ISSN: 0974-6471, Vol. 17, No. (1) 2025, Pg. 26-29

Oriental Journal of Computer Science and Technology

www.computerscijournal.org

Artificial Intelligence in IoT Security: Uncovering Opportunities and Threats

FASEL QADIR[1]* and IMTIYAZ HASSAN[2]

Department of Computer Science DCC, Shaqrs University, Kingdom Saudi Arabia.

ABSTRACT

The integration of Artificial Intelligence (AI) into the Internet of Things (IoT) ecosystem has transformed the landscape of cybersecurity. While IoT systems enable ubiquitous connectivity and automation across industries, they are also highly susceptible to cyberattacks due to their heterogeneity, limited resources, and scalability challenges. AI-based techniques, including machine learning, deep learning, and reinforcement learning, offer promising approaches to detecting anomalies, preventing intrusions, and predicting emerging threats in IoT networks. However, these opportunities are accompanied by significant challenges such as adversarial attacks, data privacy concerns, computational limitations, and the interpretability of AI models. This review article critically analyzes the dual role of AI in IoT security, highlighting its potential as both a defender and an enabler of cyber threats. Various AI-driven techniques are systematically reviewed, their applications in IoT security are discussed, and emerging risks are evaluated. The article further identifies future directions, emphasizing the importance of explainable AI, lightweight security frameworks, and robust adversarial defense mechanisms for sustainable and resilient IoT ecosystems.

Article History

Received: 03 May 2025
Accepted: 05 August 2025

Keywords

Artificial Intelligence; Internet of Things; IoT Security; Machine Learning; Deep Learning; Anomaly Detection; Cybersecurity; Adversarial Attacks

Introduction

The Internet of Things (IoT) has emerged as a transformative technology, enabling billions of interconnected devices to exchange data and deliver intelligent services in healthcare, transportation, smart homes, and industrial systems. However, the very features that make IoT powerful—ubiquity, decentralization, and heterogeneity—also make it vulnerable to cyber threats. Attacks such as Distributed Denial-of-Service (DDoS), man-in-the-middle, spoofing, and ransomware have exposed the inadequacy of conventional security models in handling the scale and complexity of IoT.

Artificial Intelligence (AI) has gained prominence as a security enabler, capable of analyzing massive streams of IoT data, detecting anomalies in real time, and adapting to evolving attack patterns. Machine learning (ML) and deep learning (DL) models have been applied to intrusion detection, malware classification, and traffic analysis. At the same time, AI introduces new vulnerabilities, such as adversarial attacks on ML models, data poisoning, and algorithm manipulation. This dual role of AI creates a paradox: while it strengthens IoT defense mechanisms, it simultaneously equips adversaries with sophisticated attack tools.

CONTACT Fasel Qadir ✉ f.qadir@su.edu.sa Computer Science Department DCC, Shaqrs University, Kingdom Saudi Arabia.

Doi: http://dx.doi.org/10.13005/ojcst17.01.08

This article reviews the opportunities and threats of AI in IoT security. It provides an in-depth analysis of AI-driven defense mechanisms, potential risks, and research gaps, aiming to guide future PhD-level research in building trustworthy and explainable AI-based IoT security solutions.

Material and Methods

This review adopts a systematic literature review methodology. Scholarly articles published between 2016 and 2025 were collected from IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and Scopus databases. Keywords such as AI in IoT security, machine learning for IoT cybersecurity, adversarial AI IoT, and anomaly detection IoT were used.

Inclusion criteria:

- Peer-reviewed articles and conference papers.
- Studies focusing on AI techniques applied to IoT security.
- Publications addressing both opportunities and threats.

Exclusion criteria

- Articles not related to IoT or AI.
- General cybersecurity studies without IoT-specific context.

A total of 145 articles were screened, of which 62 were selected for final analysis. The extracted data were categorized into AI opportunities, threats, and hybrid perspectives.

Results and Discussion

Opportunities of AI in IoT Security

AI provides robust mechanisms to enhance IoT security:

- **Anomaly Detection:** ML models detect abnormal device behaviors in real-time IoT traffic.
- **Intrusion Detection Systems (IDS):** DL architectures (CNN, RNN, LSTM) identify malware and intrusion attempts.
- **Predictive Security:** Reinforcement learning predicts evolving attack patterns.
- **Automated Decision-Making:** AI-driven orchestration of security protocols improves response time.
- **Federated Learning:** Enables distributed IoT devices to collaboratively train models without compromising privacy.

Threats of AI in IoT Security

AI is not only a defensive tool but also an enabler of threats:

- **Adversarial Attacks:** Attackers craft perturbations to fool AI models, bypassing IDS.
- **Data Poisoning:** Malicious data injections corrupt AI training datasets.
- **Model Inversion & Privacy Breaches:** Attackers extract sensitive information from AI models.
- **Resource Exploitation:** Heavy AI computations strain IoT devices with limited processing capabilities.
- **Dual-use AI:** Attackers employ AI to automate reconnaissance and optimize cyberattacks.

Balancing Opportunities and Risks

To harness AI securely, IoT ecosystems must integrate:

- **Explainable AI (XAI):** Enhances trust and interpretability of decisions.
- **Lightweight AI Models:** Optimized for resource-constrained IoT devices.
- **Adversarial Defense Mechanisms:** Defensive distillation, robust training, and GAN-based anomaly detection.
- **Hybrid Security Frameworks:** Combining AI with traditional cryptographic measures.

Table 1: Summary of AI-driven applications in IoT security

AI Technique	Application in IoT Security	Advantages	Limitations
Machine Learning	Anomaly detection, IDS	Fast detection, scalable	Data quality dependent
Deep Learning	Malware classification, traffic analysis	High accuracy, automated feature extraction	High computation
Reinforcement Learning	Adaptive threat mitigation	Dynamic learning, self-optimization	Training complexity
Federated Learning	Privacy-preserving collaborative learning	Protects data privacy	Communication overhead

Table 2: AI-enabled threats in IoT security

Threat Type	Description	Impact on IoT Security
Adversarial Attacks	Perturbed inputs deceive AI models	IDS bypass, false negatives
Data Poisoning	Injection of malicious data into training sets	Corrupts model accuracy
Model Inversion	Extraction of sensitive data	Privacy breaches
Dual-use AI	Attackers use AI for reconnaissance	Accelerated cyberattacks

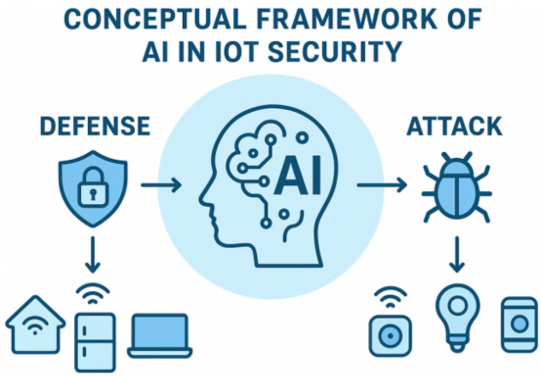

Fig. 1. Conceptual framework of AI in IoT security (showing AI as both a defense and attack enabler)

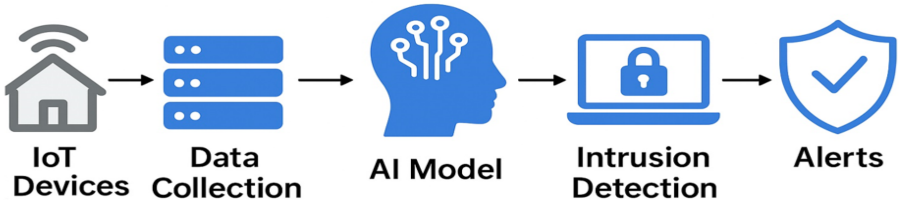

Fig. 2. Workflow of AI-driven IoT Intrusion Detection System

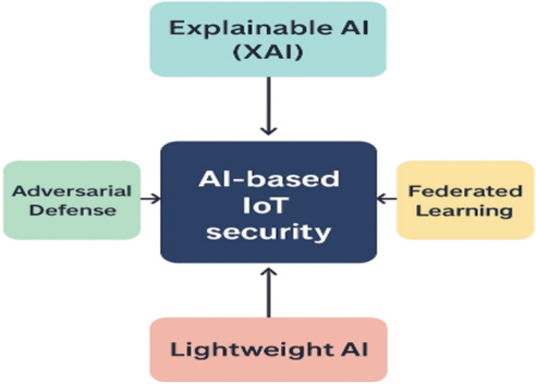

Fig. 3. Emerging research directions in AI-based IoT security (XAI, federated learning, lightweight AI, adversarial defense)

Conclusion

AI has emerged as both a safeguard and a potential threat to IoT security. While it strengthens anomaly detection, intrusion prevention, and predictive defenses, it simultaneously creates new vulnerabilities through adversarial attacks and misuse. A balanced approach integrating explainable AI, adversarial defense, and lightweight models is essential to ensure resilient IoT ecosystems. Future research must focus on the duality of AI in IoT, developing hybrid frameworks that combine AI-driven intelligence with classical security measures. This review highlights both the opportunities and inherent risks, offering a roadmap for PhD-level inquiry and innovation in AI-driven IoT security.

Acknowledgment

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of interest

The author declare that we have no conflict of interest.

REFERENCES

1. Abomhara, M., & Køien, G. M. Security and privacy in the Internet of Things: Current status and open issues., *Computer Networks*., *77*, 10-28, 2015.
2. Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., Guizani, M. A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Communications Surveys & Tutorials*., *22*(3), 1646-1685, 2020.
3. Chen, T. M., & Bridges, R. A. Automated behavioral analysis of malware: A case study of WannaCry ransomware., *Journal of Information Security and Applications*., *42*, 24-36, 2017.
4. Doshi, R., Apthorpe, N., & Feamster, N. Machine learning DDoS detection for consumer IoT devices., *IEEE Security and Privacy Workshops*, 29-35, 2018.
5. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions., *Future Generation Computer Systems*., *29*(7), 1645-1660, 2013.
6. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. Future Internet: The Internet of Things architecture, possible applications and key challenges. 10th International Conference on Frontiers of Information Technology., 2012.
7. Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. DDoS in the IoT: Mirai and other botnets., *Computer.*, *50*(7), 80-84, 2017.
8. Liu, X., Yu, W., Griffith, D., & Golmie, N. Towards deep learning in industrial IoT security: Approaches and case studies., *IEEE Internet of Things Journal*, *5*(4), 3209-3224, 2018.
9. Mosenia, A., & Jha, N. K. A comprehensive study of security of Internet-of-Things., *IEEE Transactions on Emerging Topics in Computing*., *5*(4), 586-602, 2017.
10. Nguyen, T. N., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., & Sadeghi, A. DÏoT: A federated self-learning anomaly detection system for IoT., *IEEE ICDCS*., 756-767, 2019.
11. Papernot, N., McDaniel, P., & Goodfellow, I. Practical black-box attacks against machine learning. Proceedings of the ACM on Asia Conference on Computer and Communications Security., 2017.
12. Sarker, I. H. Machine learning-based cybersecurity intrusion detection: State-of-the-art and future research directions., *Journal of Big Data*., *9*(1), 1-41, 2022.
13. Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. Internet of Things (IoT) for next-generation smart systems: A review of security challenges, machine learning solutions, and future trends., *IEEE Access*., *8*, 23022-23040, 2020.
14. Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. Twenty security considerations for cloud-supported Internet of Things., *IEEE Internet of Things Journal*., *3*(3), 269-284, 2016.
15. Suo, H., Wan, J., Zou, C., & Liu, J. Security in the Internet of Things: A Review. *International Conference on Computer Science and Electronics Engineering*., 3, 648-651, 2012.
16. Tang, Y., Mhamdi, E. M., Bellet, A., & Tommasi, M. Privacy-preserving machine learning in IoT: Threats and solutions., *IEEE Internet of Things Journal*., *6*(3), 5400-5411, 2019.
17. Verma, P., & Ranga, V. Machine learning-based intrusion detection systems for IoT applications: A Review. *Journal of Information Security and Applications*., *42*, 95-104, 2019.
18. Xu, R., Lin, Y., & Luo, Y. Adversarial machine learning in IoT: A survey., *IEEE Internet of Things Journal*., *8*(7), 5442-5459, 2021.
19. Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., Hong, C. S. Internet of Things forensics: Challenges and future trends., *Future Generation Computer Systems*, *92*, 395-411.
20. Zhang, Y., Deng, R. H., & Liu, J. K. Security and privacy in smart health: Efficient policy-hiding attribute-based access control., *IEEE Internet of Things Journal*., *5*(3), 2130-2145, 2018.