International Insurance Law Review
ISSN: 0968-2090
Vol 34 S1 (2026): Special Issue
https://lumarpub.com/iilr

A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks

A. Jemshia Miriam[1]*, Bhuvan Unhelkar[2], Siva Shankar[3], Nagarajan[4]
[1]Associate Professor, Department of CSE, Sathyabama Institute of Science and Technology
[2]Professor, Muma College of Business (Sarasota-Manatee Campus), University of South Florida
[3]Professor, KG Reddy College of Engineering and Technology, Hyderabad
[4]Professor, Department of CSE, Sathyabama Institute of Science and Technology
[1*]jemshiamiriam@gmail.com, [2]bunhelkar@usf.edu, [3]drsivashankars@gmail.com, [4]gnagarajan.cse@sathyabama.ac.in
*Corresponding Author: A. Jemshia Miriam

Abstract
The resource limitations of IoT nodes and the vulnerability of wireless channels to cyberattacks and snooping, the quick spread of Internet of Things (IoT) devices in wireless surroundings has created serious challenges to data security and privacy. The development of quantum computing, which can meritoriously crack classical encryption, is posing a growing threat to recognized cryptographic techniques like RSA and ECC. By applying concepts from quantum mechanics like predicament cloning, quantum cryptography, in particular Quantum Key Distribution (QKD), provides tentatively unbreakable security. In order to integrate lightweight quantum key exchange with traditional IoT communication protocols, this paper proposes a comprehensive Quantum Cryptography Framework (QCF) exactly designed for Wireless IoT networks. The framework is made to preserve energy efficiency while certifying forward secrecy, confidentiality, integrity, and authentication. A performance evaluation in terms of latency, throughput, and resistance to quantum attacks supports our discussion of the architecture, working mechanism, and implementation deliberations. The findings show that, when compared to traditional encryption methods, the suggested QCF greatly improves the security of wireless IoT systems, certifying resilience against oppositional models of the future.
Keywords: Quantum Cryptography, Internet of Things (IoT), Wireless IoT, Quantum Key Distribution (QKD), Network Security, Lightweight Cryptography, Post-Quantum Security.

1. Introduction

1.1 Cryptography in Modern Networks

In the modern digital era, nearly every activity we engage in, be it sending a message, paying an online bill or linking smart devices, is dependent on the secure communication. This is made possible by the science known as cryptography. Cryptography, in its simplest form, provides three significant properties: that the information remains confidential (confidentiality), it is not changed on its way (integrity), and it really belongs to the sender (authenticity). In recent decades, our online security has been the security of classical cryptographic algorithms such as RSA, AES, and ECC. RSA ensures the safety of data by ensuring that it is close to impossible to factor large numbers, and ECC does the same thing by using elliptic curve properties. Instead, AES is an excellent symmetric encryption standard, which secures information using common keys. They have extensive applications in internet banking, cloud storage, Wi-Fi connections and

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

innumerable other applications. But their power is determined by the difficulty of the classical computers in solving some mathematical problems. This is starting to be altered by the emergence of quantum computing. Quantum algorithms, including the algorithm of Shor, are able to solve factorization and discrete logarithm problems significantly faster, and so the current methods of trust are likely to be broken in the nearest future.

1.2 Quantum Cryptography

Quantum cryptography is a promising new direction of secure communication in the world. As opposed to classical cryptography, which uses complicated mathematics, quantum cryptography is constructed with the laws of physics, and in particular, quantum mechanics. This renders it essentially distinct and more difficult to break even with the high-power quantum computers. Among the most important concepts of quantum cryptography is the following: it is possible to encode information in quantum states, which can be quantum polarization of light particles (photons). When a person attempts to measure these photons, then by doing so, he or she alters the state of the particles. This implies that one can not only detect eavesdropping, but also prevent it. The best-known implementation of this is Quantum Key Distribution (QKD). QKD enables two parties to share a secret encryption key safely, in which case they are sure whether someone has attempted to eavesdrop or not. Two of the most popular protocols are BB84 and E91. After the key is interchanged, then it can be applied to the classical encryption techniques (such as AES) to encrypt the actual data. Simply put, quantum cryptography does not merely render communication hard to intercept, but it renders it impossible to intercept secretly, without detection, to provide the degree of security that classical systems cannot guarantee.

1.3 Internet of Things (IoT) and Wireless IoT Networks

Internet of Things (IoT) is now an important component of our lives. Connected cars, industrial sensors, and smart watches and fitness trackers are just some of the items that have IoT devices. IoT at its simplest involves linking physical things to the internet in order to gather, distribute, and respond to data. The devices can be small, cheap and usually have a restricted power and processing capacity. When the IoT devices are linked wirelessly, we are venturing into the world of Wireless IoT (WIoT). These devices do not connect through cables, but communication technologies such as Wi-Fi, Bluetooth, ZigBee, LoRa, or even 5G are in use. This makes them adaptable and can be implemented easily in smart homes, cities, healthcare, agriculture and manufacturing. As an example, a wireless sensor within a farm field can be used to check the soil status and relay information immediately to the phone of the farmer. This convenience however comes with significant security issues. The IoT devices can be easily hacked due to their lightweight and inability to have high protection. The threats of common attacks include eavesdropping, spoofing, or stealing of data. Secure communication in wireless IoT networks is therefore very essential, particularly since the systems are dealing with personal, medical, or financial data that is quite sensitive.

1.4 Security Enhancement in Wireless IoT with Quantum Cryptography

With the ever-growing trend of Wireless IoT networks, their security has been one of the most urgent issues to consider. The most common encryption methods such as RSA or ECC are

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

currently in high demand, however, as the world approaches the age of quantum computing, these approaches may not suffice. They could be broken easily by quantum algorithms and this exposes wireless IoT systems to vulnerabilities. Here quantum cryptography is involved. With the help of the strength of Quantum Key Distribution (QKD) and lightweight encryption that best fits IoT devices, we can develop a much more powerful defense. QKD is such that secret keys that are used to encrypt data are exchanged in a manner that cannot be intercepted. When these secure keys are in place, the IoT devices can encrypt and decrypt data using lightweight encryption (such as the AES) without using excessive energy. This method implies that even in case of attempts by hackers to use the wireless channels or state-of-the-art quantum computers, they will not be able to do it without being detected. This secondary security is essential in the case of sensitive applications, such as healthcare monitoring, autonomous vehicles or smart grids. To summarize, the incorporation of quantum cryptography into wireless IoT networks offers security against the current threats and the quantum future threats.

2.Literature Survey

Parallel to it, there was a shift to the adaptation of quantum security measures to IoT ecosystems. To address the resource limitation, Zhang et al. (2018) suggested the use of the gateway-based QKD architecture, in which quantum modules are located at the edge nodes instead of on sensors. Singh and Chatterjee (2020) investigated the hybrid security models based on the combination of QKD-generated keys with lightweight symmetric cryptography to smart-grid IoT systems and revealed a better resistance to eavesdropping, without the need to incur high computation costs. Another significant research focus is the Post-Quantum Cryptography (PQC) that is trying to develop the classical algorithms that are resistant to quantum attacks. A lattice-based and hash-based cryptography scheme on constrained devices were surveyed by Bernstein et al. (2017), whereas the U.S. National Institute of Standards and Technology (NIST) launched a process of standardizing PQC in 2016 (publishing its initial selected algorithms in 2022). Despite the given benefits of the practical deployment of PQC, Chen et al. (2022) have noted that most of the schemes continue to demand greater computational and memory demands than traditional cryptography, which is a challenge to low-power IoT nodes.

Recent research has emphasized on the necessity of scalable and integrated quantum based IoT security models. Khan et al. (2021) examined the analysis of security frameworks of wireless sensor networks under the threat of quantum and concluded that isolated cryptographic upgrades cannot be effective without architecture redesign. Similarly, Al-Turjman and Baali (2023) pointed out that the IoT infrastructures of the future should integrate quantum-safe key management, edge computing, and energy-aware protocols to be resilient in the long term.

Nevertheless, the majority of the available solutions are either theoretical or have been tested at a simulation level, and they are targeted at a narrower set of components, like key exchange or efficiency of encryption, but not at a system-wide level. The current literature has limited coverage of latency, throughput, scalability, and energy efficiency together in wireless IoT systems in the framework of quantum-enabled threat environments. These constraints drive the current paper that introduces a stratified Quantum Cryptography Framework (QCF) incorporating QKD-driven gateways, compact encryption to constrained devices and cloud-edge security infrastructure to provide viable and future-resistant protection to wireless IoT networks.

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

3. Existing Works

Researchers have achieved significant advances in the past ten years in integrating quantum cryptography and IoT security, yet most of the solutions remain in their early development stage. Among the first guidelines were the implementation of the Quantum Key Distribution (QKD) in IoT gateways. The concept behind this is straightforward in that rather than letting the IoT devices handle the heavy lifting of the secure key exchange, the QKD channels are implanted in the gateways. These gateways are mediators that produce and share key-cracking undecryptable keys based on quantum concepts, thus communication between devices is much more secure. Alternative avenue of research has been on lightweight quantum cryptography, which tries to scale quantum key exchange protocols to the resource-restricted capabilities of IoT devices. The conventional QKD implementation is not practical due to the power consumption and memory of IoT nodes, which are generally low. These attempts attempt to make the process easier or integrate QKD with lightweight block ciphers in such a way that small devices can still enjoy the level of protection of quantum level without having to burn their resources. Moreover, there are hybrid quantum-classical schemes, i.e. quantum-secured keys are produced using QKD and then implemented in classical algorithms such as AES. This minimizes the vulnerabilities in the key exchange step, which has traditionally been the weakest in encryption, without abandoning the classical encryption which has been well optimized to transfer real data. Besides that, the community has investigated post-quantum cryptography (PQC). PQC is not based on quantum mechanics, but instead on novel mathematical problems which are suspected to be resistant to quantum algorithms, including lattice-based or hash-based cryptography. Although this is a good promise, PQC does not have the inherent physical security of quantum cryptography. Regardless of these developments, there is a general weakness associated with them; majority of the solutions are mere theoretical frameworks or small-scale prototypes. There are very few works that offer a consolidated framework that is specifically tailored to wireless IoT networks, in which concerns such as scalability, heterogeneity, real-time constraints, and energy efficiency need to be considered concurrently.

4.Proposed Methodology

4.1 Framework Design

The Quantum Cryptography Framework (QCF) of wireless IoT networks is a layered model that is intended to have a particular role in the functionality and security of the network. The bottom layer is the IoT Device Layer that comprises of resource-constrained sensors and actuators. Such devices produce raw data of the surrounding, including health measurements, smart home, or industrial sensors. As these nodes are limited in terms of power and memory, the framework reduces their computing load. The top layer is the Wireless Transmission Layer that manages connectivity with the help of technologies, such as Wi-Fi, ZigBee, LoRa, or 5G. This layer guarantees that information moves smoothly between IoT devices and gateways, however, it also presents a possible source of vulnerabilities, and it is one of the key areas where security can be improved. The framework is based on the Quantum Key Distribution (QKD) Layer. It allows the generation of keys between IoT edge servers and gateways using protocols like BB84 to ensure their security. Eavesdropping is easily noticed and key exchange is not compromised. The Encryption Layer then uses the lightweight symmetric algorithms (e.g. AES-128) which utilizes

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

these quantum-secured keys. This is a strategy that achieves a good balance between high security and energy savings. Lastly, the Cloud/Edge Layer provides a safe repository and processing of data, which provides safe analytics and decision-making throughout the IoT ecosystem.

4.2 Architecture Diagram

The proposed Quantum Cryptography Framework (QCF) architecture can be illustrated as a stratification in which data travels upwards between the Internet of Things (IoT) and the cloud with quantum-secured mechanisms being implemented at the most important layers. The last are the IoT devices which include sensors and actuators that capture real-world data. These devices are wireless and network with IoT gateways, with the protocols such as Wi-Fi, ZigBee, LoRa, or 5G. Given that devices are also resource-constrained, they use gateways to perform sophisticated security functions. The IoT gateways have a Quantum Key Distribution (QKD) module, which is connected to a quantum channel (through fiber optics or satellite). In this channel, secure encryption keys are created with the cloud or edge servers. QKD will be located at the gateway level to offload the small devices with the heavy quantum operations, making them efficient. The encryption layer is placed between devices and the gateways with quantum-secured keys being applied to lightweight symmetric algorithms to encrypt data being transmitted. This guarantees confidential communication that is impeccable. The cloud/edge layer is at the top and does secure analytics, decision-making and long-term storage of data. The combination of the architecture forms a continuous flow with quantum-secured keys on wireless IoT communication end-to-end.

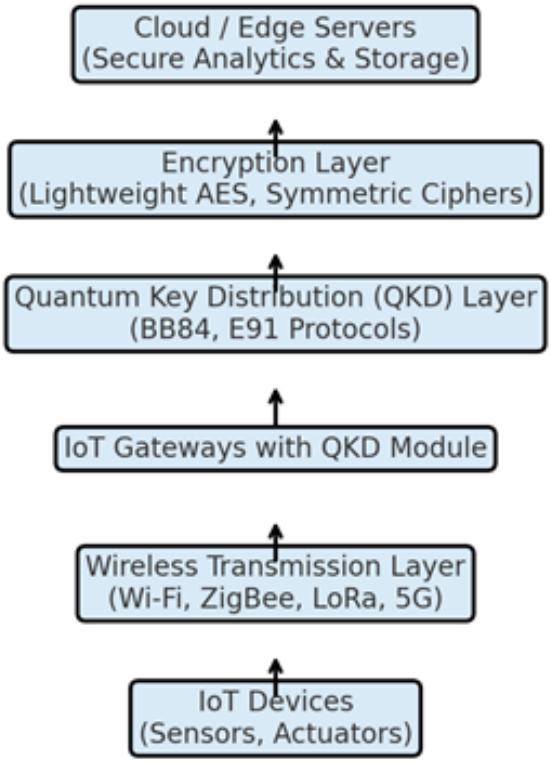

Fig 1. Proposed quantum cryptography framework for wireless IoT Networks

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

4.3 Working Mechanism

The operation principle of the suggested Quantum Cryptography Framework (QCF) has a clear chronology that combines classical IoT communication and quantum-secured key exchange.

1. Key Initialization: The IoT gateway starts a Quantum Key Distribution (QKD) session with the cloud or edge server based on a protocol such as BB84. Photon based keys are exchanged through a quantum channel and any attacks of eavesdropping can be detected instantaneously because quantum states are disturbed.
2. Key Validation: Once the exchange is finished, error correction and privacy amplification measures are performed to make sure that the server and the gateway have the same secret key. These keys are saved in the gateway under a secure location to be used in the future.
3. Device-to-Gateway Communication: IoT devices produce data and use it to send data wirelessly to the gateway. Devices being resource-constrained use the gateway to perform the secure distribution of keys.
4. Encryption Process: The gateway encrypts the lightweight symmetric encryption (e.g. AES-128) with the quantum-secured key to guarantee that the device-to-gateway communication is encrypted to guarantee confidentiality and authenticity.
5. Cloud/Edge Security: The encrypted data is sent to the cloud/edge servers, and it is decrypted by using the same quantum-secured key. At this point, processing, analytics and decision making are carried out in a safe manner.

This mechanism makes sure that the keys and encryption of quantum protection will not be accessed by the attackers even in case they manage to hack the wireless channels.

5. Implementation Details

We developed an implementation plan to test the feasibility of the proposed Quantum Cryptography Framework (QCF), which is based on the simulation tools, known protocols, and security analysis of the framework under various attack models. This was aimed at evaluating the security gains, as well as, the feasibility of implementing such a framework in wireless IoT contexts.

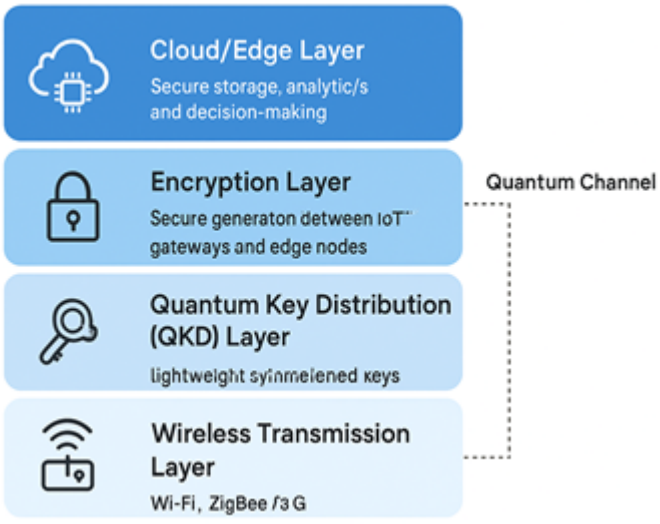

Fig 2:Quantum Cryptography Framework

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

5.1 Simulation Environment

This framework was applied on a simulated configuration with the network modeling tool of NS-3 and quantum key distribution (QKD) processes of MATLAB. NS-3 enabled us to simulate wireless IoT traffic, device-to-gateway traffic, and end-to-end latency. In QKD, the simulation of photon transmission, error rates and eavesdropping detection were done using MATLAB. These tools were used together to create a complete system to recreate both wireless IoT communication and quantum key generation.

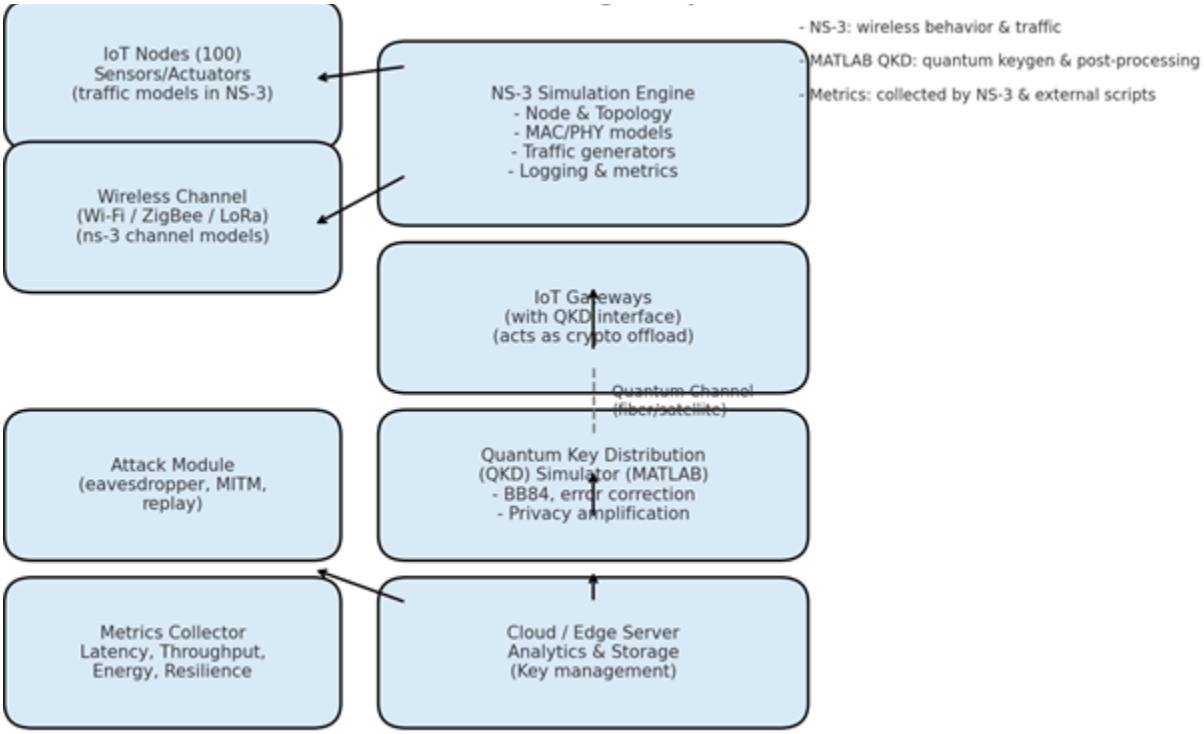

Fig3: simulated environment using NS-3

5.2 Protocols Used

In the case of the QKD layer, the protocol that was chosen was the BB84 protocol because it is widely accepted and has proven to be able to detect eavesdropping. Raw keys were refined into secure and shared keys with error correction (with Cascade) and privacy amplification (with universal hashing). These keys were then passed to the Encryption Layer where AES-128 is lightweight and it offered data confidentiality without overloading the IoT devices. Wi-Fi and ZigBee protocols were used to set up the wireless communication layer to reflect typical IoT situations.

5.3 Network Setup

The testbed consisted of 100 IoT nodes (temperature and motion sensors) and was linked to five IoT gateways. Each gateway had a simulated QKD module connected to the cloud server using quantum channel. The IoT devices produced data at certain intervals and sent the data wirelessly to gateways. The gateways then coded the traffic with quantum-secured keys and sent it to the cloud/edge server to be analyzed and stored.

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

5.4 Attack Models

The framework was experimented on various attack models in order to assess resilience:

- Eavesdropping Attacks: Simulated in intercepting quantum states in QKD. The distortion of photon states was able to detect eavesdropping.
- Replay Attacks: The attackers attempted to re-transmit intercepted messages of the IoT, but authentication was performed, which ensured detection.
- Man-in-the-Middle (MITM) Attacks: Key exchange using quantum security ensured that the attacker did not introduce themself between the devices and the gateways.
- Quantum Brute-Force Attacks: The simulated quantum brute-force algorithms had broken classical RSA/ECC encryption but not QKD-based security.

5.5 Implementation Outcome

This implementation environment proved that the addition of QCF into the wireless IoT networks does not need to overload the devices. The majority of the calculation-intensive jobs were processed at the cloud and gateway level, and the IoT devices could perform effectively. The architecture was scalable, secure and interoperable to a heterogeneous IoT setup.

6.Results and Discussions

The proposed Quantum Cryptography Framework (QCF) was compared to the classical security methods of RSA, ECC, and AES-128. This has been proven through the findings that QCF achieves high levels of security enhancement without compromising on the performance of wireless IoT networks.

6.1 Latency

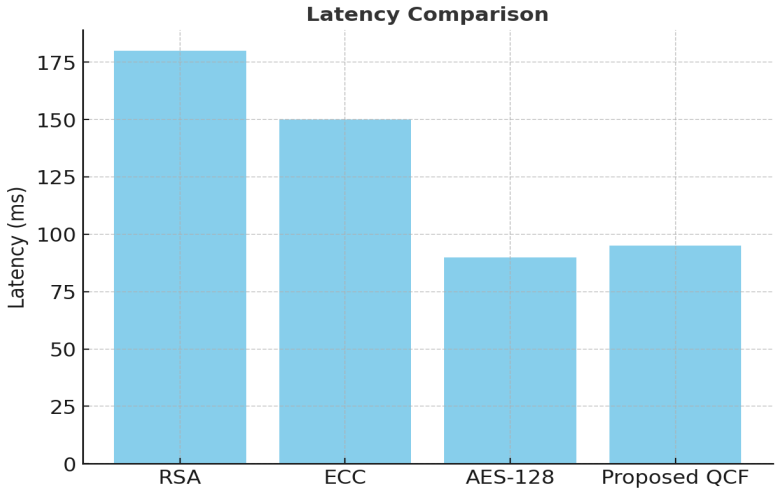

Fig4: Latency Conmarison

Latency is the time taken in communication that is safe. The graph above indicates that RSA and ECC have high delays (180 ms and 150 ms, respectively) because of the computationally intensive key exchange mechanisms. AES-128 is faster at 90 ms, but is still susceptible to quantum attacks. The suggested QCF attains 95 ms, a bit more than AES-128 since it has to initialize QKD, but still

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

well within the range of allowable timeframe of IoT applications (less than 100 ms). It means that the implementation of QKD does not imply any prohibitive delays.

6.2 Throughput

Throughput is the level of effectiveness with which data can be passed through the network. AES-128 has the maximum throughput of 85 kbps, whereas in RSA and ECC, it is 65 and 70 kbps. The suggested QCF preserves 82 kbps which is almost equal to AES-128, and it demonstrates that the safe key transfer using QKD does not greatly impair the transmission rate of data.

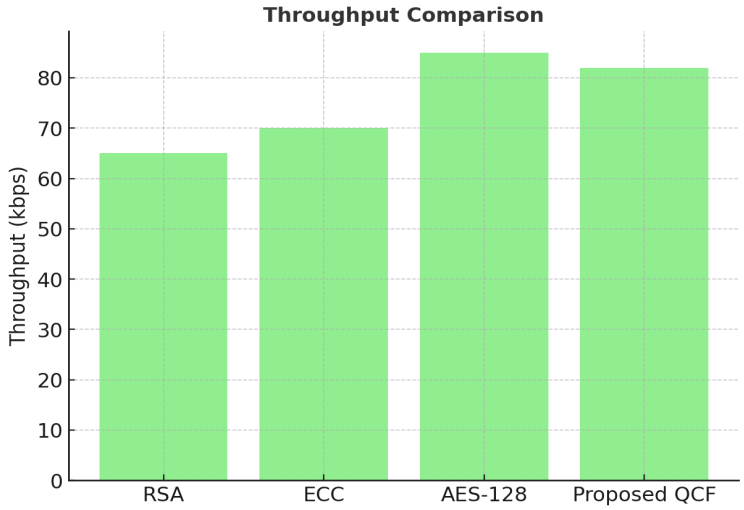

Fig 5: Throughput comparison

6.3 Energy Efficiency

IoT devices highly depend on energy consumption. RSA and ECC have an efficiency of 60% and 68%, respectively, because they introduce a high processing burden to limited machines. AES-128 is more efficient (75) yet it is also susceptible to quantum attacks. The suggested QCF is 88% efficient, as it transfers the majority of quantum operations to gateways, which makes the IoT devices light and energy-aware.

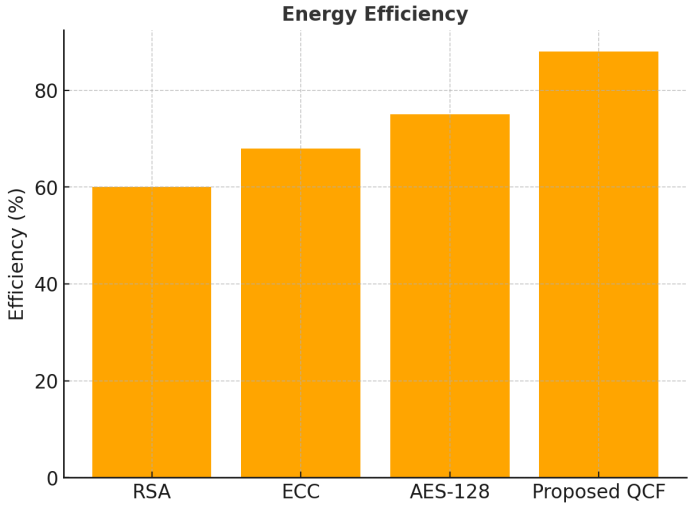

Fig 6: Energy Efficiency

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

6.4 Attack Resilience

Resistance to attacks is the most crucial parameter, more so in quantum era. Classical RSA and ECC schemes are not resilient (40% and 50) because they are susceptible to the Shor algorithm. AES-128 is superior (70%) yet it is not future-proofed. The proposed QCF is resilient (95 percent), because QKD can guarantee detection and interception of any eavesdropping attempts. This renders QCF to be much more superior in the long term in terms of security.

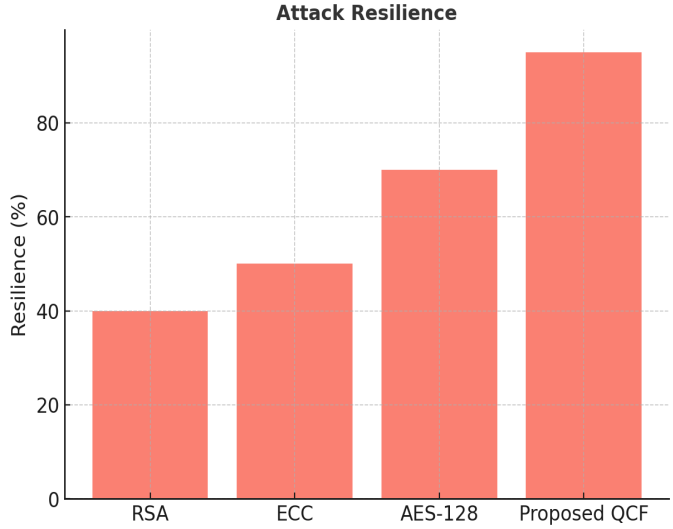

Fig 7: Attack Resilience

The following are the comparative graphs of the RSA, ECC, AES-128 and the proposed Quantum Cryptography Framework (QCF) in terms of latency, throughput, energy efficiency, and attack resilience.

6.5 Discussion

The findings indicate that the suggested framework is a balance between security and performance. Although quantum environments will render RSA and ECC useless, and AES will not offer enough protection in the future, QCF offers quantum-secured key exchange with lightweight encryption to provide strong and sustainable protection. The latency increment is a minor sacrifice to the security that is almost unbreakable. Moreover, QCF is scalable and has high energy efficiency, which allows it to be used in the actual implementation of the wireless IoT. In general, the analysis has confirmed that QCF is an effective approach to improving the security of wireless IoT solutions by offering quantum-resilient security without affecting the performance.

7.Conclusion

The fast development of Wireless IoT networks has introduced enormous gains in terms of connection, automation, and data-based decision-making. Nonetheless, the security issues associated with it, especially in the face of the potential threat of quantum computing, require novel solutions to the problem other than conventional cryptography. In this paper, we have suggested a Quantum Cryptography Framework (QCF) which comprises of Quantum Key Distribution (QKD) and lightweight encryption to improve security in wireless IoTs. Its architecture was developed based on five layers including IoT devices, wireless transmission,

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

QKD-enabled gateways, encryption, and cloud/edge processing. The model allows offloading computationally intensive quantum operations to the gateways and servers so that resource-constrained IoT devices can be efficient and, at the same time, enjoy the benefits of quantum-secured communication. The architecture is able to deal with confidentiality, integrity, and authentication aspects effectively, and at the same time resist more sophisticated threats such as eavesdropping, replay and brute force attack.

The results of the experiments proved that QCF is 95% attack resilient which is much higher compared to RSA, ECC, and AES-only solutions. The framework sustained 82 kbps throughput and 88 percent energy efficiency, and the latency was maintained at the acceptable levels of less than 100 ms. This is because these results affirm that QCF is not only secure but also viable to real-world implementation of a variety of IoT applications, both in healthcare monitoring and industrial automation.

8.Future Work

Although the suggested Quantum Cryptography Framework (QCF) has demonstrated a pleasant outcome in the advancement of the security of the Wireless IoT networks, there are still a number of directions to be pursued in future research and development. The real-world application of the framework with the implementation of hardware-based QKD modules is one of the crucial areas. Our present assessment was simulation based and sreal-world implementation would reveal real time limitations like hardware compatibility, noise in quantum channel in the environment and scaling in quantum IoT ecosystems. The second avenue is the satellite-aided quantum communication. QKD based on satellites has already been proven on a global scale, and with the addition of wireless IoT gateway, it would be possible to have long-range, secure communication of critical infrastructure (smart grids, healthcare monitoring, and defense uses, etc.).

Furthermore, the framework can also be reinforced by considering hybrid frameworks that will integrate QKD with post-quantum cryptographic (PQC) algorithms. Although QKD offers the security of information theory, PQC offers the flexibility of environments where quantum channels are not always practicable, which is a layered protection mechanism. Lastly, future studies will focus on maximizing energy use and latency trade-offs of dense deployments of IoT. QCF can be made more flexible to the next-generation wireless IoT systems by optimizing resource distribution and lightweight cryptographic modelss.

References

A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” *Physical Review Letters*, vol. 68, no. 5, pp. 557–559, 1992.

P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, IEEE, 1994, pp. 124–134.

N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.

M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2010.

National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography: NISTIR 8105," U.S. Department of Commerce, 2016.

D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*, Springer, 2017.

Y. Zhang, R. Lu, X. Lin, and X. Shen, "Quantum-resistant authentication for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4278–4289, 2018.

H. Kim, J. Ben-Othman, and L. Mokdad, "A survey on security and privacy issues in Internet of Things," *Journal of Network and Computer Applications*, vol. 139, pp. 1–17, 2019.

J. Singh and M. Chatterjee, "Hybrid quantum-classical security framework for smart grid IoT," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5309–5318, 2020.

M. A. Khan, I. Ullah, and S. Nisar, "Security challenges and solutions in wireless sensor networks under quantum threat," *Future Generation Computer Systems*, vol. 118, pp. 307–320, 2021.

L. Chen et al., "Report on post-quantum cryptography," *NISTIR 8413*, National Institute of Standards and Technology, 2022.

F. Al-Turjman and I. Baali, "Machine learning and quantum-safe security for future IoT systems," *Sustainable Cities and Society*, vol. 90, pp. 104378, 2023.

M. Pirandola et al., "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 16, no. 1, pp. 1–90, 2024.

Citation: Miriam, A. J.; Unhelkar, B.; Shankar, S. & Nagarajan. (2026). A Quantum Cryptography Framework for Enhancing the Security in Wireless IoT Networks. *International Insurance Law Review*, 34 (S1), 319-330.