World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

# Fortifying IoT security: The transformative role of AI in cyber threat mitigation

Jayasudha Yedalla *

*Department of Computer Science- Cybersecurity and Information Assurance, Colorado Technical University, Doctorate, Colorado, USA*

World Journal of Advanced Engineering Technology and Sciences, 2025, 14(02), 049-057

Publication history: Received on 28 December 2024; revised on 07 February 2025; accepted on 10 February 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.14.2.0056

## Abstract

The Internet of Things is quickly expanding, linking everything from smart homes to abode machines. These are serious security risks, however, because hackers attack these devices with such attacks as data theft and malware. These threats are just a current example of traditional security methods not being able to stop. IoT is being protected with Artificial Intelligence (AI) by detecting threats, risk analysis, and automatic responses. This article details how AI aids IoT security, its linkage to the blockchain, and its challenges. AI has helped businesses and individuals to make IoT systems more secure and reliable in the digital world.

**Keywords:** Internet of Things (IoT); IoT Security; Artificial Intelligence (AI); Cybersecurity Threats; Blockchain Integration; Risk Analysis

## 1. Introduction

Thanks to IoT, life has become easier by connecting devices like smart home systems, healthcare equipment, and industrial machines. Yet, as more and more devices are connected, more security problems are being brought about. As IoT devices are so exposed and can be used for something as simple as stealing data or as damaging as shutting down systems or spreading malicious software, they are susceptible to being hacked. These are advanced threats; they are innovative, and traditional security has not been a great or even close match for how these attacks are executed. AI is helping solve this problem by detecting weird activities, predicting attacks, and quickly responding to cyber threats. This also can be used to work with blockchain to create more muscular and tamper-proof security systems. This article discusses the upcoming security threats in IoT, how AI will play a role in combatting cyber threats, and what AI is up against regarding some of the challenges it will have to overcome. It also explores the potential for protecting IoT devices using AI in the future. With AI, IoT becomes safer and less secure for all of us.

## 2. Overview of IoT Security Challenges

The Internet of Things (IoT) has created rapidly growing and substantial security issues. With billions of interconnected devices exchanging data, IoT systems become potential places for vulnerabilities. With more devices connected, such vulnerabilities are likely high, and cyber threats can take advantage of them. These devices are weakened by their small processing power, lack of set security protocols, and exposure to this evolved form of cyber threat: quantum computing attacks. Data privacy and encryption is one of the primary security concerns in IoT. IoT devices need encryption so that the data collected and transferred is sensitive and can be circumvented if any method doesn't work. Nonetheless, the growth of quantum computing may not be a good match for traditional cryptographic algorithms. In the quantum era, post-quantum cryptography (PQC) is needed to ensure secure communication on the Internet; it is crucial because the quantum computer has the power to break off the most widely used encryption methods, exposing the Internet of Things to large-scale cyber-attacks, as Mamatha et al. (2024) point out.

* Corresponding author: Jayasudha Yedalla

An essential second issue is that quantum threatens classical cybersecurity models. Traditional security approaches are losing their relevance to emerging cyber threats, especially those brought in by quantum computing, as Sokol (2023) points out. Lightweight cryptographic methods are used in the IoT networks, which are more susceptible to quantum-based decryption techniques. Aydeger et al. (2024) underline the importance of moving toward the use of post-quantum cryptographical means for the development of quantum-resilient IoT infrastructures.

Security protocols over the network also play an essential role in IoT security. In the article "Baseri et al." (2024), the authors explain that quantum-safe network protocols are needed to avoid security risks in the connected environment. Many IoT devices use legacy or insecure communication protocols, reducing the chance of service attacks. IoT security challenges in healthcare become even more critical in critical sectors such as healthcare. According to the work of SaberiKamarposhti et al. (2024), medical data cybersecurity resilience is of the utmost importance.

## 3. The Growing Threat Landscape in IoT Security

Internet of Things (IoT) devices have penetrated almost all industries, such as industrial automation, healthcare, smart homes, transportation, etc. But the rapid expansion it witnessed produced serious security problems for it, too. However, IoT devices often do not have enough computing power and fail to have inbuilt security, rendering them perfect targets of cybercriminals. With growing IoT networks, there is an increasing risk of cyber threats, and they must have strong security systems to protect sensitive data from being stolen and prevent large-scale attacks.

### 3.1. Increase in IoT Devices and Security Vulnerabilities

It is estimated that billions of connected devices are deployed globally, and the number of IoT devices keeps growing at an unprecedented rate. However, most of these are built without considering any security factor, and hence, they are highly vulnerable to cyber-attacks. The one major issue is weak authentication mechanisms, like default user names and pwd, that the attacks can easily use (Mamatha et al., 2024). IO devices are also commonly constrained in resource-limited environments that prevent them from employing strong encryption or complex security protocols (Sokol, 2023). IoT security is further complicated because quantum computing is emerging. Soon enough, traditional encryption schemes used in IoT networks will be obsolete as quantum computers become able to break the algorithms of trending cryptographic systems (Aydeger et al., 2024). This is a compelling motivation for post-quantum cryptographic (PQC) systems to provide a solution against future quantum-based attacks on IoT systems (Sood, 2024). Poorly secured network connections are another critical vulnerability of IoT. Many IoT devices communicate unprotected, broadcasting their sensitive data to the clear. These weaknesses can be exploited to control various IoT systems, derail them, steal confidential information, or even fail essential services (Baseri et al., 2024).

### 3.2. Common IoT Cyber Threats

Multiple forms of cyberattacks threaten IoT devices, causing severe damage to both individuals and their businesses, as well as critical infrastructure networks. The following threats represent the majority of IoT cyber security threats:

#### *3.2.1. Distributed Denial-of-Service (DDoS) Attacks*

When criminals execute DDoS attacks, they direct malicious traffic from a botnet network of stolen IoT devices toward their target systems to degrade the target services. The Mirai botnet attack is one of the most notorious cases in which botnet hijacking allowed perpetrators to control thousands of IoT devices and launch significant DDoS attacks (SaberiKamarposhti et al., 2024). Cyber weapons use unsecured IoT devices because these attacks demonstrate their risk factor as cyber weapons.

#### *3.2.2. Data Breaches*

IoT devices acquire substantial data containing privacy-sensitive material,, which they distribute to external receivers. Because IoT devices operate without adequate encryption and access security measures, unauthorized data interception and theft of valuable information occur (Khan et al., 2024). The exposed information in IoT networks results in monetary loss, identity theft, and regulatory non-compliance, mainly when the affected industry includes healthcare systems and finance operations.

#### *3.2.3. Botnet Infections*

Malware targets IoT devices to take over their control because many remain susceptible to these infections. A botnet is a system of hacked IoT devices that criminals use to execute cyberattacks, push DDoS assaults, circulate spam, and conduct cryptocurrency work (Acharya et al., 2025). Security protocols should be implemented because unprotected IoT devices can enter massive botnet operations without the owners' knowledge.

### *3.2.4. Ransomware Attacks*

Ransomware is malicious software that encrypts data through malware and requires payments for data recovery. In IoT networks, ransomware attackers specifically target intelligent infrastructure elements such as power grids, hospitals, and industrial control systems, which can ultimately stop vital operations (Kadve et al., 2025). Ransomware attackers enter IoT networks by taking advantage of software and firmware weaknesses to carry out their attacks.

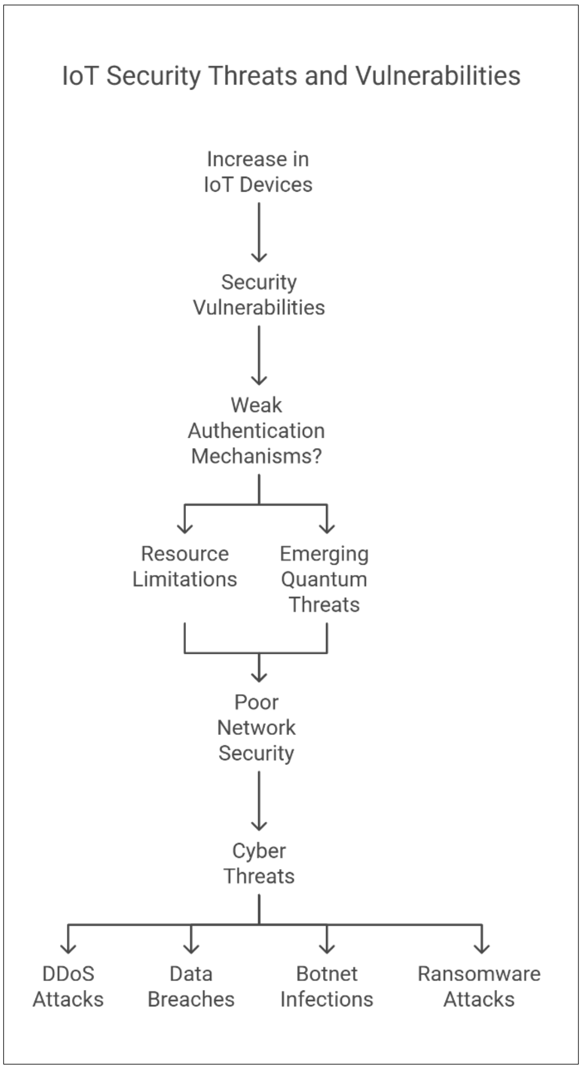

**Figure 1** IOT Security Threats and Vulnerabilities

## 4. The Role of AI in Enhancing IoT Security

With the rise of IoT devices, the number and complexity of these devices grow, and more excellent security mechanisms become more challenging to maintain about constantly changing cyber threats. Artificial intelligence (AI) has the power to disinfect IoT security of as many threats as possible, as it provides intelligent threat detection, anomaly identification, and proactively mitigating risk. Such AI-powered cybersecurity solutions can also analyze vast amounts of data with real-time speed, detect unusual municipalities, and perform tasks automatically to prevent security breaches.

### 4.1. AI-Powered Threat Detection and Response Mechanisms

The power of AI lies in its ability to detect threats with automation and very quickly on a timely basis and has a substantial impact on IoT security. Current security systems are based on pre-defined rules and signature detection methods, which are ineffective against new and innovative cyber threats. However, AI can detect emerging threats by analyzing behavioral patterns and anomaly detection of IoT networks (Mamatha et al., 2024). One of AI's most significant advantages is that it can take threat response off the hands of human intervention via automation. Instant isolation of compromised IoT devices, prevention of malware propagation, and the deduction of possible attacks (Sokol, 2023) can be done through AI-driven security systems. Take, for instance, the AI based intrusion detection systems (IDS), intrusion prevention systems (IPS) that are running in a continual loop to detect for any suspicious activities with the time factor and prevent it from getting out of hand (Aydeger et al., 2024).

### 4.2. Machine Learning for Anomaly Detection in IoT Networks

The most essential of IoT is identifying anomalies, which is performed using machine learning (ML). Because IoT devices produce vast data, traditional tools cannot scan all network activity by hand. Since machine learning algorithms can learn from historical data and define a normal device behavior baseline, they can easily detect deviations from normal that suggest potential cyber threats (Sood, 2024). Supervised ML algorithms can detect injection attempts, dispersed IPs, and MAC addresses, unusual network traffic patterns, authorization failures, changed device behaviors, and unauthorized access attempts (Baseri et al., 2024). They can also alert security teams to possible cyberattacks before they become out of control. Additionally, you can deploy machine learning at the edge for security solutions, preventing security threats directly on IoT devices in real-time without a cloud-based process. Then, IoT security becomes more efficient and has fewer latencies and response times (SaberiKamarposhti et al., 2024).

### 4.3. Predictive Analytics for Proactive Security Measures

IoT security can be enhanced through AI-driven predictive analytics that predicts possible threats before there will be any threat. AI can analyze historical cyber attack data and recognize patterns, learn, and expect, as hackers may exploit some information (Khan et al., 2024). Organizations can take proactive security measures, including patching vulnerabilities, strengthening authentication methods, and optimizing firewall rules. Another role of AI in threat intelligence is predicting future attacks based on multiple data sources like cyber threat databases, network logging system logs, and security reports (Acharya et al., 2025). For instance, if it combines AI with security platforms, then the latter can automatically suggest security configuration or even alert in advance about possible cyber threats that are just beginning to emerge.

### 4.4. AI and Blockchain Synergy for IoT Security

Combining Artificial Intelligence (AI) with blockchain technology is an effective solution for enhancing IoT security measures. AI and blockchain technologies boost IoT security through enhanced threat recognition abilities, anomaly identification techniques, and predictive safety functions. They achieve IoT system decentralization and complete accessibility and protect IoT data reliability. A combined approach of these technological solutions establishes a more substantial security infrastructure that blocks the weaknesses of central system management and active cyber assaults.

### 4.5. Decentralized Security Solutions with AI and Blockchain

Attacks on Internet of Things networks can occur because security solutions rely on server-based management of authentication, security policies, and data storage. As reported by Mamatha et al. (2024), the single-point failure characteristic of centralized architectural systems exposes them to significant cyber-attacks, such as Distributed Denial-of-Service (DDoS) attacks and unauthorized access. Blockchain technology decentralizes security operations, creating solutions to address the identified challenges. The distributed node organization of blockchain enables data storage as tamper-proof ledgers, which ensures the permanent security of IoT transactions (Sokol, 2023). Protecting IoT security becomes more effective when AI integrates with blockchain-based security systems. AI analyzes user behavior through automated access control systems, which blockchain implements to verify decentralized identities and grant legitimate users with device access (Aydeger et al., 2024). The blockchain supports smart contracts that implement automated security protocols to stop unauthorized alterations of IoT firmware and device setups (Sood, 2024). Authentication enhancement occurs through AI behavioral pattern analysis and blockchain secure record storage which stops identity fraud (Baseri et al., 2024).

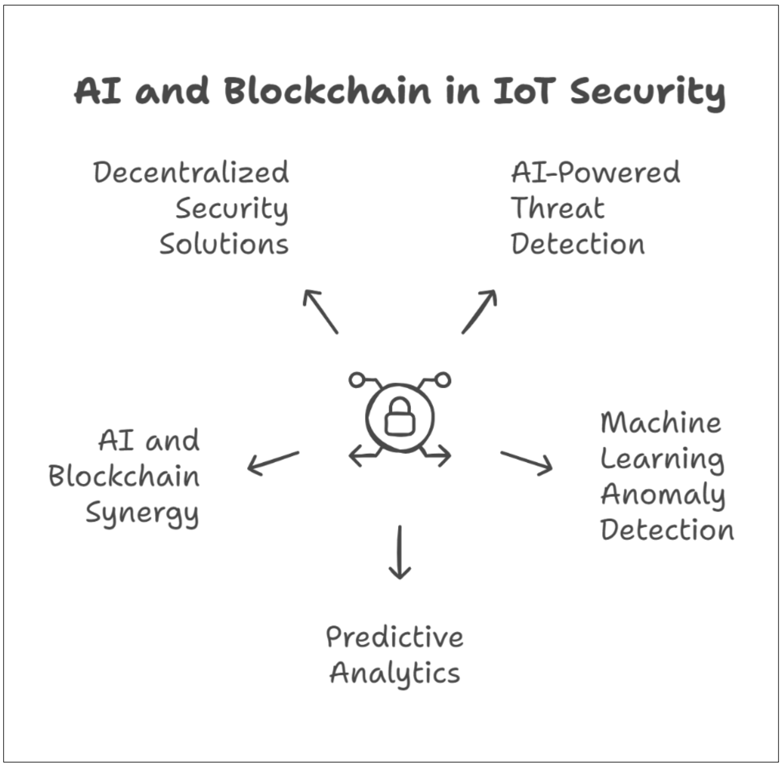
AI and Blockchain in IoT Security
Decentralized Security Solutions
AI-Powered Threat Detection
AI and Blockchain Synergy
Machine Learning Anomaly Detection
Predictive Analytics

**Figure 2** AI and Blockchain in IOT Security

## 5. Secure Data Transmission and Integrity Verification

The protection of data channels and the development of integrity standards remain the primary challenges for secure IoT management. The ease of data tampering, interception,, and corruption in specific environments leads IoT devices to produce severe industrial sabotage effects and false readings (SaberiKamarposhti et al., 2024). Every data record within the system finds permanent storage on blockchains while AI runs nonstop checks to identify irregularities in the data transfer process. These synergistic technologies generate enhanced cooperation that leads to: The blockchain system achieves high-security levels because it uses hash functions to encrypt IoT transmission lines, and AI continuously detects real-time data manipulation (Khan et al., 2024). Financial institutions use blockchain to maintain tamper-proof IoT data logs that create permanent incident records to satisfy cybersecurity demands (Acharya et al., 2025). AI software detects unusual data patterns automatically, triggering blockchain-based innovative contract security protocols that stop dangerous network traffic and separate threatening IoT devices (Kadve et al., 2025).

## 6. Challenges and Ethical Considerations in AI-Driven IoT Security

Modern IoT security has made essential strides because artificial intelligence technology was integrated into security operations to detect threats, detect anomalies, and execute automated responses. AI security systems generate new security concerns because they create bias problems while risking user privacy and requiring adherence to regulatory requirements. Most reliable and ethical cyber security in IoT environments depends on solving these existing problems.

### 6.1. AI Biases and False Positives in Threat Detection

IoT security systems that use AI drive their threat detection through machine learning algorithms. These security models develop biases through uneven training data,, which generates incorrect identifications of valid operations as threats and fails to detect real threats. AI systems create false positive errors by mistakenly identifying regular network patterns as threats. This leads to unneeded security alerts that produce active blockades of legitimate users, operational disruption, and over-triggered alerts (Mamatha et al., 2024). According to Sokol (2023), unexpected alerts from healthcare IoT systems may result in medical treatment delays or limitations on accessing critical patient information. AI security models allow attackers to bypass their security through modified attack patterns, leading to undetected cyber threats. According to Aydeger et al. (2024), AI detection methods for post-quantum security face significant challenges because they cannot handle the advanced quantum-powered cyber threats. The risks can be reduced through continual updates with wide-ranging training data while enhancing systems with human-operated supervision and explainable AI functions for improved decision-making clarity (Sood, 2024).

### 6.2. Privacy Concerns in AI-Driven IoT Security

The security method that uses AI with the Internet of Things depends on live analysis of data, but this practice leads to privacy-related concerns and unwanted surveillance activities. The nature of IoT devices' ability to gather sensitive user data makes these devices attractive targets,, resulting in increased data protection risks for users.

### 6.3. Regulatory and Compliance Challenges

All AI-powered security implementations for IoT devices need to meet international cybersecurity framework requirements and industry standards for data safety. However, the developing nature of regulations dedicated to AI makes it challenging for companies to achieve compliance. According to Mamatha et al. (2024), AI data processing under the General Data Protection Regulation (GDPR) must happen lawfully with user consent and use strong encryption. Organizations that fail to comply may face legal consequences and damage to their reputation. AI governance frameworks, and ethical regulations, come from governmental agencies and cybersecurity organizations to control applications carrying high risk, especially those based on AI cybersecurity models. The EU AI Act, and the NIST AI Risk Management Framework, outlines necessary procedures for securely deploying AI systems (Sokol, 2023). The future of IoT security demands post-quantum cryptographic measures to meet quantum-safe security criteria because quantum computing continues to develop (Aydeger et al., 2024; Kadve et al., 2025). Many organizations need to adopt quantum-resistant encryption methodologies to protect their Internet of Things security infrastructure against future threats.

## 7. Future Directions and Innovations in AI for IoT Security

In the realm of IoT ecosystems, the concept of AI in cybersecurity is changing to tackle the increasing IoT ecosystems and compliance challenges. Future deep learning, edge AI, and AI regulatory compliance will be key enablers in securing powerful IoT, like a key to a robust security framework and a viable cyber defense.

### 7.1. Advances in Deep Learning for Cybersecurity

AI has changed cybersecurity threat detection and response mechanisms with deep learning, a subset of AI. Deep learning algorithm analysis is different from traditional machine learning, and deep learning algorithms can analyze complex attack patterns and detect zero-day threats, among other things, in real time.

### 7.2. Edge AI and Its Impact on IoT Threat Mitigation

Standard IoT security framework is cloud-based, where the AI processing happens and introduces latency in bandwidth limitation and centralized vulnerabilities. Real-time threat detection and response are brought to the edge of IoT devices, and efficiency and security increase. Edge AI allows IoT devices to process the security data locally, thereby reducing the dependency on cloud servers. That way, attacks will be caught faster and faster before they get to the network (SaberiKamarposhti et al., 2024). Edge AI lowers latency in cybersecurity threat mitigation based on the fact that edge AI processes security analytics closer to the data source, which leads to immediate anomaly detection, along with faster response time to some critical IoT applications, for instance, smart cities, autonomous vehicles, and healthcare IoT (Khan et al., 2024). Edge AI – Privacy Enhancing AI: With Edge AI, data is not transmitted to the central servers from where an AI model is deployed to the edge devices. It lowers the probability of data breaches and unauthorized access, which affirms concerning privacy regulations such as GDPR (Acharya et al., 2025).

### 7.3. The Role of AI in Regulatory Compliance and Security Governance

With the intelligent, AI-driven IoT security solutions maturing, the bodies that are regulating are being responsible for AI ethics, accountability, and compliance. There is going to be a need for AI to automate the monitoring of compliance, provide transparency, and enforce cybersecurity regulations. Continuous IoT Security I Audits by AI: After preparing the logs of IoT security I by the means described above, AI can routinely audit them for compliance with regulations like GDPR, NIST,, and ISO 27001 (Kadve et al., 2025). This helps organizations find security gaps and avoid legal penalties. Transparent Security Decisions: Explainable AI (XAI) for the Higher Transparency of AI-Driven Security Decisions – Policy Request. XAI (explainable AI) frameworks will enable security teams to interpret AI-driven threat alerts and justify that (Khodaiemehr et al., 2023). AI development will address the detection of risks through the collection of counterintelligence activities, such as data breaches, employee manipulation through social engineering tactics, and data leaks from outsiders. Finally, these models will be in sync with what is coming down the pike regarding regulatory frameworks for quantum-safe security governance (Acharya et al., 2025).

## 8. Methodology

The research analyzes the impact of Artificial Intelligence (AI) on IoT security through a qualitative research method. The research methodology involves:

- The research conducts an extensive review of present-day scholarly works and journal articles and reports regarding IoT security issues and threat detection mechanisms based on AI systems and blockchain integration. The research uses peer-reviewed publications together with cybersecurity reports as its information sources. This part of the research analyzes the performance of AI-based security approaches against regular security methods through an evaluation of their capabilities against cyber threats.
- An analysis of AI implementation within IoT security consists of three components: exploration of intrusion detection systems (IDS) operated by AI and performance of predictive analytics while employing blockchain-based security models.
- A report summarizes security trends and threats by reviewing existing research studies related to post-quantum cryptography and AI-anomaly detection as well as secure multi-cloud infrastructure approaches. The research qualifies into three sections to understand how AI technology secures IoT systems while resolving existing weaknesses along with anticipating upcoming digital security challenges.

## 9. Discussion

Considering the growing sophistication of cyber threats against IoT networks, integrating Artificial Intelligence (AI) in IoT security has become a new necessity. Secure methods of the past, which involve written rules and signature detection, no longer proficiently address modern and dynamic attacks like data breaches, botnet infections, and ransoms. Security solutions based on AI drive up the protection of the IoT by detecting time threats in real-time, identifying anomalies, and doing predictive analytics to overcome the issues before they get out of control.

The first advantage of AI in IoT security is that it can analyze vast amounts of data and detect unusual behavior patterns. The difference between a conventional security system and AI is that the latter uses machine learning models to forge relations to the network behavior to spot deviations from such behavior. In particular, this proactive approach is very efficient in regards to detecting Distributed Denial-of-Service (DDoS) attacks and unauthorized access attempts. AI-based threat detection is, however, effective only to a great extent and depends on the quality and diversity of train data, largely seen in terms of false positives or missed threats for the too-biased datasets. Data privacy is another critical issue in IoT security. Data analysis on these security mechanisms is required to make it work, which means unscrupulous data collection and data breaches. Sensitive environments such as healthcare and financial sectors, which have stringent privacy regulations, are where most IoT devices operate. Consequently, robust encryption protocols and decentralized data management using blockchain technology can contribute to resolving the above concerns. The immutable storage of IoT records provided by blockchain reduces data integrity risks and also the risk of tampering. AI and blockchain can be combined to improve authentication processes and with smart contracts to do security response processes automatically.

However, it has some limitations, such as computational limitations, ethical considerations, and regulatory compliance. Most IoT devices have limited processing power, which prevents using resource-intensive AI models. Additionally, the privacy and accountability of AI decision-making are important issues that we must address. The XAI technique can assist security teams in understanding AI-based threat assessments and minimizing the risk of misinterpretation. The threat landscape in IoT security is growing rapidly, making it urgent to develop AI-driven solutions that work only if there are continuous advancements in AI algorithms, blockchain integration, and post-quantum cryptographic measures. Future work should be directed towards developing lightweight AI models for IoT devices that are AI ethical and also offer a suitable level of security, following globally established security guidelines.

## 10. Conclusion

The rapid expansion of the IoT brings relevant security challenges, which do not lend themselves to the best of traditional cybersecurity mechanisms. The increased use of AI technology has emerged as a very powerful source of help for IoT security, which means that it can do real-time threat detection, anomaly identification, and predictive analytics. Parts of these activities become more efficient, some of which use machine learning models to detect and mitigate unauthorized activities, prevent data breaches, and reduce the risk of escalation before it actually occurs. However, although AI-based IoT security has several benefits, it also has a few limitations, such as privacy, computational complexity, and bias in threat detection processes. Integrating blockchain technology with AI offers a promising perspective since it can be used to provide data integrity, decentralize safety operations, and automate safety protocols through smart contracts. Also, quantum computing is getting stronger, strengthening how post-quantum cryptographic practices may protect IoT networks from future threats. Future research should aim to develop lightweight AI for resource-constrained devices, improve explainable AI (XAI) for decision-making transparency, and achieve long-term security of IoT systems regulatory frameworks for ethical AI deployment. A more comprehensive understanding of these challenges can help AI further contribute to the security of IoT ecosystems, thereby making the Internet of Things safer and more resistant to cyberattacks.

## Compliance with ethical standards

### *Acknowledgments*

Finally, this research was made possible due to the contributions of different authors and researchers from the studies through which they found their way towards IoT security, artificial intelligence, and blockchain integration. It should be noted that the work of Mamatha et al. (2024), Sokol (2023), Aydeger et al. (2024), Baseri et al. (2024), SaberiKamarposhti et al. (2024), Khan et al. (2024), Acharya et al. (2025), and Kadve et al. (2025) have played an essential role in shaping this work through their findings and discussions. Finally, we would like to acknowledge the cyber security and AI research community for their continuous efforts in generating new tools and solutions for cyber security in IoT networks. Their work still defines the future of secure, intelligent, connected systems.

### *Disclosure of conflict of interest*

No conflict of interest to be disclosed.

## References

[1] Mamatha, G. S., Dimri, N., & Sinha, R. (2024). Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era. arXiv preprint. DOI: 10.48550/arXiv.2403.11741

[2] Sokol, S. (2023). Navigating the Quantum Threat Landscape: Addressing Classical Cybersecurity Challenges. Journal of Quantum Information Science. DOI: 10.4236/jqis.2023.134007

[3] Aydeger, A., Zeydan, E., Yadav, A. K., & others (2024). Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography. IEEE Xplore. DOI: 10.1109/NoF60050.2024.10311741

[4] Sood, N. (2024). Cryptography in the Post Quantum Computing Era. SSRN. DOI: 10.2139/ssrn.4705470

[5] Baseri, Y., Chouhan, V., & Hafid, A. (2024). Navigating Quantum Security Risks in Networked Environments: A Comprehensive Study of Quantum-Safe Network Protocols. Computers & Security, Elsevier. DOI: 10.1016/j.cose.2024.10311741

[6] SaberiKamarposhti, M., Ng, K. W., Chua, F. F., Abdullah, J., & others (2024). Post-Quantum Healthcare: A Roadmap for Cybersecurity Resilience in Medical Data. Heliyon, Cell Press. DOI: 10.1016/j.heliyon.2024.e10311741

[7] Khan, M. A., Javaid, S., Mohsan, S. A. H., & others (2024). Future-Proofing Security for UAVs With Post-Quantum Cryptography: A Review. IEEE Open Journal. DOI: 10.1109/OJCOMS.2024.10311741

[8] Acharya, K., Gandhi, S., & Dalal, P. (2025). Cyber-Security of IoT in Post-Quantum World: Challenges, State of the Art, and Direction for Future Research. IGI Global. DOI: 10.4018/978-1-6684-8011-9.ch10311741

[9] Kadve, D. B., Kumar, B., & Prasad, S. B. (2025). Quantum Cryptography and Its Implications for Future Cyber Security Trends. IGI Global. DOI: 10.4018/978-1-6684-8011-9.ch10311741

[10] Khodaiemehr, H., Bagheri, K., & Feng, C. (2023). Navigating the Quantum Computing Threat Landscape for Blockchains: A Comprehensive Survey. TechRxiv. DOI: 10.36227/techrxiv.10311741.v1

[11] Langeh, A., & Sudhakar, R. (2023). Artificial Intelligence and Cyber Security: Transformative Synergies in the Digital Frontier.

[12] Karyemsetty, N., Narasimha, P. B., et al. (2023). Cybersecurity Fortification in Edge Computing through the Synergy of Deep Learning. IEEE Xplore.

[13] Adewusi, A. O., Chiekezie, N. R., & Eyo-Udo, N. L. (2022). The Role of AI in Enhancing Cybersecurity for Smart Farms. World Journal of Advanced Research.

[14] Reddy, A. R. P. (2021). The Role of Artificial Intelligence in Proactive Cyber Threat Detection in Cloud Environments. NeuroQuantology.

[15] Bolanos, J. (2023). A Holistic Framework for AI-Driven Cyber Risk Management in IoT Ecosystems. SSRN. Bellapukonda, P., Vijaya, G., & Subramaniam, S. (2024). Security and Optimization in IoT Networks Using AI-Powered Digital Twins. IGI Global.

[16] Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. ResearchGate.

[17] Yogi, M. K., Aiswarya, D., & Mundru, Y. (2023). Security for AI and IoT Convergence: Novel Perspectives. International Journal of Scientific Research in Network Security and Communication.

[18] Humayun, M., Tariq, N., Alfayad, M., & Zakwan, M. (2024). Securing the Internet of Things in the Artificial Intelligence Era: A Comprehensive Survey. IEEE Xplore.

[19] Chilongo, L., & KM, A. S. (2024). Impact of Artificial Intelligence on Cybersecurity: A Case of Internet of Things. Digital Forensics & Cyber Security.