WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AI-Driven Cybersecurity: Predictive Threat Detection in IoT and Edge Computing Ecosystems

Surya Kiran[a], Arjun Kumar[b], Swathi Chukkala[c]*

[a,b,c]Dept. Of Computer Science, GITAM University, Gandhi Nagar, Rushikonda, Visakhapatnam, Andhra Pradesh 530045, India

DOI : https://doi.org/10.55248/gengpi.6.0325.1126

A B S T R A CT

The rapid proliferation of Internet of Things (IoT) devices and the advancement of edge computing have significantly transformed the digital landscape, introducing new cybersecurity challenges. This article explores the integration of Artificial Intelligence (AI) into cybersecurity frameworks to enhance predictive threat detection in IoT and edge computing ecosystems. This research identifies key AI-driven methodologies and evaluates their effectiveness in mitigating cybersecurity threats by conducting a comprehensive literature review of recent studies. The study emphasizes the potential of predictive analytics to identify vulnerabilities and secure IoT networks preemptively. The findings reveal that AI, particularly machine learning and deep learning models, plays a crucial role in fortifying IoT and edge computing against evolving cyber threats. The paper concludes with a discussion of the limitations of current AI-driven cybersecurity solutions and suggests directions for future research to address these challenges.

Keywords: AI, Cybersecurity, Predictive Analytics, IoT Security, Edge Computing, Threat Mitigation

1. Introduction

The exponential growth of IoT devices, projected to reach over 75 billion by 2025, and the rise of edge computing have introduced unprecedented opportunities and challenges in cybersecurity (Yang et al., 2019). IoT devices, characterized by limited computational power and memory, are inherently vulnerable to cyber threats, necessitating robust security mechanisms. Edge computing, which decentralizes data processing closer to the data source, offers reduced latency and improved efficiency but presents unique security challenges (Maturi et al., 2020). Integrating AI into cybersecurity frameworks offers promising solutions for predictive threat detection, enabling real-time identification and mitigation of potential threats before they manifest (Niknam et al., 2020). This article examines the role of AI in enhancing cybersecurity within IoT and edge computing ecosystems, focusing on predictive analytics as a key enabler for threat mitigation.

However, current research exhibits gaps in several key areas. Firstly, there is a paucity of studies comprehensively evaluating the adversarial robustness of AI models deployed in IoT environments. While many papers focus on improving detection accuracy, fewer address how effectively these models withstand adversarial attacks designed to deceive them (Goodfellow et al., 2020). Secondly, the literature often overlooks the longitudinal impact of AI-driven cybersecurity solutions. Most studies offer a snapshot of performance at a specific time, neglecting the adaptive nature of both threats and defenses. Assessing the decay in performance over time and developing strategies for continuous model retraining and adaptation remains an open research question (Maturi et al., 2023). Addressing these gaps is crucial for AI's practical and sustainable deployment in IoT cybersecurity.

To contextualize the problem, consider the 2021 ransomware attack on the Colonial Pipeline, a major fuel pipeline in the United States. While not directly an IoT attack, the incident highlights the potential for devastating consequences when critical infrastructure lacks adequate cybersecurity (Gonaygunta et al., 2025). The initial intrusion occurred via a compromised VPN account, demonstrating the vulnerability of even seemingly secure systems. Had AI-driven predictive threat detection been more robustly implemented across their network, the anomaly could have been identified earlier, potentially preventing the attack and subsequent disruption of fuel supplies (Meduri et al., 2023). This real-world example underscores the urgent need for advanced cybersecurity solutions in interconnected systems, which AI can potentially provide, assuming researchers address the identified gaps.

2. Literature Review

Recent studies have highlighted the critical role of AI in cybersecurity, particularly in the context of IoT and edge computing, and explored federated machine learning to enhance privacy and security in distributed systems, emphasizing its potential in IoT networks (Kairouz et al., 2021). provided a systematic review of quantum computing, identifying its potential to revolutionize AI algorithms for cybersecurity applications discussed federated

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000.
E-mail address: author@institute.xxx

learning in wireless communications, underscoring its significance in bridging distributed AI and privacy, a crucial consideration for IoT security (Yang et al., 2020).

(Meduri et al., 2024) Examined AI-driven predictive techniques for cybersecurity, highlighting the challenges posed by the dynamic nature of IoT environments. Their findings suggest that AI can significantly enhance threat detection capabilities by leveraging real-time data analytics. (Li et al., 2020) addressed the challenges and methods associated with federated learning, proposing strategies to overcome non-IID data issues prevalent in IoT networks. (Zhao et al., 2023) further explored federated learning with non-IID data, providing insights into its applicability in diverse IoT ecosystems.

Discussed the vision and challenges of edge computing, emphasizing the need for robust security frameworks to protect data integrity and privacy. advanced this discussion by integrating federated deep learning into edge computing proposing strategies to enhance threat detection and mitigation. introduced the concept of edge intelligence, highlighting the convergence of IoT and AI as a transformative force in cybersecurity (Deng et al., 2020).

Building on this foundation, recent works further refine AI-driven security in IoT. For instance, presented a novel anomaly detection framework using a hybrid deep learning model combining Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks for identifying malicious traffic patterns in IoT networks (Ullah & Mahmoud, 2021). Their results demonstrated superior accuracy compared to traditional machine learning algorithms. In another study, (Rathod et al., 2023) investigated the use of blockchain technology in conjunction with AI to create a secure and transparent data-sharing platform for IoT devices, mitigating data tampering and ensuring data integrity. This approach leverages the immutability of blockchain to enhance the trustworthiness of AI-driven security decisions. Furthermore, recent research by (Khamitov et al., 2024) focused on developing energy-efficient AI algorithms for resource-constrained IoT devices. They proposed a model compression technique that reduces the computational overhead of deep learning models without significantly sacrificing accuracy, enabling the deployment of sophisticated security measures on low-power devices.

However, a critical analysis reveals methodological limitations in some existing studies. For example, the study on federated machine learning relies heavily on simulated data, which may not accurately reflect the complexities and nuances of real-world IoT environments (Nadella, 2024). While allowing for precise evaluation of the algorithm's performance, the controlled experimental setup limits the generalizability of the findings to practical scenarios where data is often noisy, incomplete, and subject to adversarial manipulation. Similarly, the work by Meduri et al. 2024 focuses primarily on static analysis of network traffic, neglecting the dynamic and adaptive nature of modern cyber threats. Their approach may be vulnerable to *adversarial evasion* techniques, where attackers modify their behavior to avoid detection by the AI model. Future research should address these limitations by incorporating real-world datasets, conducting extensive *adversarial testing*, and developing adaptive AI models that can learn and evolve in response to changing threat landscapes.

3. Methodology

This study employs a qualitative research methodology, conducting a comprehensive literature review to identify and analyze key AI-driven cybersecurity strategies in IoT and edge computing ecosystems. The selection criteria for the literature review included peer-reviewed journal articles published from 2020 onwards, focusing on AI, IoT security, and edge computing. The analysis critically evaluated each study's methodologies, findings, and implications, emphasizing identifying common themes and emerging trends in AI-driven cybersecurity (Zhou et al., 2024).

To enhance the analytical rigor of the study, a hybrid approach combining Natural Language Processing (NLP) with graph theory is proposed. NLP techniques can be employed to extract key concepts and relationships from the selected literature. At the same time, graph theory can represent these relationships as a network of interconnected nodes and edges (Meduri et al., 2024). This approach allows for a more systematic and comprehensive literature analysis, identifying hidden patterns and emerging trends that may not be apparent through traditional qualitative methods. Specifically, topic modeling using Latent Dirichlet Allocation (LDA) can identify prominent themes within the cybersecurity literature. At the same time, network analysis can reveal the interconnections between different research areas and identify influential publications (Li, 2023).

This hybrid methodology is justified by its ability to provide both breadth and depth in the analysis of the cybersecurity literature. NLP techniques enable the efficient processing of large volumes of text data, while graph theory provides a powerful framework for visualizing and analyzing complex relationships (Shi et al., 2016). The study can better understand the AI-driven cybersecurity landscape in IoT and edge computing ecosystems by combining these two approaches. This methodology provides a structured and rigorous approach to synthesizing information from diverse sources, facilitating the identification of key research gaps and informing future research directions.

4. Results and Discussion

The analysis reveals that AI-driven cybersecurity frameworks offer significant advantages in predictive threat detection for IoT and edge computing ecosystems. Machine learning models, particularly those employing deep learning techniques, have demonstrated superior capabilities in identifying and mitigating cybersecurity threats in real time (Meduri et al., 2024). These models leverage datasets from IoT devices to identify patterns and anomalies indicative of potential threats, enabling proactive threat mitigation. Federated learning is a promising approach to enhancing IoT security by enabling decentralized data processing while preserving privacy (Li et al., 2020). This approach addresses the challenges associated with data heterogeneity and privacy concerns in IoT networks, facilitating the development of robust security frameworks. Integrating federated learning with edge computing further enhances the scalability and efficiency of AI-driven cybersecurity solutions (Nadella, 2024).

However, the study also identifies several limitations of current AI-driven cybersecurity frameworks. IoT environments' dynamic and heterogeneous nature poses significant challenges in developing generalized AI models capable of adapting to diverse threat landscapes (Meduri et al., 2024). Additionally, the computational limitations of IoT devices constrain the deployment of complex AI algorithms, necessitating the development of lightweight models optimized for edge-computing environments (Shi et al., 2016).

These findings contrast with the conclusions drawn by some studies that advocate for rule-based expert systems in IoT security. While expert systems offer interpretability and can effectively address known threats, they lack AI-driven approaches' adaptability and learning capabilities (Mishra et al., 2019). Furthermore, the study by Anderson et al. suggests that traditional intrusion detection systems are sufficient for securing IoT networks, arguing that the complexity of AI models is unnecessary and potentially introduces new vulnerabilities. However, this view fails to account for the evolving sophistication of cyber threats and the increasing volume of data generated by IoT devices, necessitating advanced analytics techniques (Yadav, 2021). The present analysis, grounded in a comprehensive review of recent literature, supports the conclusion that AI-driven cybersecurity frameworks offer a superior approach to predictive threat detection in IoT and edge computing ecosystems compared to traditional methods.

4.1 Ethical Considerations for Deployment

The deployment of AI-driven cybersecurity solutions in IoT and edge computing raises significant ethical considerations that must be addressed to ensure responsible and equitable use of these technologies. One key concern is algorithmic bias, where AI models trained on biased data perpetuate and amplify societal inequalities (Wayz, 2025). For example, suppose an AI-driven security system is trained primarily on data from high-income households. In that case, it may be less effective at detecting threats in low-income communities, leading to disparate security outcomes. To mitigate this risk, it is crucial to ensure that training data is diverse, representative, and free from bias (Sanghavi, 2024). Furthermore, explainable AI (XAI) techniques should be employed to understand how AI models make decisions, allowing for identifying and correcting biases.

Another ethical consideration is privacy. AI-driven security systems often collect and analyze sensitive data, raising concerns about the potential for surveillance and misuse of personal information. Differential privacy techniques can be used to protect individual privacy while still enabling the use of data for security purposes (Dwork, 2006). Additionally, clear and transparent data governance policies should be established to ensure that data is collected, stored, and used responsibly and ethically. Moreover, AI-driven security systems' potential for autonomous decision-making raises questions about accountability and control. It is essential to establish clear lines of responsibility for the actions of these systems and to ensure that human oversight is maintained, particularly in critical situations (Segar & Zolkipli, 2024). By proactively addressing these ethical considerations, the cybersecurity community can ensure that AI-driven security solutions are deployed in a manner that is both effective and ethically sound.

5. Conclusion

Integrating AI into cybersecurity frameworks offers promising solutions for predictive threat detection in IoT and edge computing ecosystems. By leveraging machine learning and deep learning techniques, AI-driven cybersecurity solutions can effectively identify and mitigate emerging threats, enhancing the security and resilience of IoT networks. However, several challenges remain, including the need for generalized AI models capable of adapting to dynamic IoT environments and the development of lightweight algorithms suitable for deployment on resource-constrained devices.

Future research should address these challenges by exploring novel AI methodologies and developing adaptive models that dynamically respond to evolving threat landscapes. Additionally, integrating quantum computing and federated learning into AI-driven cybersecurity frameworks holds significant potential for enhancing the efficiency and effectiveness of threat detection and mitigation strategies (Gonaygunta et al., 2024). The cybersecurity community can develop robust solutions to secure the rapidly expanding IoT and edge computing ecosystems by advancing these research directions.

To further strengthen cybersecurity in these domains, the following actionable policy recommendations are proposed:

1. Mandatory Cybersecurity Standards for IoT Devices: Governments should establish minimum cybersecurity standards for IoT devices to protect them adequately against common threats. These standards should include requirements for secure software updates, strong authentication mechanisms, and vulnerability disclosure programs.

2. Incentivize the Development of Lightweight AI Algorithms: Funding agencies should prioritize research grants to develop lightweight AI algorithms that can be deployed on resource-constrained IoT devices. This will enable the widespread adoption of AI-driven security solutions in IoT ecosystems.

3. Promote Data Sharing and Collaboration: Cybersecurity organizations and industry stakeholders should collaborate to share threat intelligence and develop common data standards. This will improve the accuracy and effectiveness of AI-driven threat detection systems.

Future QML algorithms may be able to discern subtle patterns indicative of fraud that are imperceptible to classical machine learning methods, especially in scenarios with high data dimensionality and intricate correlations. Furthermore, research into *explainable adversarial defense* would be invaluable. Developing techniques that defend against adversarial attacks and provide insights into the nature of these attacks would significantly improve the robustness and trustworthiness of AI-driven cybersecurity systems. Finally, a comprehensive analysis of the *economic impact* of AI-driven cybersecurity solutions in IoT and edge computing is needed to justify investment and drive adoption. The cybersecurity community can develop even more effective and efficient solutions for securing the rapidly evolving digital landscape by exploring these future research directions.

References

Deng, S., Zhao, H., Fang, W., Yin, J., Dustdar, S., & Zomaya, A. Y. (2020). Edge intelligence: The confluence of Edge Computing and artificial intelligence. IEEE Internet of Things Journal, 7(8), 7457–7469. https://doi.org/10.1109/jiot.2020.2984887

Dwork, C. (2006). Differential Privacy. Lecture Notes in Computer Science, 1–12. https://doi.org/10.1007/11787006_1

Gonaygunta, H., Maturi, M. H., Nadella, G. S., Meduri, K., & Satish, S. (2024). Quantum Machine Learning: Exploring Quantum algorithms for enhancing deep learning models. International Journal of Advanced Engineering Research and Science, 11(5), 35–41. https://doi.org/10.22161/ijaers.115.5

Gonaygunta, H., Nadella, G. S., & Meduri, K. (2025). Utilizing logistic regression in machine learning for categorizing social media advertisement. Indonesian Journal of Electrical Engineering and Computer Science, 37(3), 1954. https://doi.org/10.11591/ijeecs.v37.i3.pp1954-1963

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2020). Generative Adversarial Networks. Communications of the ACM, 63(11), 139–144. https://doi.org/10.1145/3422622

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Nitin Bhagoji, A., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R., D'Oliveira, R. G., Eichner, H., El Rouayheb, S., Evans, D., Gardner, J., Garrett, Z., Gascón, A., Ghazi, B., Gibbons, P. B., … Zhao, S. (2021). Advances and open problems in Federated Learning. Foundations and Trends® in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083

Khamitov, R., Orel, D., & Zorbas, D. (2024). Predicting solar-harvested energy for resource-constrained IOT devices using machine learning. 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), 661–668. https://doi.org/10.1109/dcoss-iot61029.2024.00103

Li, H. (2023). Latent dirichlet allocation. Machine Learning Methods, 439–471. https://doi.org/10.1007/978-981-99-3917-6_20

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 37(3), 50–60. https://doi.org/10.1109/msp.2020.2975749

Maturi, M. H., Gonaygunta, H., Nadella, G. S., & Meduri, K. (2023). Fault diagnosis and prognosis using IOT in industry 5.0. International Numeric Journal of Machine Learning and Robots. https://injmr.com/index.php/fewfewf/article/view/80

Meduri, K., Gonaygunt, H., & Nadella, G. S. (2024). Enhancing cybersecurity with Artificial Intelligence: Predictive techniques and challenges in the age of IOT. (2024). International Journal of Science and Engineering Applications. https://doi.org/10.7753/ijsea1304.1007

Meduri, K., Gonaygunt, H., & Nadella, G. S. (2024). Evaluating the effectiveness of AI-driven frameworks in predicting and preventing cyber attacks. International Journal of Research Publication and Reviews, 5(3), 6591–6595. https://doi.org/10.55248/gengpi.5.0324.0875

Meduri, K., Nadella, G., Gonaygunta, H., & Meduri, S. (2023). Developing a Fog Computing-based AI Framework for Real-time Traffic Management and Optimization. International Journal of Sustainable Development in Computing Science, 5(4), 1-24. Retrieved from https://www.ijsdcs.com/index.php/ijsdcs/article/view/517

Mishra, D. P., Mahapatra, S., & Pradhan, S. K. (2019). Performance Improvement of Intrusion Detection Systems. International Journal of Innovative Technology and Exploring Engineering, 8(10), 3705–3712. https://doi.org/10.35940/ijitee.j9669.0881019

Mohan Harish Maturi, Snehal Satish, Karthik Meduri, & Geeta Sandeep Nadella. (2020). Quantum Computing in 2020: A systematic review of algorithms, hardware development, and practical applications. Universal Research Reports, 7(10), 140–154. https://doi.org/10.36676/urr.v7.i10.1427

Nadella, G. S. (2024). Advancing Edge Computing with Federated Deep Learning: Strategies and challenges. International Journal for Research in Applied Science and Engineering Technology, 12(4), 3422–3434. https://doi.org/10.22214/ijraset.2024.60602

Niknam, S., Dhillon, H. S., & Reed, J. H. (2020). Federated Learning for Wireless Communications: Motivation, opportunities, and challenges. IEEE Communications Magazine, 58(6), 46–51. https://doi.org/10.1109/mcom.001.1900461

Rathod, T., Jadav, N. K., Tanwar, S., Polkowski, Z., Yamsani, N., Sharma, R., Alqahtani, F., & Gafar, A. (2023). Ai and blockchain-based secure data dissemination architecture for IOT-enabled critical infrastructure. Sensors, 23(21), 8928. https://doi.org/10.3390/s23218928

Sanghavi, M. (2024). Software for explainable AI. Explainable, Interpretable, and Transparent AI Systems, 266–278. https://doi.org/10.1201/9781003442509-15

Segar, M., & Zolkipli, M. F. (2024). A study on AI-Driven Solutions for Cloud Security Platform. INTI Journal, 2024(1). https://doi.org/10.61453/intij.202453

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646. https://doi.org/10.1109/jiot.2016.2579198

Ullah, I., & Mahmoud, Q. H. (2021). Design and development of a deep learning-based model for anomaly detection in IOT networks. IEEE Access, 9, 103906–103926. https://doi.org/10.1109/access.2021.3094024

Wayz, W. (2025). AI-Driven Cybersecurity Solutions Enhancing Threat Detection in Healthcare and Airlines. https://doi.org/10.20944/preprints202501.1352.v1

Yadav, V. (2021). Cybersecurity in healthcare IOT devices: Studying the vulnerabilities and defence mechanisms for IOT devices used in healthcare settings. International Journal of Science and Research (IJSR), 10(1), 1675–1681. https://doi.org/10.21275/sr24724152143

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19. https://doi.org/10.1145/3298981

Yang, Q., Liu, Y., Cheng, Y., Kang, Y., Chen, T., & Yu, H. (2020). Distributed machine learning. Synthesis Lectures on Artificial Intelligence and Machine Learning, 33–48. https://doi.org/10.1007/978-3-031-01585-4_3

Zhao, S., Liao, T., Fu, L., Chen, C., Bian, J., & Zheng, Z. (2023). Data-Free Knowledge Distillation via Generator-Free Data Generation for Non-IID Federated Learning. https://doi.org/10.21203/rs.3.rs-3364332/v1

Zhou, H., Zheng, Y., & Jia, X. (2024). Towards robust and privacy-preserving federated learning in Edge Computing. Computer Networks, 243, 110321. https://doi.org/10.1016/j.comnet.2024.110321