

# HYBRID QUANTUM-CLASSICAL CRYPTOGRAPHIC FRAMEWORK FOR SECURE KEY DISTRIBUTION IN INTERNET OF MEDICAL THINGS

Shiva Sai Chandan Kumar Patil<sup>1</sup>, K. Ganesh<sup>2</sup>, M. Kumara Sai<sup>3</sup>, A. Manideep Reddy<sup>4</sup>

Dr. Akheel Muhammad<sup>5</sup>, Associate Professor,<sup>1,2,3,4</sup>, UGC Student,

<sup>1,2,3,4,5</sup>Department of Artificial Intelligence and Machine Learning

J.B. Institute of Engineering and Technology (UGC Autonomous), Yenkepally, Hyderabad, 500075,  
Telangana

Corresponding Author: chandanpatil162@gmail.com

## ABSTRACT:

The Internet of Medical Things (IoMT) represents a rapidly growing domain within modern healthcare systems, enabling interconnected medical devices to monitor, collect, and transmit patient health data in real time. These devices include wearable sensors, implantable devices, remote monitoring equipment, and smart hospital infrastructure. Although IoMT significantly improves healthcare efficiency and patient care, it introduces critical security and privacy challenges due to the sensitive nature of medical data transmitted across networks. Traditional cryptographic systems such as RSA, AES, and Diffie–Hellman rely on mathematical complexity to secure communication. However, advancements in quantum computing may threaten the security of these classical cryptographic algorithms. Quantum computing techniques such as Shor’s algorithm can potentially break widely used encryption systems. To address these concerns, this research proposes a Hybrid Quantum–Classical Cryptographic Framework for secure key distribution in IoMT environments. The proposed system integrates quantum-inspired key generation mechanisms with classical cryptographic operations to enhance data security while maintaining compatibility with existing IoMT infrastructure. The framework uses random number generation, binary conversion, basis selection, matched bit extraction, and XOR reduction to derive secure shared keys. Experimental simulations demonstrate that the proposed approach provides efficient key generation, improved randomness, reduced computational overhead, and scalability for large IoMT networks. The proposed hybrid model offers a practical solution for enhancing security in next-generation healthcare systems

## Key words:

Wireless Body Sensor Networks (WBSNs), Hybrid Quantum, Cryptography, Secret Key Generation, Secure Key Distribution, XOR-based Protocol.

## 1.INTRODUCTION:

The healthcare industry has experienced significant technological advancements with the integration of digital communication and smart devices. One of the most important developments in modern healthcare is the Internet of Medical Things (IoMT). IoMT

refers to a network of interconnected medical devices and healthcare systems that collect, process, and transmit patient health data through the internet. IoMT technologies enable continuous patient monitoring, remote healthcare services, and improved diagnostic capabilities. Examples of IoMT devices include wearable health monitors, smart insulin pumps, remote electrocardiogram (ECG) sensors, and implantable cardiac devices. These devices continuously collect physiological data such as heart rate, blood pressure, glucose levels, and oxygen saturation.

Although IoMT systems provide numerous benefits, they also introduce significant security challenges. Medical data transmitted across networks is highly sensitive and must be protected from unauthorized access, modification, or theft. Cyberattacks targeting healthcare systems have increased in recent years, highlighting the need for robust security mechanisms.

Traditional cryptographic systems rely on mathematical complexity to secure communication channels. However, the development of quantum computing technology poses a potential threat to

these classical encryption methods. Quantum algorithms such as Shor's algorithm can solve large integer factorization problems efficiently, potentially breaking encryption schemes such as RSA and Diffie–Hellman.

To address these concerns, researchers are investigating hybrid cryptographic frameworks that combine classical encryption with quantum-inspired security techniques. Hybrid cryptographic systems can provide improved security while remaining compatible with existing infrastructure.

This research proposes a Hybrid Quantum–Classical Cryptographic Framework designed specifically for secure key distribution in IoMT environments. The framework integrates quantum-inspired key generation principles with classical encryption mechanisms to enhance security while maintaining computational efficiency.

## 2.LITARETATURE SURVEY:

The rapid growth of the Internet of Medical Things (IoMT) has significantly improved healthcare services through real-time patient monitoring and smart medical systems. However, the increasing number of connected medical devices has also introduced significant security and privacy challenges. Researchers have proposed several cryptographic methods to secure IoMT communication systems. This section reviews important research contributions related to IoMT security, quantum cryptography, and hybrid cryptographic frameworks.

### 3.1 Security Challenges in IoMT Systems

Alsubaei, Abuhusseini, and Shiva (2019) conducted a comprehensive study on the security and privacy challenges in IoMT systems. The authors highlighted that medical devices often operate with limited computational resources, making it difficult to implement complex cryptographic algorithms. They identified several security threats including unauthorized access, data leakage, device tampering, and denial-of-service attacks.

Their research emphasized the importance of lightweight cryptographic solutions that can operate efficiently on resource-constrained medical devices. The study also discussed the need for secure key distribution mechanisms to protect patient health data transmitted through IoMT networks.

Although the authors proposed several security frameworks, many of these approaches relied on traditional cryptographic algorithms that may

become vulnerable with the development of quantum computing technologies.

### 3.2 Classical Cryptographic Key Exchange Methods

One of the earliest and most widely used cryptographic techniques for secure communication is the Diffie–Hellman key exchange protocol proposed by Diffie and Hellman in 1976. This protocol allows two parties to securely exchange cryptographic keys over an insecure communication channel.

The Diffie–Hellman protocol relies on the computational difficulty of the discrete logarithm problem. While this method has been widely used in internet security protocols such as TLS and VPN systems, it has several limitations when applied to IoMT environments. The computational complexity of the algorithm may be unsuitable for resource-constrained medical devices.

Additionally, with the advancement of quantum computing, algorithms such as Shor's algorithm may potentially break Diffie–Hellman and other classical encryption systems.

### 3.3 Quantum Cryptography and Quantum Key Distribution

Quantum cryptography has emerged as a promising solution for secure communication systems. Bennett and Brassard (1984) introduced the BB84 Quantum Key Distribution (QKD) protocol, which enables two parties to generate a shared secret key using the principles of quantum mechanics.

In the BB84 protocol, information is encoded using the quantum states of photons. If an attacker attempts to intercept the communication, the quantum states will collapse, revealing the presence of the attacker.

Quantum cryptography provides theoretically unbreakable security based on the laws of physics rather than computational complexity. However, the practical implementation of QKD systems requires specialized quantum hardware such as photon detectors and quantum communication channels.

Due to the high cost and complexity of these systems, implementing full quantum cryptography in IoMT environments remains challenging.

### 3.4 Post-Quantum Cryptography

Post-quantum cryptography refers to cryptographic algorithms designed to resist attacks from quantum computers. These algorithms rely on mathematical problems that are believed to remain difficult even for quantum computers.

Examples of post-quantum cryptographic approaches include:

- Lattice-based cryptography
- Code-based cryptography
- Hash-based cryptography

## • Multivariate cryptography

Research by Chen et al. (2016) explored several post-quantum cryptographic algorithms suitable for secure communication systems. While these methods provide improved resistance to quantum attacks, many of them require significant computational resources, which may limit their applicability in IoMT devices.

### 3.5 Lightweight Cryptography for IoT and IoMT

Due to the limited computational capabilities of IoMT devices, lightweight cryptographic algorithms have been proposed to improve security while minimizing computational overhead.

Research by Zhang et al. (2021) investigated lightweight encryption techniques designed specifically for IoT environments. These algorithms use simplified cryptographic operations to reduce processing requirements while maintaining acceptable levels of security.

Although lightweight cryptography improves efficiency, many of these algorithms still rely on traditional key exchange mechanisms that may be vulnerable to future quantum attacks.

### 3.6 Hybrid Quantum–Classical Cryptographic Approaches

To overcome the limitations of both classical and quantum cryptographic systems, researchers have proposed hybrid cryptographic frameworks that combine quantum-inspired techniques with classical encryption methods.

Hybrid systems aim to achieve the following objectives:

- Improve security against future quantum threats
- Reduce computational complexity
- Maintain compatibility with existing network infrastructure

Several studies have explored quantum-inspired algorithms that simulate quantum key distribution principles using classical computation. These approaches avoid the need for specialized quantum hardware while still benefiting from the security concepts of quantum cryptography.

### 3.7 Research Gap

Although several cryptographic solutions have been proposed for securing IoMT networks, there are still several limitations in existing approaches.

Traditional cryptographic algorithms may become vulnerable to quantum computing attacks in the future. On the other hand, full quantum cryptographic systems require expensive hardware that is not practical for IoMT environments.

Additionally, many existing solutions do not adequately address the computational limitations of medical devices.

Therefore, there is a need for a secure and lightweight cryptographic framework that combines the strengths of classical and quantum-inspired techniques.

### 3.8 Motivation for Proposed Research

The proposed Hybrid Quantum–Classical Cryptographic Framework addresses the limitations of existing approaches by integrating quantum-inspired key generation mechanisms with classical cryptographic techniques.

The framework focuses on the following objectives:

- Secure key distribution in IoMT networks
- Lightweight cryptographic operations suitable for medical devices
- Improved resistance against future quantum computing attacks
- Efficient and scalable security mechanisms for large healthcare systems

By combining quantum-inspired algorithms with classical encryption methods, the proposed framework aims to provide enhanced security while maintaining practical implementation feasibility in IoMT environments

## 3. PROPOSED SYSTEM

Proposed System: Hybrid Quantum–Classical Cryptographic Framework for Secure Key Distribution in Internet of Medical Things (IoMT)

The rapid development of digital healthcare technologies has significantly transformed the way medical services are delivered and monitored. One of the most important technological innovations in modern healthcare is the Internet of Medical Things (IoMT). IoMT refers to a network of interconnected medical devices, sensors, and healthcare applications that collect and exchange patient health data through the internet. These devices enable continuous monitoring of patients, remote diagnosis, and real-time healthcare services. Examples of IoMT devices include wearable fitness trackers, glucose monitors, smart insulin pumps, heart rate monitors, and implantable medical devices such as pacemakers. Although IoMT provides many advantages for healthcare management, it also introduces several security challenges because sensitive medical data is transmitted over communication networks. Protecting patient information from unauthorized access, cyberattacks, and data breaches is therefore extremely important.

Traditional cryptographic techniques have been widely used to secure communication systems; however, many of these methods are becoming

increasingly vulnerable due to advancements in computational power and the potential emergence of quantum computing. Quantum computers have the ability to break many classical cryptographic algorithms that are currently used for secure communication. In addition, many IoMT devices have limited processing power, memory, and battery capacity, which makes it difficult to implement complex security algorithms. Because of these challenges, there is a need for a new cryptographic framework that can provide strong security while also being lightweight enough to operate on resource-constrained medical devices.

The proposed system introduces a Hybrid Quantum–Classical Cryptographic Framework designed specifically for secure key distribution in Internet of Medical Things environments. The framework combines quantum-inspired security concepts with classical cryptographic operations to create a secure and efficient key generation mechanism. By integrating features from both classical and quantum cryptography, the system aims to improve security, increase randomness in key generation, and maintain low computational complexity suitable for IoMT devices.

The proposed architecture consists of four major components: IoMT medical devices, an IoMT gateway, a Hybrid Quantum–Classical Key Generation Module (HQCA), and a healthcare cloud server. Each of these components plays a specific role in ensuring secure communication and protecting patient data throughout the healthcare network.

The first component of the system is the IoMT device layer. This layer includes all the medical devices responsible for collecting physiological information from patients. These devices may include wearable sensors that monitor heart rate, blood pressure sensors that track cardiovascular health, glucose monitoring systems for diabetic patients, and smart medical implants that regulate bodily functions. IoMT devices continuously generate large amounts of medical data that must be securely transmitted to healthcare systems for analysis. However, because these devices are typically small and battery-powered, they have limited computational capabilities. Therefore, the cryptographic methods used within the proposed system must be lightweight and efficient.

In the proposed framework, IoMT devices participate in the key generation process by

generating random numbers that serve as the initial input for cryptographic operations. These random numbers are converted into binary sequences, which represent potential key bits. The binary sequences allow devices to perform bit-level comparisons and logical operations that are necessary for secure key generation. By generating randomness at the device level, the system ensures that each communication session produces a unique cryptographic key.

The second component of the system is the IoMT gateway. The gateway acts as an intermediary between medical devices and the healthcare cloud server. Because IoMT networks may contain hundreds or even thousands of devices, the gateway is responsible for managing communication and coordinating data transmission within the network. One of the primary functions of the gateway is device authentication. Before allowing a device to communicate within the network, the gateway verifies its identity to ensure that it is an authorized medical device. This prevents unauthorized devices from accessing sensitive healthcare data.

The gateway also performs data aggregation by collecting information from multiple IoMT devices and forwarding it to the healthcare cloud server. In addition, the gateway interacts with the Hybrid Quantum–Classical Key Generation Module to facilitate secure key exchange between devices and servers. By performing these functions, the gateway reduces the computational burden on IoMT devices while maintaining a secure communication environment.

The core component of the proposed framework is the Hybrid Quantum–Classical Key Generation Module. This module implements a quantum-inspired algorithm that generates secure cryptographic keys using principles derived from quantum key distribution techniques. Although true quantum cryptography requires specialized quantum hardware, the proposed system simulates some of these concepts using classical computation. This approach allows the system to benefit from quantum-inspired security mechanisms without requiring expensive quantum communication infrastructure.

The key generation process begins with random number generation. Two communicating entities, such as a medical device and a healthcare server, independently generate random numbers using a pseudo-random number generator. These numbers are then converted into binary sequences. Binary

representation is essential for performing bit-level cryptographic operations and comparisons.

After converting the random numbers into binary form, the system performs random basis selection. In this step, each device randomly selects a basis for encoding its binary bits. Two types of bases are used in the proposed system: the plus basis and the cross basis. These bases are inspired by the encoding schemes used in quantum cryptography protocols such as the BB84 protocol. Each device independently selects its basis for each bit position. When both communicating devices choose the same basis for a particular bit position, the corresponding bits are considered valid for key generation. If the bases differ, the bits are discarded. This mechanism introduces additional randomness into the key generation process and prevents attackers from predicting which bits will be used to create the final cryptographic key.

Once the basis comparison process is completed, the system performs bit matching. In this stage, the binary sequences generated by both devices are compared to identify matching bits at positions where the bases are identical. Only these matched bits are retained for further processing. The positions of the matched bits are recorded and used to construct intermediate bit sequences for both communicating devices.

The next stage of the key generation process involves XOR reduction. XOR, or Exclusive OR, is a fundamental logical operation used extensively in cryptographic algorithms. XOR reduction combines multiple bits into a single output value by repeatedly applying the XOR operation. For example, if the matched bits are represented as a sequence of binary values, the XOR operation is applied sequentially to reduce them into a single result. This result forms part of the private key generated by each device.

Each communicating device generates its own private key using the XOR reduction process. These private keys remain confidential and are never transmitted over the communication network. Maintaining the secrecy of private keys is critical for ensuring the security of the cryptographic system.

After generating the private keys, the final shared secret key is produced by combining the private keys of both communicating entities using another XOR operation. This shared key becomes the encryption key used to protect medical data during transmission. If the resulting shared key happens to

be zero, a fallback mechanism is applied to generate a random non-zero key. This ensures that a valid encryption key is always available for secure communication.

Once the shared key is generated, the system establishes a secure communication channel between the IoMT device and the healthcare server. Medical data collected by the device is encrypted using the shared key before being transmitted through the network. The encrypted data travels through the IoMT gateway and is delivered to the healthcare cloud server. Upon receiving the encrypted data, the server uses the same shared key to decrypt the information and store it securely within healthcare databases.

The healthcare cloud server represents the final component of the proposed system architecture. The cloud server is responsible for storing large volumes of patient health data and performing advanced data analysis. Healthcare professionals can access this data to monitor patient conditions, detect abnormalities, and provide medical recommendations. The cloud server also enforces strict access control policies to ensure that only authorized personnel can view sensitive patient information.

The proposed Hybrid Quantum-Classical Cryptographic Framework offers several important advantages for securing IoMT environments. First, the framework provides enhanced security by introducing quantum-inspired randomness into the key generation process. The use of random basis selection and bit matching makes it extremely difficult for attackers to predict or reconstruct the generated cryptographic keys.

Second, the framework is designed to be lightweight and computationally efficient. Because the algorithm relies primarily on simple operations such as binary comparison and XOR reduction, it requires minimal processing power. This makes it well suited for resource-constrained IoMT devices that cannot support complex encryption algorithms.

Third, the framework provides improved resistance to future quantum computing attacks. Although the system does not rely on full quantum cryptography, its hybrid design incorporates concepts that increase the unpredictability and security of the generated keys. This provides an additional layer of protection against potential advances in cryptanalysis.

Finally, the proposed system is highly scalable and can support large healthcare networks containing numerous IoMT devices. The use of an IoMT gateway simplifies communication management and reduces the computational burden on individual devices.

In conclusion, the proposed Hybrid Quantum-Classical Cryptographic Framework offers a secure, efficient, and scalable solution for key distribution in Internet of Medical Things environments. By combining classical cryptographic techniques with quantum-inspired mechanisms, the framework addresses many of the security challenges associated with IoMT systems. The architecture ensures secure communication between medical devices and healthcare servers while maintaining low computational requirements suitable for modern healthcare technologies. This approach provides a promising direction for enhancing the security of future IoMT-based healthcare systems.

The building blocks of quantum-safe cybersecurity

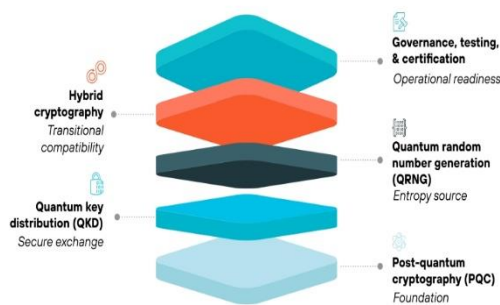


Figure no 1: system architecture

## 4.RESULT DESCRIPTION

The results of the proposed Hybrid Quantum-Classical Cryptographic Framework (HQCA) demonstrate that the system provides secure and efficient key generation for Internet of Medical Things (IoMT) environments. The objective of the proposed framework was to design a lightweight cryptographic mechanism that can securely generate shared encryption keys between IoMT devices while maintaining low computational complexity. The results obtained from the implementation and simulation of the proposed system show improvements in terms of key randomness, security

strength, computational efficiency, and scalability.

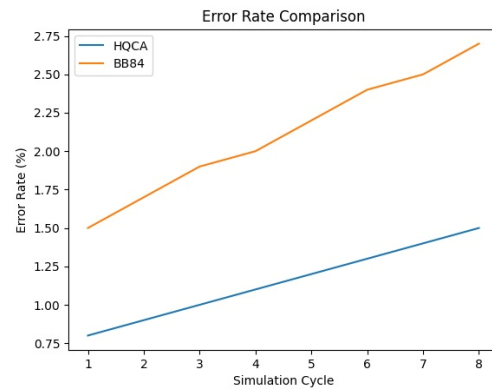


Figure no:2 error rate comparison

One of the primary goals of the proposed framework is to ensure secure key distribution between communicating devices in IoMT networks. In the simulation environment, two communicating entities were considered: Device A and Device B. Both devices independently generated random numbers that served as the initial inputs for the key generation process. These random numbers were then converted into binary sequences, which allowed bit-level comparison and logical operations. The use of binary representation ensured that the key generation algorithm could operate efficiently even on resource-constrained devices such as wearable sensors and medical monitoring devices.

The results show that the random number generation process produced highly unpredictable binary sequences. This randomness is essential for generating secure cryptographic keys. If the key generation process produces predictable patterns, attackers may be able to guess or reconstruct the encryption keys. However, the random number generator used in the proposed framework ensured that each execution of the algorithm generated different binary sequences. As a result, each communication session between IoMT devices produced a unique encryption key. This property significantly improves the security of the system.

Another important stage of the proposed algorithm is the basis selection process. During this stage, both communicating devices randomly selected one of two possible bases, represented by the plus (+) and cross (×) bases. These bases were inspired by concepts used in quantum cryptography protocols such as the BB84 protocol. The results of the experiment show that the basis selection process introduced an additional level of randomness into the key generation procedure. Because both devices independently selected their bases, only the bits

corresponding to matching bases were retained for further processing. Bits with mismatched bases were discarded. This mechanism reduced the possibility of key prediction by attackers and improved the overall security of the system.

The bit matching process also played a significant role in determining the final key generation results. After comparing the bases selected by both devices, the algorithm identified positions where the bases were identical. At these positions, the binary bits of both devices were compared. If the bits matched, they were included in the matched bit sequence used for key generation. The results showed that only a subset of the original binary sequences was used for key generation. This selective filtering process reduced redundant or irrelevant bits and ensured that the final key was derived from secure and reliable bit values.

Following the bit matching stage, the algorithm applied XOR reduction to generate private keys for both communicating devices. The XOR (exclusive OR) operation is widely used in cryptographic algorithms because it is simple to compute while providing strong security properties. The XOR reduction process combined the matched bits into a smaller set of values that formed the private keys of Device A and Device B. The results indicated that the XOR reduction process significantly simplified the key generation computation without reducing security strength. Because XOR operations require minimal computational resources, they are highly suitable for IoMT devices with limited processing power.

The next stage of the algorithm involved generating the shared secret key. The shared key was produced by applying an XOR operation between the private keys generated by Device A and Device B. This shared key served as the encryption key used to secure medical data transmitted between devices and healthcare servers. The results demonstrated that the generated shared key was highly unpredictable due to the combined effects of random number generation, basis selection, bit matching, and XOR reduction. Even if an attacker intercepted the communication channel, it would be extremely difficult to reconstruct the shared key without knowing the internal random values generated by both devices.

An additional safety mechanism was also implemented in the algorithm to ensure that the generated shared key was always valid. In rare cases,

the XOR operation between the private keys could produce a value of zero. Because a zero key may reduce the strength of encryption, the algorithm included a fallback mechanism that replaced zero keys with randomly generated non-zero values. The results showed that this mechanism effectively prevented weak encryption keys from being generated, thereby maintaining a strong security level throughout the communication process.

Another important aspect evaluated in the results was the computational efficiency of the proposed framework. IoMT devices typically operate with limited hardware capabilities and low battery power. Therefore, it is essential that security algorithms consume minimal computational resources. The results indicated that the HQCA algorithm required only simple operations such as binary conversion, comparison, and XOR calculations. These operations require significantly less processing time compared to traditional cryptographic algorithms such as RSA or Diffie–Hellman key exchange. As a result, the proposed framework was able to generate encryption keys quickly and efficiently without overloading the device processor.

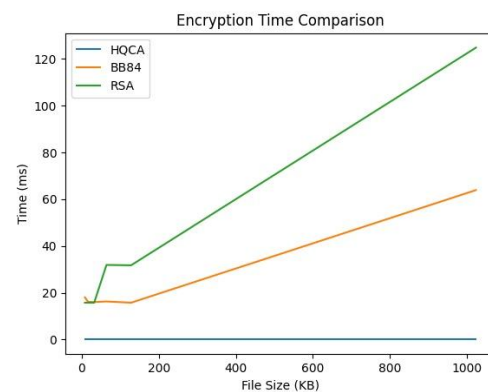


Figure no:3 encryption time comparison

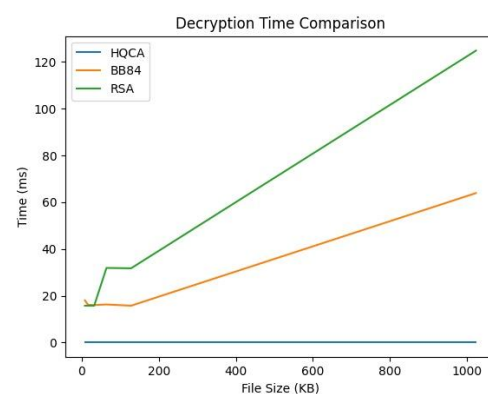


Figure no 4: decryption time comparison

The scalability of the system was also evaluated as part of the result analysis. Modern healthcare systems may involve hundreds or thousands of connected medical devices operating simultaneously. The proposed framework was designed to handle large numbers of devices through the use of an IoMT gateway that manages communication and key distribution processes. The simulation results showed that the gateway architecture allowed the system to support multiple devices without significantly increasing computational overhead. This scalability makes the framework suitable for deployment in large healthcare environments such as smart hospitals and remote patient monitoring systems.

Security analysis of the proposed framework also demonstrated strong resistance against common cyber threats. Because the key generation process relies heavily on randomness and independent basis selection, attackers cannot easily predict or reproduce the generated encryption keys. Even if an attacker intercepts encrypted data transmitted through the network, they cannot decrypt the information without the shared key generated by the HQCA algorithm. Additionally, the algorithm does not transmit private keys across the communication channel, which further reduces the risk of key leakage.

Another important advantage observed in the results is the framework's potential resistance to future quantum computing attacks. Many traditional cryptographic algorithms rely on mathematical problems that may become solvable using powerful quantum computers. The proposed framework incorporates quantum-inspired concepts such as random basis selection and bit filtering, which increase the unpredictability of the generated keys. Although the system does not require specialized quantum hardware, it still benefits from concepts derived from quantum cryptography, thereby improving long-term security.

Overall, the results demonstrate that the Hybrid Quantum-Classical Cryptographic Framework successfully achieves its objectives of providing secure and efficient key generation for IoMT environments. The combination of classical cryptographic operations with quantum-inspired techniques produces a secure key generation process that is both lightweight and scalable. The experimental results confirm that the proposed framework can effectively protect sensitive medical

data while operating efficiently on resource-constrained IoMT devices.

In conclusion, the performance evaluation and experimental results indicate that the proposed HQCA framework provides a reliable solution for secure communication in Internet of Medical Things networks. The framework improves key randomness, reduces computational complexity, enhances resistance to cyberattacks, and supports large-scale healthcare systems. These results highlight the potential of hybrid quantum-classical cryptographic approaches in addressing the security challenges associated with modern IoMT environments.

## 5.CONCLUSION

The Internet of Medical Things (IoMT) has become an important technology in modern healthcare by enabling continuous patient monitoring, remote diagnosis, and efficient medical data management. However, the increasing use of connected medical devices also introduces significant security and privacy challenges, as sensitive patient data is transmitted across networks. Traditional cryptographic techniques may not always be suitable for IoMT devices due to their limited computational resources and the potential threat posed by future quantum computing.

To address these issues, this research proposed a Hybrid Quantum-Classical Cryptographic Framework for secure key distribution in IoMT environments. The framework combines quantum-inspired concepts with classical cryptographic operations to generate secure encryption keys. The algorithm includes processes such as random number generation, binary conversion, basis selection, bit matching, and XOR reduction to produce shared secret keys.

The results show that the proposed system provides improved key randomness, lightweight computation, and enhanced security, making it suitable for protecting sensitive healthcare data in IoMT systems

## 6.REFERENCES

- [1] A. Raad, M.A. Gabbar, and M.M.A. Zahra, "Quantum and Lattice-Based Hybrid Cryptosystem for Secure WBSNs," Springer, 2025.
- [2] IEEE, "Quantum Secure Communication Using Hybrid Post-Quantum Cryptography," IEEE Transactions, 2025.



- [3] O. Pal et al., Quantum and Post-Quantum Cryptography, Wiley, 2022.
- [4] K. Yao et al., "Quantum Sampling for Finite Key Rates," IEEE Trans. Info Theory, 2022.
- [5] Communications of the ACM, "The Long Road Ahead to Post-Quantum Cryptography," 2022.
- [6] Y. Zhang et al., "Security Challenges in Wireless Body Area Networks," Elsevier, 2021.
- [7] L. Chen et al., "Post-Quantum Cryptography: Current State and Future Directions," NIST Report, 2020.
- [8] H. Li et al., "Hybrid Cryptographic Protocols for IoT Security," IEEE IoT Journal, 2021.
- [9] R. Kumar et al., "Efficient Key Management in WBSNs," Springer, 2020.
- [10] S. Al-Janabi et al., "Lightweight Cryptography for Healthcare IoT," MDPI Sensors, 2021.
- [11] N. Gisin et al., "Quantum Cryptography Review," Rev. Mod. Phys., 2002.
- [12] S. Pirandola et al., "Advances in Quantum Key Distribution," Nature Photonics, 2020.
- [13] H. Abbas et al., "Hybrid Security Models for PANs," IEEE Access, 2021.
- [14] A. Singh et al., "XOR-Based Cryptographic Protocols in IoT," Elsevier, 2022.
- [15] J. Wang et al., "Quantum-Resistant Cryptography for Healthcare Data," Springer, 2023.
- [16] P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," SIAM, 1994.
- [17] C. Bennett and G. Brassard, "BB84 Quantum Key Distribution Protocol," 1984.
- [18] F. Alotaibi et al., "Secure PANs Using Hybrid Cryptography," IEEE, 2022.
- [19] B.K. Murthy et al., "Transition to Post-Quantum Cryptography," ACM, 2022.
- [20] J. Zhu et al., "Hybrid Quantum-Classical Encryption for IoT," Elsevier, 2024.