Securing IoT in the Post-Quantum Era: Implementation, Challenges, and Future Directions

Muhammad Asghar Khan and Muhammad Attique Khan

Abstract

The Internet of Things (IoT) is involved in almost every industry, paving the way for innovative applications, including smart cities, intelligent systems, smart homes, smart agriculture, healthcare, and more. However, due to their asset value, these applications are under continuous and evolving cyberattacks. Furthermore, the advent of quantum computing presents a severe threat to traditional cryptographic methods that typically secure IoT systems, potentially rendering existing security mechanisms ineffective against quantum-enabled attacks. To tackle quantum-enabled and traditional cyberattacks, post-quantum cryptography (PQC) has emerged as a promising solution for providing future-proof security for IoT devices and networks against the quantum computing threat. PQC algorithms can resist cyberattacks from classical and quantum computers, ensuring long-term security solutions. This article explores the integration of PQC into practical IoT systems. It highlights the vulnerabilities of classical cryptographic methods and the necessity of transitioning to quantum-resistant solutions. Moreover, the implementation of PQC on IoT systems is analyzed. By proactively exploring the opportunities and challenges associated with PQC, this research lays out future directions for implementing robust, scalable, and secure IoT systems.

Introduction

The Internet of Things (IoT) is a modern-day infrastructure for connecting everyday devices to the Internet, enabling seamless communication and automation across various applications, from smart homes to large industrial setups. In IoT, billions of interconnected devices generate, transmit, and receive massive amounts of data, offering knowledge to service providers and customers. There has been a marvellous trend in the growth of both smart devices and the networks they are connected to with the intensifying use of the Internet of Things (IoT). Based on GSMA statistics, IoT global devices were growing at 12.70% from 2019 through 2022. In 2025, the amount of IoT devices is predicted to grow to 41.6 billion with an annual growth rate of 16.7% by 2026 [1]. However, the exponential growth of IoT devices and the enormous amount of data they generate are vulnerable to various security threats, including unauthorised access, data breaches, and malicious attacks. Furthermore, evolving cybersecurity threats from the advent of quantum computing technology severely threaten traditional cryptographic methods that typically secure IoT systems, potentially rendering existing security mechanisms ineffective against quantum-enabled attacks. To tackle quantum-enabled and traditional cyberattacks, PQC has emerged as a promising solution for providing future-proof security for IoT devices and networks against the quantum computing threat [2]. Fig. 1 shows a layered IoT architecture that implements PQC to ensure quantum-resistant security.

Quantum computers offer the potential for specific computational tasks, such as factorization and quantum simulation, to be completed exponentially faster than classical computers [3]. Quantum computers can solve complex science problems that are even difficult for present-day supercomputers to solve. They will revolutionize artificial intelligence/machine learning (AI/ML) by dramatically boosting computation power. This capability challenges the security assumptions underlying traditional cryptographic algorithms, sparking concerns about the susceptibility of sensitive data to quantum-powered attacks. Such attacks impact the most popular asymmetric schemes, including rivest, shamir, adleman (RSA), elliptic curve digital signature algorithm (ECDSA), elliptic curve diffie-hellman (ECDH) or digital signature algorithm (DSA), which can be broken in polynomial-time with Shor's algorithm on a sufficiently powerful quantum computer. Moreover, quantum computers can use Grover's algorithm to reduce the effective key length by a factor of two by providing quadratic speed up for the unstructured search, which applies to searching the key in symmetric schemes like AES and 3DES [4].

With the increasing threat posed by quantum computers, there is an urgent need to secure existing IoT systems. Although significant progress has been made in developing and testing PQC algorithms, ongoing research means the threats

Digital Object Identifier:
10.1109/MCOMSTD.2025.3584658
Date of Current Version:
2 March 2026
Date of Publication:
30 June 2025

Muhammad Asghar Khan (corresponding author) is with the Department of Electrical Engineering, Prince Mohammad Bin Fahd University, Al-Khobar 31952, Saudi Arabia; Muhammad Attique Khan is with the Department of AI, Prince Mohammad Bin Fahd University, Al-Khobar 31952, Saudi Arabia.

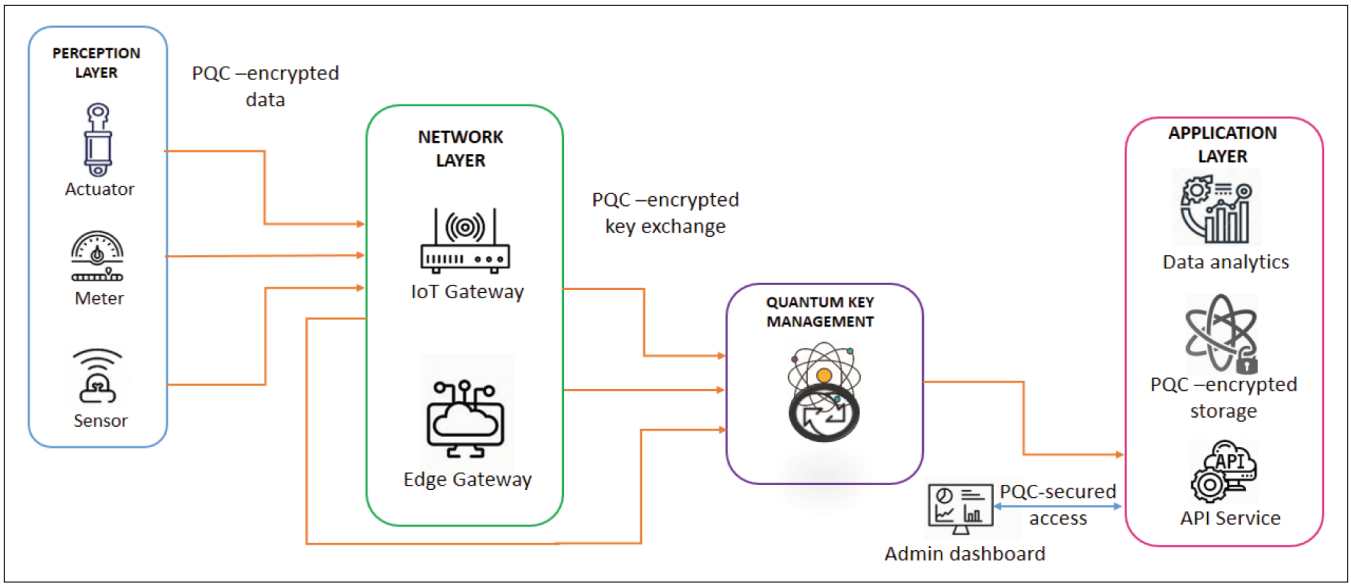

FIGURE 1. Layered IoT Architecture Integrating PQC Security.

remain unresolved and require continuous attention. This article focuses entirely on IoT security using PQC. The main contributions of this work include:

- In this study, we present a comprehensive discussion on PQC and its integration into IoT systems.
- We examine the security landscape of IoT systems by analyzing traditional security threats, emerging risks posed by AI/ML and the challenges posed by quantum computing.
- The practical implementation of PQC on IoT systems is also discussed in this work.
- Finally, this paper emphasizes the key challenges and outlines future directions, providing a foundation for innovative advancements in developing secure IoT systems.

The rest of the article is structured as follows. The "Security Landscape of IoT Systems" section discusses security threats and requirements of IoT systems. The "Post-Quantum Cryptography" section delves into the details of PQC. Finally, the "Challenges and Future Directions" section highlights open challenges and research directions.

Security Landscape of IoT Systems

IoT systems are typically at high risk of security and privacy breaches due to their vast attack surface, weak security algorithms, and lack of standardized security protocols. This risk arises from the connectivity of billions of IoT devices and sensors over open wireless channels, inadequate onboard computing resources, transmission of unencrypted data, lack of regular security updates and others. Moreover, botnet-enabled distributed denial of service (DDoS) attacks can leverage hacked IoT devices. The advancement of AI/ML fields brings with it uncontrollable risks, such as the ability to perform adversarial attacks on IoT-enabled AI systems, resulting in flawed decisions and gaps in the security of the system. Also, the growth of quantum computers poses a risk to encryption standards used in IoT devices and hence to the security employed in IoT.

Security Threats

This section examines the security landscape of IoT systems by analyzing traditional security threats, emerging risks posed by AI/ML and the challenges brought about by quantum computing.

1) Traditional Security Threats: Traditional security threats in IoT systems continue to pose significant data confidentiality, integrity, and availability risks. Common attacks include spoofing, where an attacker impersonates a legitimate device to gain unauthorized access, and DoS or DDoS, which overwhelms devices or networks, causing service disruptions [5]. Man-in-the-middle (MitM) attacks involve intercepting and manipulating communication between IoT devices, while jamming attacks disrupt wireless communication frequencies. Through cyberattacks, IoT devices are taken under control and utilized for malicious purposes, such as data harvesting and botnets. The system is tricked through injection attacks by inserting harmful code or commands. Replay attacks employed previously belong to verbatim data, bypassing the defense system. To alter a device's operation, fabrication attacks implant misleading information, while Sybil attacks impersonate multiple users to manage different sections of the network. Attackers can surreptitiously obtain sensitive data through Eavesdropping, whereas data can be dropped, routed, or fetched in wireless networks using wormhole and black hole attacks.

2) AI/ML Driven Security Threats: As AI and ML technologies continue to be integrated into IoT systems, they introduce a new set of sophisticated security threats. Model Inversion attacks involve attackers using access to a machine learning model to infer sensitive information about the training data, effectively reversing the model's predictions to extract confidential data. Model extraction attacks occur when an attacker repeatedly queries an ML model to steal and replicate its functionality, gaining access to the underlying intellectual property or proprietary knowledge. Poisoning attacks deliberately modify training data

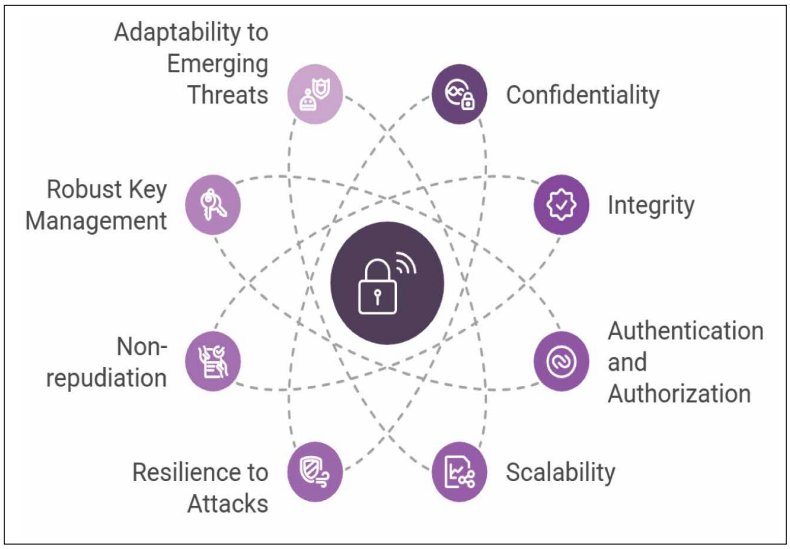

FIGURE 2. Illustration of key security requirements for a cryptographic scheme to secure IoT systems.

by introducing harmful data, which contaminates the data and results in inaccurate predictions, thereby deteriorating the dependability of the system. Automation attacks take advantage of the AI's automated functions to expand malicious actions such as instigating extensive botnet assaults or leveraging the vulnerabilities of numerous IoT devices, which complicates the processes of being discovered and having their impact obliterated. In adversarial attacks, relevant input data is modified in such a way that an ML model is deceived into making wrong predictions or classifications. Such actions could result in grave blunders in essential systems, including autonomous vehicles and industrial machinery. Deepfake attacks [6], driven by AI and DL techniques, can create realistic counterfeit media (audio, video, images) to impersonate legitimate users or devices, facilitating unauthorized access or manipulation of IoT systems.

3) Quantum Computing Treats: Quantum computing introduces a new era of potential threats to IoT security, challenging traditional cryptographic protocols and presenting new attack avenues. One of the most significant risks is breaking traditional cryptography — quantum algorithms like Shor's algorithm can efficiently solve problems that classical cryptographic methods rely on, such as factoring large numbers or solving discrete logarithms [7]. This ability threatens to render encryption techniques, such as RSA and ECC, obsolete, putting the confidentiality and integrity of IoT communications at risk. Another concern is quantum eavesdropping, where quantum computing could enable attackers to intercept and decode encrypted communications with unprecedented efficiency, compromising the privacy of data transmitted between IoT devices. In response, quantum key distribution (QKD) [8] has been proposed to secure key exchange. Still, attacks against QKD systems, such as QKD attacks, could undermine the security of this method by exploiting vulnerabilities in the transmission process. Additionally, quantum computing can be leveraged for AI model manipulation attacks, where quantum algorithms could be used to deceive ML models more efficiently or perform more powerful data extraction attacks. Quantum-enabled side-channel attacks represent another emerging threat, where quantum algorithms could potentially break encryption via indirect observations like power consumption or electromagnetic leakage. Botnet control attacks could also evolve, with quantum computing enabling more rapid and sophisticated manipulation of compromised devices within large-scale botnets, making them harder to detect and mitigate. Finally, future quantum-enhanced attacks could introduce entirely new attack vectors, such as cracking passwords and bypassing authentication systems using quantum speedups, creating a need for IoT systems to adopt quantum-resistant technologies to stay secure. These quantum-based threats highlight the importance of developing PQC and other advanced security measures to protect IoT systems in the quantum era.

Security Requirements

To ensure the security of IoT systems, any cryptographic scheme or security protocol implemented must address a comprehensive set of attributes specific to the unique nature of IoT networks. These attributes typically include the need for scalability, efficiency, privacy, integrity, authentication, and resilience against a wide array of threats, as shown in Fig. 2. Below are the key security requirements a cryptographic or security scheme should address for IoT systems:

- Confidentiality: To ensure that the sensitive data transmitted between IoT devices and the network is protected from unauthorized access.
- Integrity: To ensure that data has not been altered, either in transit or during storage, by unauthorized parties.
- Authentication and Authorization: To ensure that only legitimate devices and users can access IoT networks and perform authorized actions.
- Scalability: To ensure that the scheme can handle a large number of devices without compromising performance or security.
- Resilience to Attacks: To ensure that the scheme can resists various types of attacks, including both traditional and emerging threats like AI/ML-powered or quantum-based attacks.
- Non-Repudiation: To ensure that once a transaction or communication occurs, the involved parties cannot deny their participation or the content of the message.
- Robust Key Management: To ensure effective key management, especially when devices are distributed across vast areas.
- Adaptability to Emerging Threats: To ensure that the scheme continues to evolve as new threats, such as those introduced by AI/ML and quantum computing, emerge.

Post-Quantum Cryptography

The development of the first universal quantum computing model by David Deutsch, based on physical principles and the Church-Turing hypothesis [9], provided the theoretical basis for evaluating the security of PQC primitives. At its core, quantum computing operates on quantum bits or qubits, which, unlike classical bits, exist in

Parameter	Traditional Cryptography (RSA, ECC, AES)	PQC
Quantum Resistance	Vulnerable to quantum attacks (e.g., Shor's Algorithm)	Quantum-resistant (Designed to withstand quantum computing threats)
Security Against Classical Attacks	Strong but susceptible to machine learning-based attacks	Stronger (Resistant to classical and machine learning-based attacks)
Long-Term Viability	Vulnerable to advancements in quantum computing	High (Specifically designed for long-term security, ensuring resilience against quantum computers)
Adaptability to New Threats	Limited (Quantum computing undermines classical algorithms)	High (Adaptable to new and emerging threats, including quantum and machine learning advancements)
Post-Compromise Security	Weak (Key compromise leads to full security collapse)	Stronger (Some PQC schemes offer resilience even after part of the key is compromised)
Algorithm Diversity	Limited (Dominated by a few classical algorithms)	Growing (Multiple diverse schemes, including lattice-based, code-based, and multivariate polynomial approaches)
QKD Integration	Limited (No native support for QKD systems)	Native Support (Seamless integration with QKD systems, enhancing security in quantum environments)
Scalability	Limited (Performance degradation with larger key sizes, especially in RSA)	Improved (PQC schemes can be designed to scale efficiently, supporting large-scale deployments)
Multi-Party Computation Security	Vulnerable (Classical MPC schemes are at risk from quantum adversaries)	Enhanced (PQC strengthens multi-party computations, even in the presence of quantum adversaries)
Integration with Blockchain	Vulnerable to quantum attacks (RSA/ECC-based blockchain systems susceptible to quantum computers)	Quantum-resistant (PQC ensures blockchain security with quantum-safe digital signatures and key exchanges, future-proofing blockchain systems)
Integration with FL	Susceptible to machine learning and quantum-based attacks	Stronger (Ensures secure aggregation of model updates, protecting data and model integrity from quantum and ML-based attacks)

TABLE 1. Comparison of Cryptographic Parameters: PQC versus Traditional Cryptography.

multiple states such as both 0 and 1 at the same time due to the principle of superposition. This property enables quantum computers to perform computations on multiple possible inputs simultaneously, increasing computation power exponentially. Shor's algorithm, developed by mathematician Peter Shor in 1994, is one of the most prominent examples of the computational power of quantum computing [11]. Shor's algorithm efficiently factors large integers and solves the discrete logarithm problem, which is foundational to many asymmetric cryptographic schemes such as RSA and ECC. Similarly, Grover's algorithm, proposed by Lov Grover in 1996, demonstrates another facet of quantum computing's impact on classical cryptography in symmetric schemes like AES and 3DES. Grover's algorithm provides a quadratic speedup over classical algorithms for searching an unsorted database [12]. It reduces the security strength of symmetric encryption and hash functions by halving their effective key lengths. Table 1 provides a comparison of cryptographic parameters: PQC vs. traditional cryptography.

Table 2 compares the widely adopted symmetric and asymmetric cryptosystems and their security levels against pre-and post-quantum attacks. These tables reflect the impact of Shor's and Grover's algorithms on classical cryptosystems, giving the impression that quantum computers destroy the viability of asymmetric cryptography, leaving only symmetric cryptography alive, however, with the option of considering larger key sizes. Asymmetric cryptosystems, including the RSA, DSA, DH, ECDH key exchange, and the ECDSA, are insecure against quantum computing attacks, which are cracked by Shor's algorithm. The security toughness of the RSA cryptographic method generally relies on the hardness of factoring large bi-prime numbers, also known as the integer factorization (IF) problem [10]. In contrast, ECC argues that ECDL problems are challenging to solve [13]. However, both IF and the DLP are considered to be difficult for classical computers to solve. Still, they can be cracked in polynomial time by a quantum computer large enough to run Shor's algorithm. In today's time, however, small experimental quantum computers are not equipped enough to solve practical ciphers, and researchers estimate the quantum resources needed to achieve such a goal will be available shortly. Likewise, by cracking the symmetric cryptographic methods, Grover's algorithm can potentially reduce the security strength of existing ciphers by offering a quadratic speed-up for exhaustive key searching. However, the attack's practical implications are still debated because Grover's algorithm necessitates running queries sequentially. Nevertheless, researchers have calculated that Grover's search against the AES with 128, 192, and 256-bit security can be performed by a quantum architecture with 2953, 4449, and 6681 qubits, respectively. Consequently, it is

Cryptographic Algorithm	Type	Function	Pre-Quantum Security Level (in bits)	Post-Quantum Security Level (in bits)	Status
AES-128	Block cipher	Encryption	128	64	Cracked by Grover's algorithm
AES-256	Block cipher	Encryption	256	128	Cracked by Grover's algorithm
DES	Block cipher	Encryption	56	28	Cracked by Grover's algorithm
Salsa20	Stream cipher	Encryption	256	128	Cracked by Grover's algorithm
GMAC	MAC	Authentication	128	128	No impact
Poly1305	MAC	Authentication	128	128	No impact
SHA-256	Hash Function	Hashing	256	128	Cracked by Grover's algorithm
SHA-3	Hash Function	Hashing	256	128	Cracked by Grover's algorithm
RSA-3072	Asymmetric encryption	Encryption	128 bits	Broken	Cracked by Shor's algorithm
RSA-3072	Asymmetric digital signature	Digital signatures	128 bits	Broken	Cracked by Shor's algorithm
DH-3072	Asymmetric key exchange	Key exchange	128 bits	Broken	Cracked by Shor's algorithm
DSA-3072	Asymmetric digital signature	Digital signatures	128 bits	Broken	Cracked by Shor's algorithm
256-bit ECDH	Asymmetric key exchange	Key exchange	128 bits	Broken	Cracked by Shor's algorithm
256-bit ECDSA	Asymmetric digital signature	Digital signatures	128 bits	Broken	Cracked by Shor's algorithm

TABLE 2. Comparison of the widely adopted symmetric cryptosystems and their security levels against pre- and post-quantum attacks.

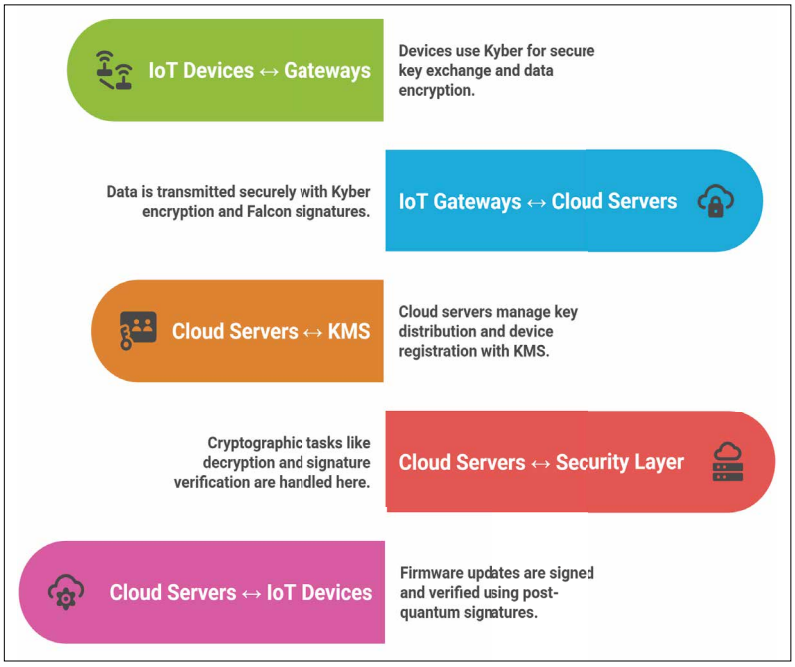

FIGURE 3. An illustration of the secure communication flow within IoT systems using PQC.

well accepted that quantum computers seriously threaten both symmetric and asymmetric cryptosystems; however, the danger to asymmetric cryptography is far greater than that to symmetric cryptography [14]. The ongoing efforts towards the standardization of PQC are spearheaded by NIST, which is currently selecting and standardizing quantum-resistant PQC algorithms. These algorithms are meant to replace classical schemes, which are vulnerable to quantum attacks. These organizations focus on evaluating candidate algorithms for security, efficiency, and practicality across a range of applications such as IoT, communications, and even cloud services. Other organizations, such as the Internet Engineering Task Force (IETF) and ISO, are also actively working towards the integration of PQC into existing protocols and standards, facilitating universal acceptance and interoperability in the post-quantum world.

Implementation of PQC on IoT Systems Security

This section outlines the key components and steps for implementing PQC in IoT systems security. Fig. 3 depicts the secure communication flow within IoT systems using PQC.

Post-Quantum Key Exchange With Kyber

The key exchange mechanism forms the foundation of secure communication in IoT systems. Kyber, a lattice-based key exchange protocol, is suitable for quantum-resistant key exchange due to its robustness against quantum attacks. In a typical IoT system, devices use Kyber to securely establish a shared secret with cloud servers or other devices.

Post-Quantum Key Exchange With Kyber

The key exchange mechanism forms the foundation of secure communication in IoT systems. Kyber, a lattice-based key exchange protocol, is suitable for quantum-resistant key exchange due to its robustness against quantum attacks. In a typical IoT system, devices use Kyber to securely establish a shared secret with cloud servers or other devices.

- Key Exchange Process: In the key exchange process, each IoT device and cloud server generates public and private key pairs based

on the Kyber algorithm. In the first contact between the device and cloud server, they share public keys and agree using Kyber encryption on a common secret which can be utilized for symmetric encryption like AES to encrypt and decrypt data.

Using Kyber for key exchange, IoT systems are protected from quantum adversaries attempting to penetrate communication channels.

Data Encryption and Transmission With Kyber and Falcon Signatures

Following the completion of the secret key exchange, maintaining the confidentiality and authenticity of the data exchanged between devices and cloud servers becomes crucial. Kyber may be applied apart from just key exchange, as it may also be applied to encrypt data during transmission. Devices and servers can sign and verify messages using Falcon, a post-quantum signature scheme, thus ensuring the integrity and authenticity of the data.

- Encryption and Authentication Process: IoT devices use Kyber to encrypt the data before transmission, making it unreadable to unauthorized entities, even in the presence of quantum attackers. Falcon signatures are applied to the encrypted data to prevent tampering and ensure the authenticity of the message. Each message is signed using a private key, and the recipient verifies the signature using the corresponding public key. The cloud server or receiving IoT device checks the Falcon signature to confirm the integrity and authenticity of the received data before decrypting it with the shared secret.

This dual-layer approach of encryption (Kyber) and signature verification (Falcon) ensures the data's confidentiality and integrity.

Cloud Server Role in Key Management and Device Registration

Within any IoT system, it is mandatory to manage the cryptographic keys and identities of the devices in a centralized way. A cloud server may serve as a trusted third party for device registration and key distribution. Using a KMS, the cloud can securely execute key lifecycle managed operations which include key creation, distribution, and rotation.

- Key Management and Device Registration Process: Each device is registered with the cloud server, which issues it a unique cryptographic identity. Furthermore, the cloud server provides public keys for exchange (e.g., Kyber) and securely stores private keys. New devices joining the network authenticate with pre-shared keys or certificates, while the cloud server automates the process of issuing new keys for secure communication. Moreover, the cloud server takes charge of key rotation, guaranteeing that compromised or deprecated keys are revoked and replaced.

This centralized management helps maintain control over cryptographic operations and ensures the security of devices across the network.

Offloading Cryptographic Tasks to Cloud Servers

IoT devices typically have limited processing power, memory, and energy resources. Performing computationally intensive cryptographic tasks, such as decryption and signature verification, on these devices can be impractical and inefficient. Offloading these tasks to more robust cloud servers can enhance the system's performance while maintaining security.

- Offloading Process: IoT devices perform lightweight encryption tasks and generate encrypted data that is sent to the cloud. The cloud server, equipped with more processing power, handles data decryption using the shared secret from the Kyber key exchange. The cloud verifies Falcon signatures before processing or forwarding data to other devices or applications.

Offloading these cryptographic tasks ensures that IoT devices are not burdened by resource-intensive operations, allowing them to focus on their core functionalities while maintaining security.

Secure Firmware Updates With Post-Quantum Signatures

Firmware updates are one of the most common attack vectors for IoT devices, as attackers can exploit vulnerabilities in outdated software to gain control over devices. Using post-quantum signatures, such as Falcon, to sign firmware updates provides an additional layer of security by ensuring that only authorized updates are installed.

- Firmware Update Security Process: Firmware updates are signed by the manufacturer or trusted entity using a private key. The IoT device receives the firmware update along with its signature. Before installing the update, the device verifies the signature using the public key, ensuring that the update has not been tampered with and originates from a trusted source.

This process mitigates the risk of malicious firmware injections, which could otherwise compromise device functionality and security.

Performance Considerations and Optimization

While PQC algorithms like Kyber and Falcon are quantum-resistant, they tend to be more resource-intensive than traditional cryptographic algorithms. To ensure efficient performance, it is crucial to consider the computational limits of IoT devices during the design phase.

- Optimization Strategies: Use hardware acceleration for cryptographic operations (e.g., specialized chips or modules designed for cryptography). Optimize cryptographic algorithms to reduce the computational overhead, balancing security with resource efficiency. Implement hybrid cryptographic models that allow IoT devices to switch between classical and post-quantum algorithms based on available resources or communication protocols.

Efficient implementation ensures IoT devices maintain secure operations without excessive energy consumption or performance degradation.

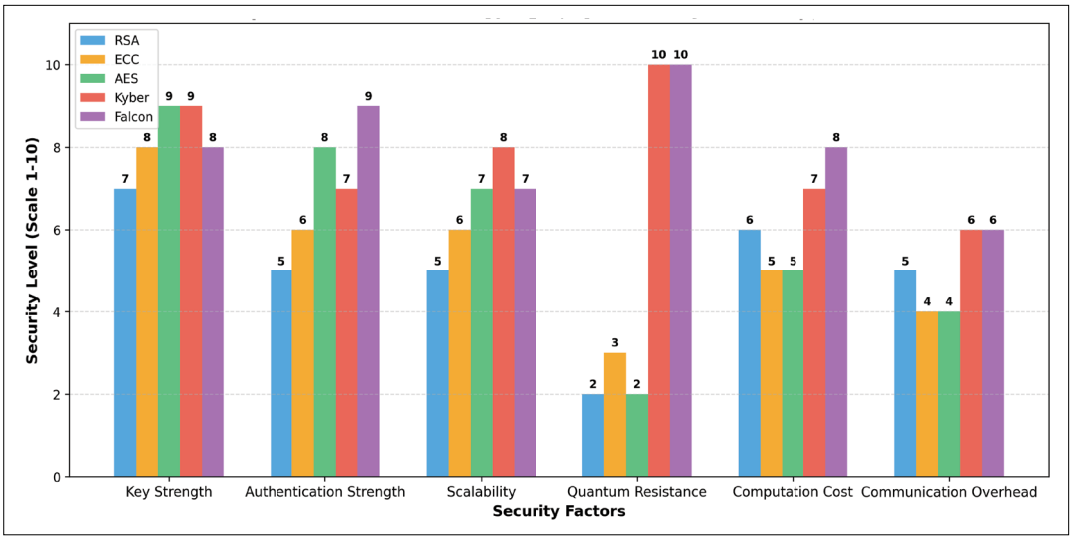

FIGURE 4. Security level comparison of traditional and post-quantum cryptographic protocols across key evaluation factors.

Discussion

The security comparison graph provides a detailed evaluation of various cryptographic schemes — RSA, ECC, AES, Kyber, and Falcon — based on six critical security factors relevant to IoT systems. While historically significant, RSA exhibits high computation cost, large key sizes, and poor scalability, making it inefficient for IoT applications. Moreover, it lacks quantum resistance, which increases its potential risk for future harm. Enhancements such as ECC superseding RSA weakened susceptibility to threats due to improved security in smaller key sizes, but they remain vulnerable to quantum exploitation. AES is a highly efficient, symmetric encryption used most in IoT due to its scalability and speed. However, it lacks built-in authentication, making it partially vulnerable to quantum threats via Grover's algorithm. In comparison, Kyber, a KEM for PQC, also excels in scalability and quantum security, and thus is more suited for future IoT security. However, it lacks self-sustained authentication features. Pairing Falcon, a lattice-post quantum signature scheme, with Kyber enables instant signature verification and compact signatures, which are ideal for IoT authentication and secure firmware updates. In summary, RSA, ECC, and AES, classical methods of IoT security, require the integration of newer quantum-based computing technologies like Kyber and Falcon to withstand the growing demands of sustainable, flexible, and comprehensive security. Fig. 4 presents a comparative evaluation of the security level of traditional and post-quantum cryptographic protocols across key evaluation factors.

PQC presents a promising solution for securing IoT systems against future quantum threats, ensuring long-term data protection and resilience. While traditional cryptographic methods like RSA and ECC are efficient today, their vulnerability to quantum attacks makes them unsuitable for future-proof security. PQC algorithms such as Kyber and Falcon offer strong resistance against quantum adversaries, making them viable candidates for next-generation IoT security. However, despite their advantages in quantum resistance and authentication strength, PQC algorithms currently exhibit high computational costs, increased key sizes, and higher communication overhead, which pose challenges for resource-constrained IoT devices.

Challenges and Future Directions

In this section, we examine key challenges and future direction in areas that require concentrated efforts to strengthen IoT security and privacy in a post-quantum world.

Challenges

- *Resource Constraints:* Implementing the PQC protocols on the next-generation IoT is challenging because they are slightly computationally intensive, and most IoT devices are generally equipped with limited computational resources. To tackle this, optimizing hardware and software is crucial to balance security with performance while designing PQC algorithms. Hence, lightweight PQC solutions, i.e., efficient and secure, can play a significant role in this effort.
- *Backward Compatibility:* Maintaining the interoperability of PQC schemes with existing classical cryptosystems is a critical challenge. Hybrid cryptosystems can provide an effective solution by combining classical and quantum-resistant algorithms to address this challenge. This ensures compatibility with current cryptographic infrastructures while paving the way for a gradual migration to PQC.
- *Deployment Costs:* The main challenge of deploying the PQC protocols on IoT systems is the high costs of redesigning compatible devices and updating the overall infrastructure. However, this challenge can be addressed with the supportive and collaborative efforts of industry partnerships and public-private initiatives.

Future Research Directions

- *Research and Development:* PQC is a newly emerging field that requires dedicated future

research efforts to develop lightweight algorithms. Most existing PQC algorithms incur high computations, which are unsuitable for resource-constrained IoT devices and sensors. Similarly, emerging technologies, such as neuromorphic computing and edge AI-based cryptographic accelerators, can be explored to improve the efficiency of existing PQC schemes and explore new ones. These innovations will make PQC protocols more practical and scalable for diverse IoT applications.

- *Inter-Industry Collaboration:* Effective deployment of PQC protocols on IoT devices requires close partnerships between semiconductor manufacturers, cryptography experts, the telecommunications sector, and IoT devices companies. This collaboration will enable the co-design of hardware and software solutions optimized for seamless integration of PQC.
- *Policies and Awareness:* Policies at the government level need to be initiated to drive global collaboration, establish universally accepted PQC standards for IoT devices, and address interoperability concerns. Public awareness campaigns about the importance of quantum-resistant security adaptation can foster consumer demand, further incentivizing manufacturers to adopt PQC standards.

Conclusion

PQC presents a promising solution for securing IoT systems against future quantum threats, ensuring long-term data protection and resilience. While traditional cryptographic methods like RSA and ECC are efficient today, their vulnerability to quantum attacks makes them unsuitable for future-proof security. PQC algorithms such as Kyber and Falcon offer strong resistance against quantum adversaries, making them viable candidates for next-generation IoT security. However, despite their advantages in quantum resistance and authentication strength, PQC algorithms currently exhibit high computational costs, increased key sizes, and higher communication overhead, which pose challenges for resource-constrained IoT devices. As technology evolves, advancements in hardware acceleration, optimization techniques, and hybrid cryptographic approaches may help mitigate these limitations, allowing IoT ecosystems to transition toward PQC adoption gradually.

References

[1] M. Huang et al., "Ensuring trustworthy and secure IoT: Fundamentals, threats, solutions, and future hotspots," *Comput. Netw.*, vol. 263, May 2025, Art. no. 111218.

[2] K. Mansoor et al., "Securing the future: Exploring post-quantum cryptography for authentication and user privacy in IoT devices," *Cluster Comput.*, vol. 28, no. 2, p. 93, Nov. 2024.

[3] B. Fauseweh, "Quantum many-body simulations on digital quantum computers: State-of-the-art and future challenges," *Nature Commun.*, vol. 15, no. 1, p. 2123, Mar. 2024.

[4] M. A. Khan et al., "Future-proofing security for UAVs with post-quantum cryptography: A review," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 6849–6871, 2024.

[5] C. Singh and A. K. Jain, "Defense strategies of DDoS attacks in SDN-IoT network: A survey," *Proc. Comput. Sci.*, vol. 259, pp. 809–817, Jan. 2025.

[6] A. F. Gambín et al., "Deepfakes: Current and future trends," *Artif. Intell. Rev.*, vol. 57, no. 3, p. 64, Feb. 2024.

[7] M. Kumar and B. Mondal, "Study on implementation of Shor's factorization algorithm on quantum computer," *Social Netw. Comput. Sci.*, vol. 5, no. 4, p. 413, Apr. 2024.

[8] Y. Cao et al., "The evolution of quantum key distribution networks: On the road to the QInternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart., 2022.

[9] F. V. Massoli et al., "A leap among quantum computing and quantum neural networks: A survey," *ACM Comput. Surv.*, vol. 55, no. 5, pp. 1–37, Dec. 2022.

[10] S. Sharma et al., "Post-quantum cryptography: A solution to the challenges of classical encryption algorithms," in *Modern Electronics Devices and Communication Systems* (Lecture Notes in Electrical Engineering). Singapore: Springer, 2023, pp. 23–38.

[11] D. Joseph et al., "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, May 2022.

[12] G. Yuan et al., "Quantum computing for databases: Overview and challenges," 2024, *arXiv:2405.12511*.

[13] M. A. Khan et al., "Security and privacy issues and solutions for UAVs in B5G networks: A review," *IEEE Trans. Netw. Service Manage.*, vol. 22, no. 1, pp. 892–912, Feb. 2025.

[14] M. Shafiq et al., "The rise of 'Internet of Things': Review and open research issues related to detection and prevention of IoT-based security attacks," *Wireless Commun. Mobile Comput.*, vol. 2022, no. 1, 2022, Art. no. 8669348.

[15] S. Chib et al., "Standardized post-quantum cryptography and recent developments in quantum computers," in *Proc. 1st Int. Conf. Adv. Comput. Sci., Electr., Electron., Commun. Technol. (CE2CT)*, Feb. 2025, pp. 1018–1023.

Biographies

Muhammad Asghar Khan (Senior Member, IEEE) (m.asghar@ieee.org) is currently with the Department of Electrical Engineering, Prince Muhammad Bin Fahd University, Al Khobar, Saudi Arabia.

Muhammad Attique Khan (Member, IEEE) (mkhan3@pmu.edu.sa) is currently with the Department of AI, Prince Muhammad Bin Fahd University, Al Khobar, Saudi Arabia.