AI-POWERED SECURITY IN THE WORLD OF IOT AND QUANTUM TECHNOLOGIES

Mohammed Maaz Mohammed Niyaz
Shri Shivaji college of Arts, Commerce and Science Akola
mohammadmaaz8262@gmail.com

Mayuri R. Gudade
Shri Shivaji college of Arts, Commerce and science, Akola
mayuri.gudade@gmail.com

Abstract

The rapid growth of the Internet of Things (IoT) has introduced significant cybersecurity challenges due to heterogeneous, resource-constrained, and large-scale networks. Traditional security mechanisms are inadequate to address modern threats, motivating the development of AI and Deep Learning-based Intrusion Detection Systems (IDS) for effective anomaly detection. In Industry 5.0 environments, Explainable AI (XAI) enhances transparency and trust in security decisions, while quantum computing threatens classical cryptographic protocols. Consequently, in this paper we explore post-quantum cryptography, lightweight encryption algorithms, blockchain-based frameworks, and Quantum Machine Learning (QML) to enhance resilience and privacy in IoT networks. Integrating these innovative approaches offers a comprehensive security framework capable of effectively mitigating both classical and quantum-era cyber-attacks, ensuring reliable protection for critical infrastructures.

Keywords: *Internet of Things (IoT), Artificial Intelligence (AI), Deep Learning (DL), Quantum Computing, Blockchain, Quantum Machine Learning (QML), Cybersecurity.*

Introduction

The Internet of Things (IoT) is expanding rapidly, connecting billions of smart devices in homes, industries, healthcare, and transportation. While this connectivity enables automation, efficiency, and innovation, it also increases the attack surface. Because IoT devices are heterogeneous (different hardware/software), resource-constrained (low power, limited storage), and highly scalable (millions of devices), traditional security approaches (like simple firewalls or classical encryption) are not enough to stop modern cyber threats.

To address this, Artificial Intelligence (AI) and Deep Learning (DL) are being used for Intrusion Detection Systems (IDS) and anomaly detection in IoT networks [1]. However, in Industry 5.0 environments, where humans and machines collaborate, Explainable AI (XAI) is important to provide transparent and interpretable security decisions. Without explainability, AI models work like a “black box,” reducing trust [2].

Meanwhile, quantum computing poses another critical challenge. Classical cryptography (RSA, ECC) is vulnerable to quantum algorithms such as Shor’s algorithm, which can break them in polynomial time. Hence, researchers are building quantum risk assessment tools [3] and exploring AI + blockchain–based frameworks with quantum-resistant algorithms to enhance privacy and resilience in IoT [4].

In critical sectors like smart grids, where massive data exchanges occur, hybrid encryption models combining classical and post-quantum cryptography are used to maintain security against both classical and quantum attacks [5]. For specialized cases such as vehicular IoT, lightweight ciphers like Post-Quantum Enhanced Ascon are designed for high performance and strong resilience [6].

On the AI side, Quantum Machine Learning (QML) is emerging as a powerful tool that leverages quantum computing to improve cybersecurity tasks such as intrusion detection [7].

For cryptographic solutions, lattice-based post-quantum schemes (like identity-based signatures) provide authentication and secure communication in IoT networks [8]. To make IDS models efficient, research also emphasizes feature selection and data balancing to optimize deep learning models for IoT traffic [9]. Finally, surveys highlight that the future of IoT security requires complete adoption of post-quantum cryptography standards [10].

Thus, the convergence of AI, post-quantum cryptography, lightweight algorithms, and blockchain forms the next-generation IoT security framework, capable of resisting both classical and quantum-era threats.

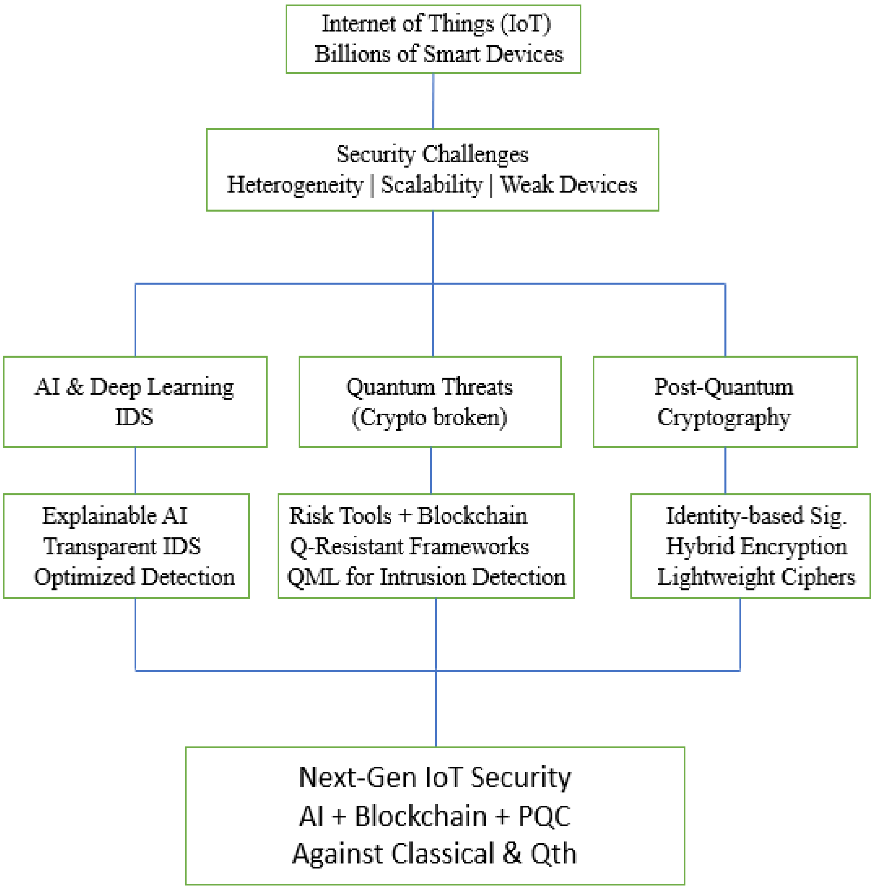

Fig 1: Future IoT Security Framework

Literature survey:

Alaa Mohammed Banaamah et al. (2022) investigate intrusion detection techniques based on deep learning, assessing the performance of various models and determining the most effective approach for detecting intrusions in IoT environments. Their study utilizes deep learning architectures such as Convolutional Neural Networks (CNNs), Extended Short-Term Memory (ESTM), and Gated Recurrent Units (GRUs). The evaluation was carried out using a benchmark IoT intrusion detection dataset. The experimental findings were compared with existing methods, demonstrating that the proposed approach delivers superior accuracy compared to current intrusion detection techniques [1].

Naseem Khan et al. (2024) explore human–AI collaboration in manufacturing environments that incorporate robots, IoT devices, AR/VR, and other advanced technologies, emphasizing security risks in key sectors such as healthcare, defence, and the economy. While AI has proven effective in identifying intrusions, malware, and phishing attempts, concerns over the opaque nature of black-box machine learning models have led to growing interest in Explainable AI (XAI). Their work surveys XAI-driven intrusion detection systems within the context of Industry 5.0, underlining the need for transparency, the role of adversarial methods, and future research opportunities in high-stakes cybersecurity applications [2].

Basel Halak et al. (2024) introduced a quantum readiness assessment tool designed to help organizations adapt their security protocols for the post-quantum era. To implement this, they developed a comprehensive web application with an integrated database and hosting infrastructure. The tool uses a risk assessment formula to analyse organizational vulnerabilities based on survey responses, generating recommendations informed by extensive research on existing systems and encryption methods. Furthermore, the solution was systematically evaluated through qualitative feedback from cybersecurity experts and network administrators, which was used to enhance its precision and usability. Findings confirm the tool’s practicality and effectiveness in supporting organizations to prepare for quantum-related security challenges [3].

Mahmoud Elkhodr et al. (2025) propose the Integrated Adaptive Security Framework for IoT

(IASF-IoT), which combines artificial intelligence, blockchain, and quantum-resistant cryptography to deliver a unified security approach for IoT ecosystems. The framework features an adaptive AI-based security orchestration system, blockchain-enabled identity management, lightweight quantum-resistant protocols, and Digital Twins to predict and mitigate potential risks. Its effectiveness was evaluated through a theoretical model and large-scale simulations involving 1,000 diverse IoT devices. The findings revealed detection rates ranging from 85% to 99%, energy consumption below 1.5 mAh per day, and average response times of approximately 2 seconds, demonstrating its scalability, efficiency, and suitability for resource-constrained IoT environments [4].

Jian Xiong et al. (2025) suggest Quantum-Resistant Hybrid Encryption for IoT (QRHE-IoT), a novel technique designed to improve communication security within IoT-based smart grids. This system combines symmetric and asymmetric encryption methods with quantum-resistant algorithms to deliver strong protection. The research outlines its underlying mechanism, theoretical basis, and ability to address security challenges in smart grid communications. Simulation tests in a smart grid environment validated its performance, showing that QRHE-IoT offers a dependable defence against evolving threats, particularly those arising from quantum computing [5].

Bhuvaneshwari A. J. et al. (2025) introduce a post-quantum cryptography (PQC)–based security method that enhances Ascon encryption through a quantum-resistant key exchange. The answer ensures secure verification while protecting in contradiction of replay, Sybil, collision, phishing, and man-in-the-middle outbreaks. To ensure data integrity, it merges a 32-bit Ascon hash by SHA-512. Experiments in resource-limited vehicular environments show superior results, generating 128–512-bit keys within microseconds—much faster than Kyber and Falcon. It also surpasses standard Ascon in hash processing, completing a 256 × 256 grayscale image in just 0.0782s compared to 0.822s. These findings confirm the method’s ability to provide secure, low-latency communication for vehicles, making it highly effective in protecting future connected and autonomous vehicles against quantum-era cyber threats [6].

Armando Bellante et al. (2025) examine the potential role of Quantum Machine Learning (QML) in advancing cybersecurity applications that currently rely on traditional ML. The study first highlights the possible benefits quantum computing can bring to machine learning tasks in cybersecurity. It then outlines a methodology for assessing the long-term impact of fault-tolerant QML algorithms on real-world problems. As a practical case study, the approach is applied to common methods and datasets used in network intrusion detection, a key area of ML-based cybersecurity research. The findings offer valuable insights into the conditions required to achieve quantum advantage, while also emphasizing the necessity of future developments in quantum hardware and software [7].

Yang Zhang et al. (2024) current a comprehensive safety model for IoT network applications that join in blockchain with a post-quantum safe identity-based signature (PQ-IDS) structure. The model constructions IoT networks into three coatings—perceptual, network, and application—ensuring both data security and user privacy throughout the data-sharing process. The PQ-IDS scheme leverages lattice-based cryptography, where the bimodal Gaussian distribution and discrete Gaussian sampling algorithm are used to formulate the core hard problem underlying the lattice assumption. This design provides resilience against quantum attacks during IoT device communication. Additionally, the identity-linked signature mechanism ensures non-repudiation of signed information. Authorized safety study approves that PQ-IDS reaches unforgeability, non-repudiation, and non-transferability. Relative efficiency and performance valuations additional validate its practicality and efficiency in IoT network atmospheres [8].

S. Kumar Reddy Mallidi et al. (2025) present a systematic review designed to direct future research by examining six key research questions central to the advancement of intrusion detection systems (IDS) for IoT environments. The study emphasizes the role of Machine Learning (ML) and Deep Learning (DL) in strengthening IDS performance. It further investigates feature selection methods aimed at creating lightweight IDS solutions that maintain both efficiency and effectiveness in IoT contexts. The review also evaluates diverse datasets and data balancing techniques, which are essential for training IDS models with accuracy and reliability. By thoroughly analysing prior research, the study uncovers major trends, identifies existing gaps, and proposes directions for future work to refine IDS frameworks suited to the rapidly evolving IoT ecosystem [9].

Adarsh Kumar et al. (2025). This paper proposals a broad literature study of post-quantum cryptography for IoT networks, with the challenges and research guidelines to adopt in real-time applications. The work draws focus towards post-quantum cryptosystems that are useful for resource-constrained devices. Further, the paper surveys quantum attacks that may occur over traditional and lightweight cryptographic primitives.[10]

Research work:

Deep learning-based intrusion detection methods for IoT have shown superior accuracy with CNN, LSTM, and GRU models [1]. Human–AI collaboration in Industry 5.0 highlights security risks and promotes Explainable AI (XAI) for intrusion detection [2]. A quantum risk assessment tool was developed to aid post-quantum security transition [3], while the Integrated Adaptive Security Framework for IoT (IASF-IoT) achieved high detection accuracy with low resource use [4]. Quantum-Resistant Hybrid Encryption (QRHE-IoT) for smart grids proved robust against quantum attacks [5], and Ascon encryption was enhanced with quantum-proof key exchange for secure vehicular communication [6]. Quantum Machine Learning (QML) has been investigated for cybersecurity, stressing hardware and software advancements for quantum advantage [7]. A blockchain-based post-quantum identity signature model was proposed, ensuring unforgeability and efficiency in IoT [8]. IoT intrusion detection reviews identified gaps in feature selection and dataset balancing [9], while post-quantum cryptography analysis revealed challenges and opportunities for resource-constrained IoT [10].

Conclusion:

The rapid expansion of IoT has enhanced industries, healthcare, and smart systems but also raised major cybersecurity risks due to device diversity and limited resources. Traditional methods are insufficient, making AI and Deep Learning-based IDS crucial for anomaly detection. In Industry 5.0, Explainable AI builds trust by clarifying security decisions, while quantum computing challenges existing cryptography, driving research into post-quantum cryptography, lightweight algorithms, and blockchain-based frameworks. Overall, future IoT security depends on integrating AI, XAI, blockchain, and quantum-resilient solutions to protect critical infrastructures.

Reference:

1. Alshamrani, S., & Alenezi, F. (2022). Intrusion detection in IoT using deep learning. Sensors, 22(19), 7468.
2. Elhabshy, A. A., Sallam, M. A., Younis, M., & Zomaya, A. Y. (2024). Explainable AI-based intrusion detection system for Industry 5.0: An overview of the literature, associated challenges, existing solutions, and potential research direction. Expert Systems with Applications, 242, 122825.
3. Halak, B., Ali, S., & Alenezi, F. (2024). A security assessment tool for quantum threat analysis.
4. Alshahrani, H., & Alshamrani, S. (2025). An AI-driven framework for integrated security and privacy in Internet of Things using quantum-resistant blockchain. Future Internet, 17(2), 45.
5. Guo, Y., Zhou, X., & Chen, H. (2024). Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. Scientific Reports, 14(1), 12185.
6. Singh, A., & Sharma, V. (2025). OPEN post-quantum enhanced Ascon for secure vehicular IoT data integrity. Scientific Reports, 15(1), 2234.
7. Kumar, R., & Gupta, S. (2025). Evaluating the potential of quantum machine learning in cybersecurity: A case-study on PCA-based intrusion detection systems. Computers & Security, 136, 103567.
8. Zhang, Y., & Wang, L. (2024). Post-quantum secure identity-based signature scheme with lattice assumption for Internet of Things networks. Sensors, 24(13), 4188.
9. Rahman, M. M., & Hossain, M. S. (2025). Optimizing intrusion detection for IoT: A systematic review of machine learning and deep learning approaches with feature selection and data balancing. WIREs Data Mining and Knowledge Discovery, 15(2), e1643.
10. Ali, I., & Hussain, M. (2022). Securing the future Internet of Things with post-quantum cryptography: A survey. IET Information Security, 16(6), 551–566.