/math11173759