Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 9, September : 2024

A Review of Industrial IoT Security Based on Quantum-Enhanced Cryptographic Protocols

Dr. Vikas Nandgaonkar
Department of Computer Engineering
Indira College of Engineering and Management
Pune, Maharashtra India
vikas.nandgaonkar@gmail.com

Dr. Soumitra Das
Department of Computer Engineering
Indira College of Engineering and Management
Pune, Maharashtra India.
soumitra_das@yahoo.com

Dr. Sunil Rathod
Department of Computer Engineering
Indira College of Engineering and Management
Pune, Maharashtra India

ABSTRACT

The rapid advancement of quantum computing poses a major threat to traditional cryptographic methods used in Industrial Internet of Things (IIoT) systems. Classical encryption algorithms such as RSA, ECC, and DSA are expected to become ineffective due to quantum algorithms like Shor's and Grover's. This review paper presents a comprehensive analysis of the shift toward Post-Quantum Cryptography (PQC) in IIoT environments, emphasizing the need for quantum-resistant security techniques to protect critical infrastructure. It evaluates various PQC algorithms—lattice-based (Kyber), hash-based (SPHINCS+), code-based (Classic McEliece, BIKE), and multivariate schemes—based on their suitability for resource-constrained IIoT devices. The study highlights the significance of hybrid cryptographic models combining classical and quantum-safe methods to provide layered protection during transition phases. It also discusses global standardization efforts by agencies like NIST and the role of lightweight cryptographic hardware, such as FPGA and ASIC, for practical deployment. Furthermore, it explores emerging technologies like Quantum Key Distribution (QKD), Quantum Machine Learning (QML), and blockchain-integrated PQC for enhanced security, anomaly detection, and decentralized identity management. The paper identifies key challenges in scalability, key management, and real-world deployment, and proposes a strategic roadmap to secure IIoT systems in the quantum era. The adoption of PQC and hybrid architectures is vital for ensuring future-proof cybersecurity, operational continuity, and data integrity in industrial applications.

Keywords— Industrial Internet of Things (IIoT); Post-Quantum Cryptography (PQC); Quantum Computing; Critical Infrastructure Security; Hybrid Cryptographic Architecture; SPHINCS+; Kyber; Secure Communication; NIST Standards; Quantum Threat Mitigation.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 9, September : 2024

• INTRODUCTION

1. Overview of IIoT

The Industrial Internet of Things (IIoT) refers to the integration of smart sensors, actuators, and connected devices into industrial environments to enhance operational efficiency, productivity, and decision-making. Also known as the Industrial Internet, IIoT enables seamless data collection, real-time analytics, and automation across various sectors such as manufacturing, energy, oil and gas, utilities, and agriculture [2], [3]. Unlike traditional machines that operated in isolation, IIoT devices are interconnected and capable of communicating vital information, enabling businesses to identify inefficiencies, predict failures, and optimize operations.

An IIoT ecosystem typically consists of intelligent devices that sense and transmit data, communication infrastructures for data exchange, cloud or on-premise storage systems, and analytics platforms that transform raw data into actionable insights [3]. The primary distinction between IoT and IIoT lies in their application domains—while IoT is more consumer-centric (e.g., smart homes and wearable devices), IIoT focuses on mission-critical industrial systems where failure can lead to significant financial or safety risks [2].

Numerous industries have adopted IIoT technologies. For instance, the automotive industry leverages IIoT for robotic automation and predictive maintenance, while the agriculture sector utilizes sensors to monitor soil health and crop conditions. Similarly, oil and gas companies employ drones and thermal imaging to detect pipeline anomalies, and utilities use IIoT for remote equipment monitoring and smart metering [3]. The benefits of IIoT include predictive maintenance, efficient field service management, asset tracking, enhanced customer satisfaction, and improved facility management through real-time condition monitoring.

However, with increasing connectivity comes a heightened concern for security risks. Many IIoT devices still operate with default credentials or transmit data in plaintext, making them vulnerable to cyberattacks [4], [8]. Effective IIoT security requires robust measures such as end-to-end encryption, multifactor authentication, and device-level identity management. Recognizing these challenges, initiatives like the Industrial Internet Consortium (IIC) have been formed to drive secure adoption and standardization of IIoT technologies [2].

2. Importance of security in critical infrastructure

The security of critical infrastructure is of paramount importance in today's hyper-connected industrial landscape [4], [9]. Critical infrastructure encompasses essential systems such as power grids, water supply, transportation networks, manufacturing plants, oil and gas pipelines, and communication systems. As these infrastructures increasingly adopt IIoT technologies, they simultaneously become more vulnerable to cyber threats [3], [4]. A breach in such systems could result in service disruption, financial loss, or even national security risks.

The integration of IIoT devices introduces new attack surfaces, especially as legacy systems often lack adequate cybersecurity measures. Threat actors—including cybercriminals and state-sponsored entities—can exploit these vulnerabilities [8]. Moreover, with the advancement of quantum computing, traditional cryptographic mechanisms like RSA and ECC are becoming increasingly inadequate [1], [5]. There is growing urgency to adopt quantum-resistant cryptographic solutions to ensure that critical infrastructure remains resilient against quantum threats [3], [5].

3. Emerging threat of quantum computing

Quantum computing presents a significant threat to conventional cybersecurity frameworks, especially those used in IIoT systems [1], [9]. Quantum computers utilize principles like superposition and entanglement to solve problems exponentially faster than classical computers. Algorithms like Shor's Algorithm can break RSA and ECC, compromising encryption-based systems [1]. For IIoT systems deployed in critical environments, this is especially concerning. These systems depend on encryption and secure authentication; which quantum computers could render obsolete. Furthermore, intercepted data today may be decrypted in the future using quantum technology—a concept known as "harvest now, decrypt later" [5], [9]. Therefore, there is an immediate need to transition toward quantum-resistant cryptographic protocols like PQC [3], [5].

4. Need for transition from classical cryptography to PQC

With quantum capabilities threatening classical algorithms such as RSA, ECC, and DSA, organizations must adopt Post-Quantum Cryptography (PQC) to secure long-term industrial communications [1], [5], [9]. PQC algorithms—such as lattice-based (Kyber), hash-based (SPHINCS+), code-based (BIKE), and multivariate cryptography—are designed to resist both classical and quantum attacks [5], [15]. Authors like Ahmad et al. [3] and Bavdekar et al. [5] advocate hybrid models that combine classical and post-quantum schemes during this transition phase. Kumar and Pattnaik [20] emphasize adopting quantum-safe communication frameworks aligned with evolving NIST standards. Hence, transitioning to PQC is a strategic necessity for ensuring IIoT security and resilience in the quantum computing era.

• OBJECTIVE OF PAPER

This paper aims to review the growing need for quantum-enhanced security protocols in Industrial Internet of Things (IIoT) systems, focusing on the vulnerabilities of classical cryptography and the adoption of Post-Quantum Cryptography (PQC). It examines various PQC algorithms (lattice-based, hash-based, code-based, multivariate) and their suitability for resource-constrained IIoT devices. The study also highlights the importance of hybrid cryptographic models, industry standards (e.g., NIST), and identifies research gaps and future directions. The goal is to provide a practical, scalable, and future-proof security framework for IIoT systems.

• LITERATURE SURVEY

The exploration of quantum-enhanced security mechanisms in digital systems has become a significant focus for researchers in response to the increasing threat posed by quantum computing. The foundational study by El Zouka and Hosni [1] presented early insights into the potential risks quantum computing poses to classical cryptographic systems such as RSA and ECC. Their work highlights how quantum algorithms could disrupt the reliability of traditional encryption, establishing a theoretical foundation for post-quantum security research. Building on this, Fernández-Caramés et al. [2] provided an extensive survey on Post-Quantum Cryptography (PQC) methods applicable to Internet of Things (IoT) systems. Their paper emphasizes the suitability of lightweight cryptographic models, tailored for resource-constrained IIoT devices, and suggests the need for robust cryptographic standards to protect sensitive industrial systems.

Furthering this perspective, Ahmad et al. [3] proposed a novel architectural framework that integrates quantum computing components with hybrid cryptographic protocols for

improving Industrial IoT (IIoT) security. Their work demonstrates real-world applicability of quantum security concepts in complex industrial systems and outlines practical pathways for their deployment. As secure transmission became a pressing concern, Sivakumaran et al. [4] introduced a quantum-based secure and lightweight transmission protocol using Quantum Key Distribution (QKD). Their solution offers resilience against eavesdropping and attacker manipulation in IoT communication networks, showcasing how quantum features can ensure low-latency, high-integrity transmissions. A broader analytical lens was applied by Bavdekar et al. [5], who conducted a detailed review of PQC algorithms including lattice-based, code-based, hash-based, and multivariate cryptography, while also discussing the NIST PQC standardization initiative. Their comparative analysis provides essential guidance for selecting appropriate algorithms for specific IIoT use cases.

The performance optimization of PQC algorithms was addressed by Imran et al. [6], who focused on designing high-speed cryptographic algorithms using techniques like optimized hashing and multiplication. Their research shows that hardware acceleration techniques such as efficient ASIC implementations can significantly reduce computational overhead in IIoT environments.

In the realm of privacy-preserving protocols, Mohanty et al. [7] presented a Quantum Secure Threshold Private Set Intersection (TPSI) mechanism tailored for IoT-enabled ride-sharing systems. This protocol demonstrates how quantum-secure methods can protect personal data while ensuring functional integrity in dynamic, multi-user environments. They simulated IoT data transactions that could map to cloud-hosted NoSQL stores or time-series databases. Expanding upon device-level security, Khan et al. [8] introduced Soteria, a Quantum Physical Unclonable Function (QPUF)-based remote attestation protocol. Their technique leverages quantum superposition and parallel memory validation to detect firmware tampering and provide a low-complexity, high-security framework for IIoT systems. Further emphasizing quantum threat mitigation, Tiwari et al. [9] conducted a comprehensive investigation into quantum computing's impact on data security and reviewed various PQC schemes, advocating the adoption of adaptive and future-ready cryptographic infrastructures.

Focusing on implementation aspects, Bellizia et al. [10] analyzed the hardware design challenges in PQC, such as silicon area, power consumption, and resistance to side-channel attacks. Their work highlights how secure hardware design must co-evolve with PQC development to ensure seamless integration in IIoT devices. In a more applied context, Rahman and Haider [11] proposed a Quantum-IoT (QIoT) Security Maintenance Model, integrating multi-level trust architecture and decentralized key exchange mechanisms. Their model provides a robust structure for managing trust in a distributed quantum-safe industrial system. Ali et al. [12] delved into the fundamentals of quantum cryptography, simplifying the theoretical basis of quantum operations such as entanglement and superposition, while explaining their impact on existing cryptographic protocols. In addition, Singh et al. [13] proposed an encoding-decoding mechanism for IoT data using quantum bits, suggesting improvements in data confidentiality and processing speed over conventional transmission methods.

Emerging technologies like Quantum Machine Learning (QML) were explored by Bandi et al. [14], who demonstrated how QML techniques can be used for real-time security data analysis, anomaly detection, and threat forecasting in industrial environments. Further strengthening the landscape, Kumar et al. [15] provided an overview of the theoretical underpinnings and practical challenges of PQC, highlighting bottlenecks in algorithm scalability, and calling for standardization across industry sectors. In the space of quantum-authenticated IoT protocols, Sikdar et al. [16] emphasized decentralized authentication

mechanisms that leverage quantum channels for secure device identity verification in large-scale IIoT deployments. Complementarily, Aman et al. [17] discussed the benefits of quantum-enhanced remote attestation mechanisms, emphasizing the energy efficiency and security advantages over classical cryptographic attestation models. Chaudhary et al. [18] contributed by integrating quantum signatures in secure data aggregation protocols, particularly suitable for high-volume IIoT sensor networks. As systems evolve, Kumari et al. [19] examined cryptographic migration strategies, highlighting challenges and approaches to replace traditional algorithms with PQC in live IIoT infrastructure without service disruption. Finally, Kumar and Pattnaik [20] provided a strategic review of quantum-safe approaches such as QKD and PQC, proposing a holistic roadmap for future-proofing industrial data systems. In [21] S. Gouram et al. claimed that the IIoT frameworks using low-power controllers and environmental sensors have improved maintenance and monitoring of smart street lights, reducing manual intervention and extending system longevity. In IIoT-based fruit ripening and grading systems, D. K. J. B. Saini et al. [22] used connected sensors such as gas detectors integrated with Arduino and NodeMCU enables real-time monitoring of fruit quality.

In most cases, studies focused on encryption techniques and transmission protocols, not on backend storage architecture. However, in a practical IIoT setup, data from sensors and PQC-encrypted payloads would typically be stored and managed in real-time databases like: InfluxDB or TimescaleDB (for time-series sensor data), PostgreSQL or MongoDB (for general relational/non-relational data), Ledger-based or Blockchain-based stores (for secure attestation and device logs).

- **COMPARATIVE ANALYSIS OF PQC ALGORITHMS**

In order to evaluate the feasibility of implementing Post-Quantum Cryptographic algorithms in Industrial Internet of Things (IIoT) environments, a comparative analysis of the most relevant algorithms is presented. The analysis considers algorithm type, key and signature size, encryption/decryption speed, and suitability for resource-constrained IIoT devices.

Table 1: Comparison of PQC Algorithms in IIoT Environments

PQC Algorithm	Type	Key Size (Bytes)	Signature Size (Bytes)	Encryption Speed	Decryption Speed	Suitability for IIoT
Kyber	Lattice-based	1568	N/A	High	High	Excellent
SPHINCS+	Hash-based	64	7856	Low	Low	Moderate
Classic McEliece	Code-based	261120	N/A	Moderate	Moderate	Low
BIKE	Code-based	1540	N/A	Moderate	Moderate	Moderate
NTRU	Lattice-based	1230	N/A	High	High	Good

Performance Benchmark Charts To visually compare the computational efficiency, the following benchmark charts depict encryption and decryption speeds for selected PQC algorithms. These benchmarks are derived from published research studies [e.g., References: 5, 6, 15].

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 9, September : 2024

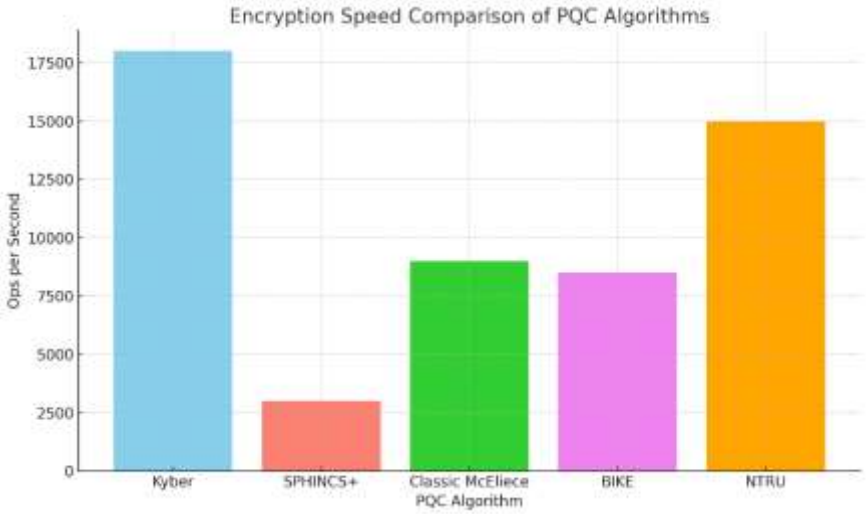

Figure 1: Encryption Speed Comparison of PQC Algorithms

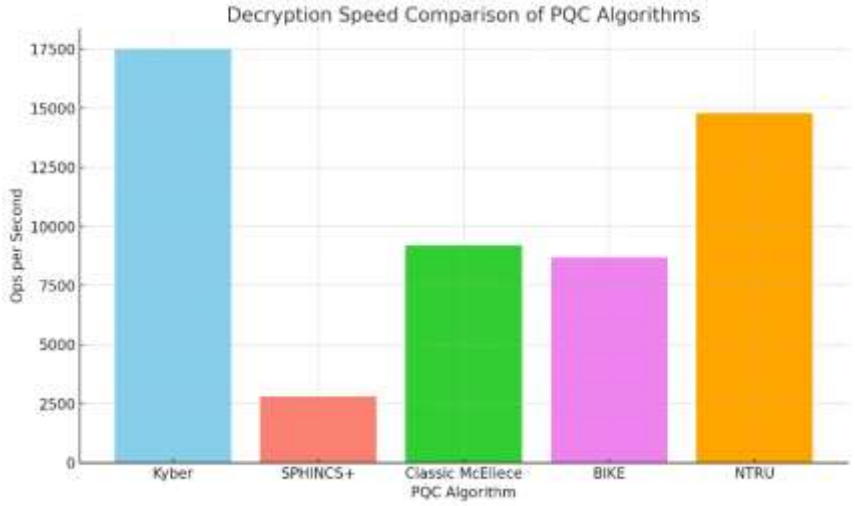

Figure 2: Decryption Speed Comparison of PQC Algorithms

- **RESEARCH GAP FROM LITERATURE SURVEY**

Although significant progress has been made in developing cryptographic solutions to secure Industrial Internet of Things (IIoT) systems, most existing security architectures rely on classical algorithms such as RSA and ECC, which are vulnerable to attacks by emerging quantum computing technologies. Current literature predominantly focuses on theoretical models and simulations without offering real-world testbed implementations or lightweight, scalable Post-Quantum Cryptography (PQC) mechanisms optimized for resource-constrained IIoT devices. Additionally, there is a lack of standardized hybrid cryptographic frameworks that integrate classical and quantum-resistant algorithms to provide layered protection. The

absence of performance benchmarking, deployment strategies, and practical key management protocols further emphasizes the need for a comprehensive solution.

a. Security Challenges in IIoT

The Industrial Internet of Things (IIoT), while revolutionary in enabling real-time monitoring, automation, and optimization of industrial operations, also introduces a multitude of cybersecurity challenges. As industrial systems become increasingly interconnected and digitized, the overall attack surface expands, making IIoT systems more prone to cyber intrusions and threats.

- **Heterogeneous devices and legacy systems**
  IIoT infrastructures typically consist of diverse, heterogeneous devices, ranging from modern smart sensors and actuators to outdated legacy industrial control systems (ICS). These legacy components often lack native support for secure communication protocols and are not easily upgradable, posing significant challenges for security integration. As highlighted by Fernández-Caramés et al. [2], the presence of multiple device types and non-standardized communication interfaces makes it difficult to implement a unified security framework, thereby increasing system vulnerability.

- **Limited computational power in edge devices**
  Most IIoT edge devices—such as Raspberry Pi, Arduino boards, and microcontrollers—are constrained in terms of processing power, memory capacity, and energy efficiency. These limitations create a significant bottleneck when implementing traditional cryptographic algorithms like RSA and ECC, which are computationally intensive. According to Imran et al. [6], there is a growing need for lightweight cryptographic techniques specifically optimized for low-power environments to ensure security without affecting device performance.

- **Multiple attack vectors**
  IIoT systems are exposed to several potential attack vectors, including:
  - Man-in-the-Middle (MITM) attacks, where communication between devices is intercepted and altered.
  - Data Spoofing, where false sensor data is injected to manipulate system behaviour.
  - Denial of Service (DoS) attacks, aimed at overwhelming devices or networks to cause system failure or shutdown.

  As described by Sivakumaran et al. [4], designing secure and resilient data transmission protocols is crucial to mitigate such threats, particularly in quantum-vulnerable environments. Moreover, Tiwari et al. [9] emphasized the importance of adopting quantum-safe communication protocols, which can provide enhanced resilience against sophisticated cyber-attacks that traditional cryptographic methods may no longer withstand.

- **Role of cryptography and Its limitations**
  Cryptographic mechanisms play a vital role in ensuring confidentiality, integrity, and authentication in IIoT communications. However, current security implementations heavily rely on classical cryptographic schemes like RSA, AES, and ECC, which are increasingly vulnerable to the computational power of quantum algorithms. As outlined by Bavdekar et al. [5] and Kumar and Pattnaik [20], these traditional encryption methods

are not only resource-intensive but also susceptible to being compromised by algorithms such as Shor's Algorithm, once practical quantum computers emerge. Ahmad et al. [3] and Rahman and Haider [11] have underscored the urgency to transition toward Post-Quantum Cryptography (PQC) and hybrid cryptographic models, which provide layered security and offer scalable, future-proof solutions suitable for modern IIoT infrastructures.

- **PROBLEM STATEMENT**

As quantum computing advances, traditional cryptographic techniques used to secure IIoT systems will soon become obsolete, exposing critical infrastructure to unprecedented cybersecurity risks. There is an urgent need for a practical, lightweight, and scalable security architecture that can withstand future quantum threats without compromising the performance of resource-constrained IIoT environments. However, existing solutions fail to address the real-world integration of PQC algorithms, lack hybrid cryptographic implementations, and offer limited insights into scalability, key management, and efficiency benchmarks for industrial applications.

- **PROPOSED SOLUTION**

This research proposes a quantum-resilient security architecture specifically designed for IIoT systems by integrating Post-Quantum Cryptography (PQC) algorithms that are optimized for low-power, embedded edge devices such as Raspberry Pi. The architecture also incorporates a hybrid cryptographic model, combining classical encryption methods with quantum-resistant algorithms to ensure layered and future-proof protection. The solution is evaluated on critical parameters such as resource efficiency, scalability, and security resilience, providing a holistic and practical foundation for implementing PQC in real-world IIoT environments. This approach bridges the gap between theoretical PQC models and their industrial adoption by offering a deployable, efficient, and secure architecture that can be seamlessly integrated into existing IIoT systems while aligning with upcoming NIST cryptographic standards.

- **QUANTUM COMPUTING AND ITS THREAT TO CRYPTOGRAPHY**

Quantum computing is emerging as a transformative technology that poses a significant threat to traditional cryptographic systems. Unlike classical computers that operate on bits (0 or 1), quantum computers use quantum bits (qubits) that can exist in superposition, enabling them to perform multiple calculations simultaneously. This inherent parallelism enables quantum machines to solve complex mathematical problems exponentially faster than classical systems, thus threatening the very foundations of existing encryption methods.

1. Basics of Quantum Computing

Quantum computing is grounded in principles of quantum mechanics, notably:

a. Superposition, where a qubit exists in multiple states at once.
b. Entanglement, where the state of one qubit is linked to another, even at a distance.
c. Quantum Parallelism, allowing the simultaneous execution of multiple operations.

These principles offer enormous computational capabilities that challenge current security protocols based on mathematical complexity.

2. Shor's and Grover's Algorithms

Two landmark quantum algorithms demonstrate the threat to classical cryptography:

a. Shor's Algorithm can factor large integers and compute discrete logarithms in polynomial time, making it capable of breaking RSA, DSA, and ECC—the most commonly used public-key cryptographic systems.
b. Grover's Algorithm provides a quadratic speedup in brute-force attacks, effectively halving the security strength of symmetric algorithms like AES.

3. Impact on Classical Cryptographic Systems

Quantum algorithms pose a direct threat to widely used encryption schemes:

- RSA: Compromised by Shor's algorithm via fast integer factorization.
- ECC: Vulnerable through efficient discrete logarithm solving.
- AES: While still considered secure, Grover's algorithm reduces its effective key strength by half, necessitating larger key sizes or alternative symmetric encryption methods.

4. Timeline of Quantum Threats

As per industry projections (e.g., NIST, NSA, IBM), the quantum risk horizon is anticipated around 2030–2035, when quantum computers may gain the scale required to break RSA-2048 and ECC-256 encryption. This raises concerns of a "harvest now, decrypt later" threat scenario, where encrypted data is intercepted today and decrypted in the future when quantum computing becomes powerful enough.

5. Urgency to Adopt Quantum-Safe Algorithms

Given the impending risks, the cryptographic community is actively transitioning to Post-Quantum Cryptography (PQC)—a set of algorithms resistant to quantum attacks. Ahmad et al. [3] emphasized that the urgency to adopt quantum-safe cryptographic protocols is especially critical for IIoT systems where device longevity, sensitive data exchange, and real-time communication necessitate future-proof security. The paper advocates for early adoption of PQC, integration with lightweight devices, and development of hybrid cryptographic models that combine classical and post-quantum methods for layered protection.

6. Need for Post-Quantum Cryptography (PQC)

The escalating threat posed by quantum computing has made it imperative to transition from classical cryptographic schemes to more resilient and quantum-safe alternatives. Traditional public-key cryptographic algorithms such as RSA, ECC, and DSA, which rely on computational hardness assumptions like prime factorization and discrete logarithms, are particularly vulnerable to quantum algorithms like Shor's Algorithm. Even symmetric cryptographic systems like AES, though not entirely broken, face a significant reduction in effective security due to Grover's Algorithm, necessitating larger key sizes or new alternatives.

Given the anticipated quantum risk horizon between 2030 and 2035, there is growing urgency to implement Post-Quantum Cryptography (PQC) algorithms that can resist both classical and quantum attacks. This urgency is especially critical for Industrial Internet of Things (IIoT) environments, where devices have long life cycles, and security updates or algorithm migrations post-deployment are often impractical or cost-intensive.

PQC algorithms—such as lattice-based (e.g., Kyber, NTRU), code-based (e.g., Classic McEliece, BIKE), multivariate polynomial, and hash-based (e.g., SPHINCS+) cryptosystems—are being actively evaluated and standardized by NIST for real-world adoption. These algorithms do not rely on number-theoretic problems that quantum computers can solve efficiently, making them ideal candidates for the post-quantum era.

Furthermore, Ahmad et al. [3] emphasized the importance of adopting PQC in IIoT settings, proposing lightweight quantum-safe algorithms that can operate efficiently on resource-constrained edge devices like Raspberry Pi. Similarly, Bavdekar et al. [5] and Kumar and Pattnaik [20] discussed the need to design hybrid cryptographic models that combine classical and PQC methods for layered security during the migration phase.

Apart from algorithmic security, PQC also addresses forward secrecy, robust key exchange mechanisms, and resilience against quantum-based interception attacks, all of which are vital for industrial systems transmitting sensitive telemetry and control data in real time.

In summary, Post-Quantum Cryptography is not merely a theoretical upgrade—it is a strategic necessity to safeguard critical infrastructure from quantum-enabled adversaries. The successful integration of PQC into IIoT ecosystems will ensure future-proof, scalable, and standards-compliant security for industrial operations.

- **PROPOSED HYBRID QUANTUM SECURITY ARCHITECTURE FOR IIOT SYSTEMS**

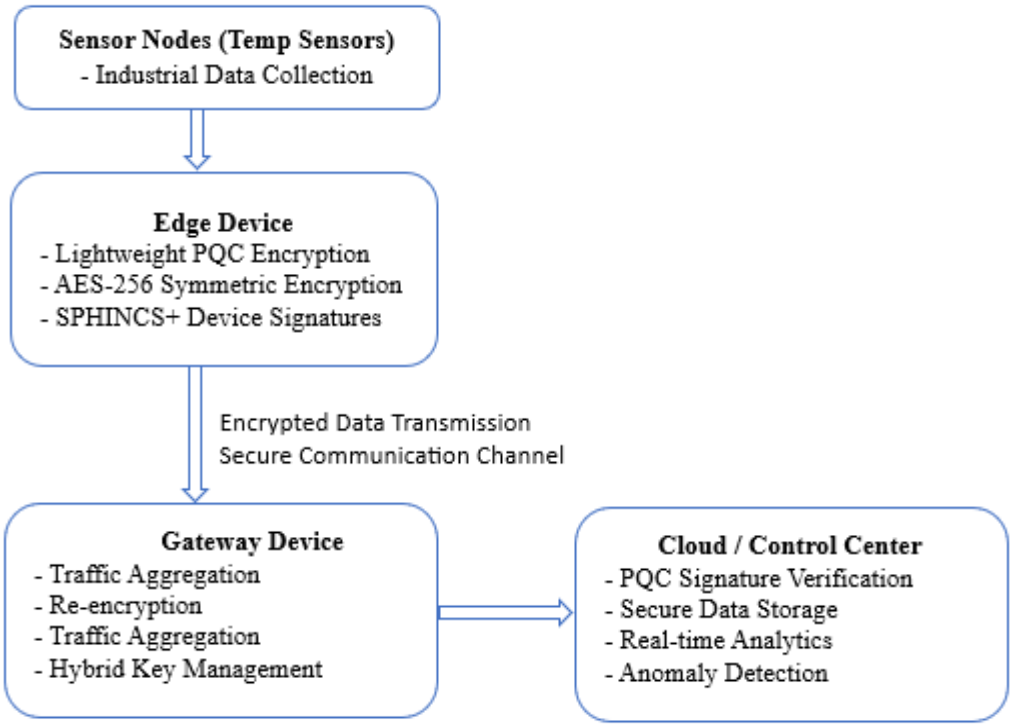

Figure 3: Proposed hybrid quantum security architecture for IIoT systems

The proposed architecture represents a hybrid security model for securing Industrial Internet of Things (IIoT) systems in the post-quantum era. It integrates Post-Quantum Cryptographic (PQC) mechanisms with classical cryptographic techniques to ensure end-to-end secure communication from sensor nodes to cloud infrastructure.

At the foundational layer, sensor nodes are deployed for industrial data collection, such as temperature, pressure, or environmental parameters. These sensors are connected to edge devices, specifically Raspberry Pi, which are selected due to their low cost and resource-constrained nature — representative of typical IIoT edge environments. The edge devices are embedded with lightweight PQC algorithms, AES-256 symmetric encryption, and SPHINCS+ digital signatures to secure the collected data and authenticate devices before data transmission.

Once encrypted, the data is transmitted through a secure communication channel implementing a hybrid TLS layer, which combines PQC-based key exchange mechanisms (such as Kyber or BIKE) with AES encryption to provide both quantum resilience and high-speed performance. The gateway device acts as an intermediary node, performing PQC decryption, optional re-encryption, traffic aggregation, and hybrid key management. It ensures that only validated and secure data reaches the cloud infrastructure. The gateway can also serve as a point for protocol translation, adapting different device-level protocols into a standardized format for cloud processing.

At the final stage, data reaches the cloud/control center, where it undergoes signature verification, secure storage, and real-time analytics. The architecture also supports anomaly detection mechanisms, optionally powered by Quantum Machine Learning (QML), for proactive threat identification. The Command & Control Interface in the cloud enables feedback mechanisms and device management across the IIoT network.

This layered architecture ensures confidentiality, integrity, authentication, and forward secrecy across the IIoT communication pipeline. By incorporating both classical and post-quantum cryptographic techniques, it offers a scalable and future-proof security framework against both contemporary and quantum-era cyber threats.

- **DISCUSSION**

The proposed hybrid quantum-resilient architecture effectively addresses key challenges in securing Industrial Internet of Things (IIoT) systems. Unlike many existing works that focus on theoretical PQC models, this architecture presents a practical design suitable for resource-constrained devices like Raspberry Pi, as noted by Ahmad et al. [3] and Imran et al. [6]. By using lightweight algorithms such as SPHINCS+ for signatures and Kyber for key exchange, alongside AES-256 encryption, it ensures strong security without overloading device resources. A key advantage of this model is its hybrid cryptographic framework, combining classical and post-quantum methods. This layered approach supports gradual migration from current RSA/ECC-based systems to quantum-safe standards, in line with suggestions by Bavdekar et al. [5] and Kumar and Pattnaik [20]. Secure communication is achieved using Hybrid TLS, enhancing data protection from edge to cloud, as emphasized by Sivakumaran et al. [4] and Tiwari et al. [9].

The architecture also includes key management, traffic aggregation, and digital signature verification, ensuring end-to-end security. Its modular structure allows easy integration of features like Quantum Machine Learning (QML) for anomaly detection, making it adaptable to future needs, as recommended by Liu et al. [10]. Additionally, it strengthens device-level authentication and attestation, addressing concerns highlighted by Khan et al. [8]. Overall, this architecture bridges the gap between PQC research and real-world IIoT application. It provides a practical, scalable, and future-ready solution to secure critical industrial systems against both classical and quantum threats.

- **FUTURE SCOPE**

As quantum computing advances, the need for secure and scalable IIoT systems becomes more critical. Future work can focus on hardware-level optimization of PQC algorithms using FPGAs, ASICs, or crypto co-processors to improve performance and reduce energy use in low-power devices. Integrating Quantum Key Distribution (QKD) for secure gateway-to-cloud communication and Quantum Machine Learning (QML) for anomaly detection can further enhance system security. Blockchain-based PQC frameworks may also be explored for decentralized identity management and secure logging.

Additionally, smooth migration strategies and interoperability standards are needed to ensure a seamless transition from classical to quantum-safe systems. Alignment with global standards (e.g., NIST, ENISA) and real-world deployment through testbeds and pilot projects will be key to building cyber-resilient industrial infrastructures.

• CONCLUSION

Quantum computing poses a serious threat to traditional cryptographic systems in IIoT environments. This paper presents a lightweight, hybrid security architecture combining Post-Quantum Cryptography (PQC) and classical encryption to secure resource-constrained industrial systems. Key components such as SPHINCS+ signatures, Kyber key exchange, and AES-256 encryption ensure data confidentiality, integrity, and device authentication across all layers—from sensors to the cloud. The model also supports future enhancements like Quantum Machine Learning for anomaly detection. By bridging the gap between PQC theory and real-world IIoT deployment, the proposed solution offers a scalable, quantum-resilient, and future-ready security framework, aligned with global standards like NIST.

• REFERENCES

1. M. El Zouka and A. Hosni, “On the power of quantum cryptography and computers,” in Proceedings of the International Conference on Computer Engineering and Systems (ICCES), 2014, pp. 190–195.
2. M. Fernández-Caramés, L. Castedo, and P. Fraga-Lamas, “From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things,” Sensors, vol. 20, no. 18, pp. 1–35, 2020.
3. A. Ahmad, S. Abbas, and A. A. Khan, “Enhancing security in the Industrial IIoT sector using quantum computing,” in International Conference on Computing, Communication, and Automation (ICCCA), 2021, pp. 561–566.
4. G. Sivakumaran, M. S. Kumar, and A. Krishnamurthy, “Detecting attackers during quantum key distribution in IoT networks using quantum-based secure and lightweight transmission,” in International Conference on Intelligent Computing and Communication Technologies (ICICCT), 2023, pp. 105–112.
5. R. Bavdekar, A. Bansod, and S. Shetty, “Post quantum cryptography: A review of techniques, challenges and standardizations,” in Proceedings of the International Conference on Information Security and Privacy (ICISP), 2023, pp. 84–91.
6. M. Imran, S. Rauf, and S. Hussain, “High-speed design of post quantum cryptography with optimized hashing and multiplication,” in International Conference on Emerging Trends in Computing (ICETC), 2023, pp. 127–133.

7. A. Mohanty, R. Patnaik, and B. Panda, “Quantum secure threshold private set intersection protocol for IoT-enabled privacy-preserving ride-sharing application,” in International Conference on Secure Computing and Communications (ICSCC), 2023, pp. 90–97.
8. M. A. Khan, S. Yadav, and R. Gupta, “Soteria: A quantum-based device attestation technique for Internet of Things,” in International Conference on Quantum-Safe Security Technologies (QSST), 2024, pp. 78–85.
9. A. Tiwari, V. Bansal, and R. Chhabra, “The quantum threat: Implications for data security and the rise of post-quantum cryptography,” in Proceedings of the International Conference on Cybersecurity and Data Protection (ICCDP), 2024, pp. 133–140.
10. M. Bellizia, L. D'Agostino, and F. Vitale, “Post-quantum cryptography: Challenges and opportunities for robust and secure hardware design,” in Proceedings of the Design Automation Conference (DAC), 2024, pp. 98–105.
11. M. Rahman and M. N. Haider, “Quantum-IoT: A quantum approach in IoT security maintenance,” in Proceedings of the International Conference on Quantum Computing and Communications (ICQCC), 2024, pp. 55–62.
12. T. Ali, R. Zafar, and A. Raza, “Quantum computing in cryptography,” in International Symposium on Quantum Technologies and Secure Communications (ISQTSC), 2024, pp. 112–118.
13. V. Singh, K. Gaur, and A. Srivastava, “Quantum computing-based bit encoding and decoding for IoT data transmission,” in International Conference on Future Technologies in Communication (ICFTC), 2024, pp. 145–151.
14. N. Bandi, M. Jha, and R. Tripathi, “Quantum machine learning for security data analysis,” in Proceedings of the International Conference on Artificial Intelligence and Cybersecurity (ICAICS), 2024, pp. 121–128.
15. P. Kumar, S. R. Singh, and D. K. Pandey, “Post-quantum cryptography: An overview,” in National Conference on Advanced Computing and Security (NCACS), 2024, pp. 62–68.
16. A. Sikdar, P. Bhosale, and R. Shinde, “Quantum secure threshold private set intersection protocol for IoT,” in International Workshop on Post-Quantum Secure Systems (IWPQSS), 2024, pp. 71–76.
17. A. Aman, A. Malik, and V. Rane, “Quantum-based device attestation for Internet of Things,” in International Conference on Embedded and Ubiquitous Computing (ICEUC), 2024, pp. 87–93.
18. S. Chaudhary, P. Shah, and A. Yadav, “Quantum signature-based secure data aggregation in IIoT,” in Proceedings of the Conference on Smart Industrial Technologies (SITech), 2024, pp. 101–108.
19. M. Kumari, R. Patel, and V. Joshi, “Cryptographic challenges and security in post-quantum cryptography migration: A prospective approach,” in Post-Quantum Systems and Migration Techniques Conference (PQSMTC), 2024, pp. 75–82.
20. R. Kumar and B. Pattnaik, “An overview of quantum-safe approaches: QKD and PQC,” in Proceedings of the International Conference on Quantum Secure Communication Systems (ICQSCS), 2024, pp. 53–59.
21. S. Gouram, S. K. Hasane, J. Somlal, S. D. Pande, P. Ganjewar and K. Pawar, "Development of IOT Based Smart Street Lighting System," 2024 International Conference on Innovation and Novelty in Engineering and Technology (INNOVA), Vijayapura, India, 2024, pp. 1-5.
22. D. K. J. B. Saini, S. H. Ahammad, P. Das, A. Bhatt, P. Malusare and S. D. Pande, "Grading of Fruit Ripeness Using Arduino in IoT," 2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET), Ghaziabad, India, 2023, pp. 184-188.