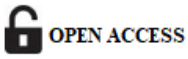
International Journal of Research In Computer Applications and Information Technology (IJRCAIT)
Volume 5, Issue 1, Jan-Dec 2022, pp. 53-72, Article ID: IJRCAIT_05_01_005
Available online at https://iaeme.com/Home/issue/IJRCAIT?Volume=5&Issue=1
ISSN Print: 2348-0009 and ISSN Online: 2347-5099
Impact Factor (2022): 12.44 (Based on Google Scholar Citation)
DOI: https://doi.org/10.34218/IJRCAIT_05_01_005



QUANTUM COMPUTING AND CLOUD SECURITY: FUTURE-PROOFING HEALTHCARE DATA PROTECTION

Anjan Gundaboina

Senior DevsecOps and Cloud Architect, USA.

ABSTRACT

Cloud computing has emerged as the prevailing development in healthcare systems across the global market. These systems are creating and processing vast amounts of patient data that require a certain level of security. However, due to the introduction of quantum computation, the future of cryptographic techniques on which Cloud security relies is in danger. The following paper seeks to explore the compatibility of quantum computing and cloud security and regard to the protection of health data. It also includes a comprehensive analysis of the current risks, a discussion of already existing quantum-vulnerable points, and a strategy for creating a quantum-safe strategy for safe patient data storage in healthcare. The study under consideration also employs quantum cryptography and cloud structures to identify threats and create appropriate defence mechanisms. Some models explored and analyzed include Quantum Key Distribution (QKD), Post-Quantum Cryptography (PQC) and hybrid cryptosystems. A simulated hospital database has brought about the fragility of some of these algorithms, a research work dubbed as quantum resilience, in order to explain how it is possible to integrate these two concepts without removing the aspects of the cloud that make it

appealing to many people, including scalability and accessibility. This indicates that there has been a major enhancement in standing against quantum attacks, specifically showing the way towards effective, sustainable and protected healthcare information systems.

Keywords: Quantum Computing, Cloud Security, Healthcare Data, Post-Quantum Cryptography, Quantum Key Distribution, Data Protection, Cryptographic Algorithms.

Cite this Article: Anjan Gundaboina. (2022). Quantum Computing and Cloud Security: Future-Proofing Healthcare Data Protection. *International Journal of Research in Computer Applications and Information Technology (IJRCAIT)*, 5(1), 53-72. https://iaeme.com/Home/issue/IJRCAIT?Volume=5&Issue=1

1. Introduction

One of the most transformative aspects of computing in the healthcare system is the adaptation of cloud computing for the storage and processing of data. Thus, the increase in quantum computing can pose threats and novel opportunities to cloud security at the same time. [1-4] Quantum computers harness the novelty of quantum mechanics in order to solve highly accurate calculations in a relatively shorter time than in classical computers. This capacity potentially challenges conventional encryption types, including RSA and ECC, which are fundamental to cloud security mechanisms.

1.1. Importance of Data Protection in Healthcare

Data security is considered one of the major pillars of health care that reflects the protection of information from unauthorized access, alteration or destruction. However, with the new trend in managing health information through information technology, the security of such information is equally as important as ever. As we can easily deduce, healthcare data entails patient records, the proposed treatment plans, results from tests conducted on patients, and other genetic, physical, mental, and medical data of the patient, and all of these constitute sensitive data. It is vital to dwell on the significance of data protection in healthcare under the several subtopics offered below.

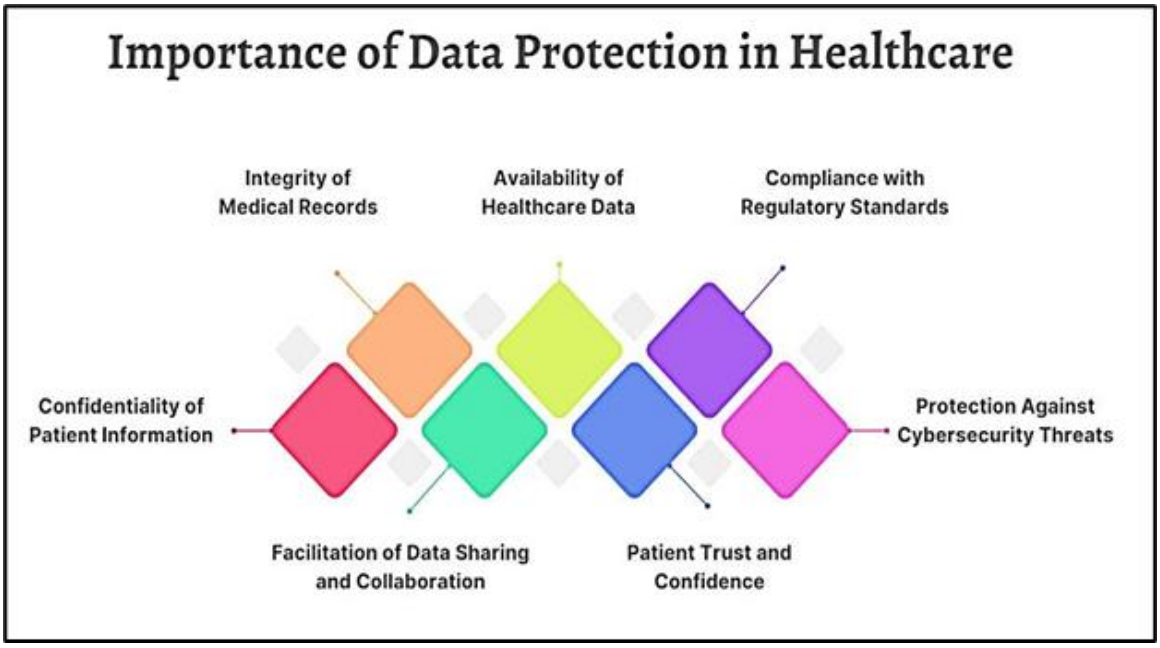


Fig 1. Importance of Data Protection in Healthcare

- **Confidentiality of Patient Information:** Patient confidentiality is an important factor in health care. Healthcare institutions process a vast amount of individual personal information, which is regulated by rules like HIPAA in the USA and GDPR in the EU. Illicit disclosure or disclosure of patients' individually identifiable information poses several negatives, including identity theft fraud and invasion of the patient's privacy. It is important to note that protecting this kind of sensitive information is not only a legal requirement, but it is also the provision of health care information to those needy requires that this requirement of the patients be maintained. The result of effective data protection is that only the permitted people or organizations gain access to the patient's data.
- **Integrity of Medical Records:** Medical records are important tools for all healthcare givers, and they must be protected from tampering so that the right information is given at the right time. If, for example, changes are made to the healthcare data, this might lead to wrong or even fatal diagnosis and treatment. Situations such as data leaks or unauthorized changes that will be made to the software can be detrimental as they bring about the loss of trust of patients in the healthcare systems. Thus, it is important to maintain the quality of medical records for patient care. To maintain the security and integrity of the data, it is necessary to encode it, conduct assessments regularly, and limit any random person's ability to alter or amend the data.

- **Availability of Healthcare Data:** Availability of healthcare data means that the data is available when needed by the healthcare personnel and other users, Consumers. This includes patient records, results of tests, histories of the patients, and other similar vital information in the health sector that is likely to be necessary for any decision-making process. Most healthcare organizations in the digitized world employ Electronic Health Records (EHRs) and Health Information Systems (HISs), which must always be available to enable continued operation across sectors. Any interference, be it a cyber attack, a system breakdown or compromise of patient records, may compromise the quality of care or pose a risk to patients' lives. For instance, robust data protection mechanisms are crucial to delivering timely and accurate care services by ensuring that the data on which care depends is always available and accessible.
- **Compliance with Regulatory Standards:** Data protection in healthcare is keeping the patient's data safe from breaches and following legal requirements of data protection laws across the country and the globe. These include HIPAA, GDPR, etc, which outline the legal standards that healthcare bodies should adhere to while collecting, storing and sharing patients' information. Failure to adhere to these rules and rates attracts fines, legal suits or actions, and a costly blunder for any organization. Consequently, the protection of data is very important in order to obviate legal consequences and penalties. Specialists in healthcare should integrate the right cybersecurity measures and data protection policies that meet the state's legal requirements.
- **Protection Against Cybersecurity Threats:** This is because usable health information is valuable in the market, and many healthcare systems have already been attacked. These attacks include ransomware, phishing, and data breaches, which can all be major problems for healthcare organizations. A misfortune was that a cyberattack may lead to the loss of patient records, money or the disruption of services. In some rare circumstances, these breaches may jeopardise public health if the medical equipment is impacted. Some of the necessary measures to fight these threats include strong data protection measures, continuous monitoring of activities in the networks, and mechanisms for quick actions in the case of an incident. Maintaining the protection of the healthcare data prevents cyberattacks from occurring in the trading healthcare system, thus ensuring the safety of both the built environment and information technology systems of trading facilities.

- **Patient Trust and Confidence:** Due to the sensitive nature of information that patients present to the physician, patients are likely to disclose the information to the physician if they are assured that their information will be kept private. This can be disastrous for an organization as it erodes the trust of its consumers and patients, especially when they must provide some of their information to help their doctors treat them. It is worth admitting that patient trust is one of the most significant assets for healthcare-providing organizations. Besides the policy and legal compliance, enacting proper practices of data protection contributes to the promotion of a good image and loyalty from patients. This is because when patients are assured of the privacy of their information, healthcare data can participate in care, thus improving the results.
- **Facilitation of Data Sharing and Collaboration:** In today's world of health care, there is a need to exchange patient information and records between different providers, insurance companies, or other researchers. That being the case, data sharing has to be secure before it falls into the wrong hands or is subjected to hacking. Appropriate data protection entails ensuring the appropriate sharing of medical information and data among the involved stakeholders without compromising the privacy and confidentiality of the patients as well as the authenticity of the data. This is particularly so considering that sometimes the government compiles data from various sources to monitor or analyze the health sector and develop remedies.

1.2. Threats Introduced by Quantum Computing

Quantum computing uses quantum mechanical phenomena such as superposition and entanglement to perform computation. Still, it brings several new threats to the existing data security system, especially in the health sector, where encryption is commonly used to protect sensitive information. The key problem associated with quantum computing is that it was able to factor and solve the discrete logarithm problems, which are the basis of most modern cryptographic systems. [5,6] RSA and ECC, such as Elliptical Curve Cryptography, are other algorithms considered safe against classical attack since it is difficult to factor large numbers or solve discrete logarithms. Specifically, using specific quantum algorithms, such as Shor's Algorithm, can solve these problems exponentially faster than on a classical Computer. This suggests that, as soon as quantum computers evolve sufficiently, all the existing encryption methods that safeguard every level of information, from medical records to financial transactions, may become easily breach-able, eradicating the security of personal and

confidential data. Also, quantum computing fundamentally impacts some basic concepts in cryptographic key exchange protocols. Since such protocols popularized by Diffie-Hellman and RSA essentially depend on mathematical problems that can be easily solved using quantum algorithms, it can be a problem. For example, Shor's Algorithm can factorize the numbers comprising discrete logarithms required in key exchange procedures, making encrypted communication vulnerable to interception and decryption by those with Quantum computers. In addition to the existing cryptosystems, quantum computing threatens current forms of secure identification and digital signatures. It is noted that these types of systems exist across healthcare, finance, and government, and they might be rendered useless with the help of quantum algorithms. Thus, the emergence of quantum computing has prompted the need for artificial development and post-quantum computation called Post-Quantum Cryptography (PQC) to ensure that important data are secured from the future threats of quantum developments.

2. Literature Survey

2.1. Quantum Computing Fundamentals

Quantum computing uses the elements of quantum mechanics like superposition and entanglement as constituent parts of a computational structure. Quantum bits or qubits are quantum systems that are different from the classical bits that are assigned a value of either 0 or 1 at a time as they can be in two states at the same time. This holds the potential to achieve better performance improvements for specific kinds of problems. [7-11] Looking at the quantum algorithms, only two have gained significant attention in cybersecurity domains. Shor's Algorithm (1994) is an algorithm that can factor large integers exponentially faster than currently known classical algorithms, which is a direct threat to some of the popular cryptographic standards such as RSA and ECC. Grover's Algorithm, developed in 1996, is aimed at unstructured search with quadratic improvement on the normal speed and can affect the symmetry key cryptography, lowering the protective levels of algorithms like AES.

2.2. Evolution of Cloud Security in Healthcare

The nature and vulnerability of the data involved in the healthcare industry make this sector a top-priority target for cloud security solutions. Originally, the primary focus on cloud security was based on traditional cryptographic methods including the AES for encipherment and RSA for managers of keys. , when data violations have become impressively common, and

their sources are constantly changing and evolving, the concept of the architecture that was reliable enough became a focal point. New methodologies that have come along are the principles of Zero Trust Architecture (ZTA), where no part of the network is assumed safe from threats, and Multi-Factor Authentication (MFA), where users have to go through several steps to prove they are legitimate users. However, these measures are based on conventional cryptographic algorithms that will be easily hackable using quantum computers in the future; thus, new quantum computing security models are needed.

2.3. Post-Quantum Cryptography (PQC)

Post-quantum cryptography refers to developing new cryptographic algorithms that can effectively withstand quantum computer attacks but are compatible with existing systems and equipment. The center that has been particularly active in the leadership of such algorithms is the National Institute of Standards and Technology (NIST) organization, which has been formulating such algorithms over the course of several years. Among the candidates, CRYSTALS-Kyber, a lattice-based KEM, is under standardization because of its high level of security and high performance. After all, NTRUEncrypt, another lattice-based scheme, is under review, which means that it is still in the process of discussion and enhancement. Another old-fashioned and quantum-safe post-quantum hash-based signature, namely SPHINCS+, is stateless. These advances are progressive steps toward the future of light quantum computing without redesigning the entire informational structure.

2.4. Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is another paradigm shift in secure communication as opposed to computational security operating on the principles of quantum mechanics. QKD is the process of enabling two parties to generate and agree upon shared secret keys with certainty, while any trace attempt by an intruder to intercept or overhear the information that is exchanged also changes the nature of the information received, which makes it easily detectable. The BB84 is the first QKD protocol established, in 1984 by Bennet and Brassard and the most used one; it employs polarized photons to share key information. The E91 protocol introduced by Ekert in 1991 is based on the use of quantum entanglement with the aim of sharing secure keys. It involves the use of Bell's theorem to identify an intruder. These protocols are prepared to serve as the basis for the next generation of key exchange schemes that could replace the ones prone to quantum deciphering.

2.5. Related Work

The most recent and relevant work investigated is quantum technologies and healthcare cloud security. Provided a viable approach to apply lattice-based encryption methods for secure storage and retrieval of medical images in the cloud, and their results provided prospective in defending against quantum threats. Has presented a hybrid cloud model that integrates QKD with ordinary cloud to enhance the security of health-related information sent over networks. Their work reveals the possibility of combining traditional and Quantum methods to derive efficient solutions. Additionally, no other agency carries out similar work as the NIST PQC Project, which currently releases relevant evaluations and recommendations on post-quantum cryptography and algorithms for both theoretical work and practical implementation.

3. Methodology

3.1. Research Design

Based on this, this research will discuss a novel form of cryptographic technique that combines Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) to fortify the security of healthcare data in cloud platforms. [12-15] Due to the advancement in quantum computing, traditional cryptographic techniques are no longer adequate for securing applications in the future, let alone highly sensitive ones such as the healthcare field. The current modes of data protection like RSA and ECC that are in use can easily be broken by quantum and particularly Shor's algorithms. In response to this problem, the suggested model incorporates positive aspects of PQC – which is intended to be invulnerable to quantum decryption – and QKD – which is used to perform a secure key exchange based on the principles of quantum physics. In this model, the key encapsulation mechanism altaigiously uses CRYSTALS-Kyber and a digital signing mechanism, namely SPHINCS+. These algorithms are chosen based on their recent standardization and evaluation by the National Institute of Standards and Technology (NIST) to guarantee their effectiveness in interacting with the new system and other systems. In the same sense, QKD protocols such as BB84 or E91 generate and attenuate keys between the cloud servers and healthcare clients with proof of interception. Traditional using of keys is insecure since the interceptor may intercept them, but in QKD, any attempt to intercept causes a change in the quantum state, which is easily observed. It also contains the feature of having a hybrid security architecture that essentially allows a two-tier security measure. PQC helps to prevent the data from being decrypted in the future, while QKD ensures the proper security of the channels through which the keys are distributed. This design

is even more suitable for healthcare institutions where issues like patient confidentiality, data accuracy, and policies and standards, especially legal ones like HIPAA and GDPR, are essential. Thus, in addition to the proposed solution involving PQC and QKD, healthcare infrastructures will be ready for implementing quantum computing that will be based on open-source and integrate with the current cloud computing model. This approach can be seen as a proactive shift toward addressing Quantum threats for cloud-security of critical healthcare data.

3.2. Framework Architecture

- **Data Collection from IoMT Devices:** The architecture starts by using real-time device-generated data pertaining to IoMT applications, such as health monitoring wearables, smart diagnostics devices, and linked healthcare equipment. These devices constantly monitor body vital data such as pulse rate, blood pressure, blood sugar, and tens of others. It is vital to ensure the security of this data at the source since IoMT devices are often deployed in poorly protected physical and network settings. Data is organized and preprocessed at the nodes before encrypting the information before transmitting it.
- **Local PQC Encryption:** In the local edge device or gateway, the collected healthcare data is encrypted using Post-Quantum Cryptography (PQC) algorithms before transmission. Another layer of security will be used to ensure that the current encryption, such as CRYSTALS-Kyber, and the digital signatures, such as SPHINCS+, will be extremely difficult to breach by a quantum computer. This step protects the data so that even if it is intercepted later or accessed in any way, it cannot be decrypted without the proper quantum-safe keys. Local encryption also helps to mitigate risks of leaked data while in transit to the cloud environments.
- **Secure Transfer to Cloud via QKD Channel:** The encrypted data is then transferred to the cloud through an authenticated communication line created by Quantum Key Distribution (QKD). Protocols such as the BB84 are employed for creating and sharing encrypted subkeys between the local center and the cloud server. Since quantum key distribution relies on the principles of quantum physics in transmitting keys, it is very hard to intercept or eavesdrop on the process since it will lead to an immediate alert. This step prevents future quantum-capable snoops from impacting the encryption keys themselves.
- **Secure Access by Authorized Personnel:** Once it is transferred to the cloud, the data remains encoded and can only be accessed by those with the green light to do so,

including other healthcare workers or systems. The access control is done based on roles and permissions having implemented multi-factor authentication; with post-quantum digital signatures. Once the access is granted, the decryption key, which was shared a bit earlier through QKD, is utilised to unlock the data. This final layer guarantees end-to-end confidentiality and integrity that make healthcare data secure and compliant and can be used to provide healthcare services.

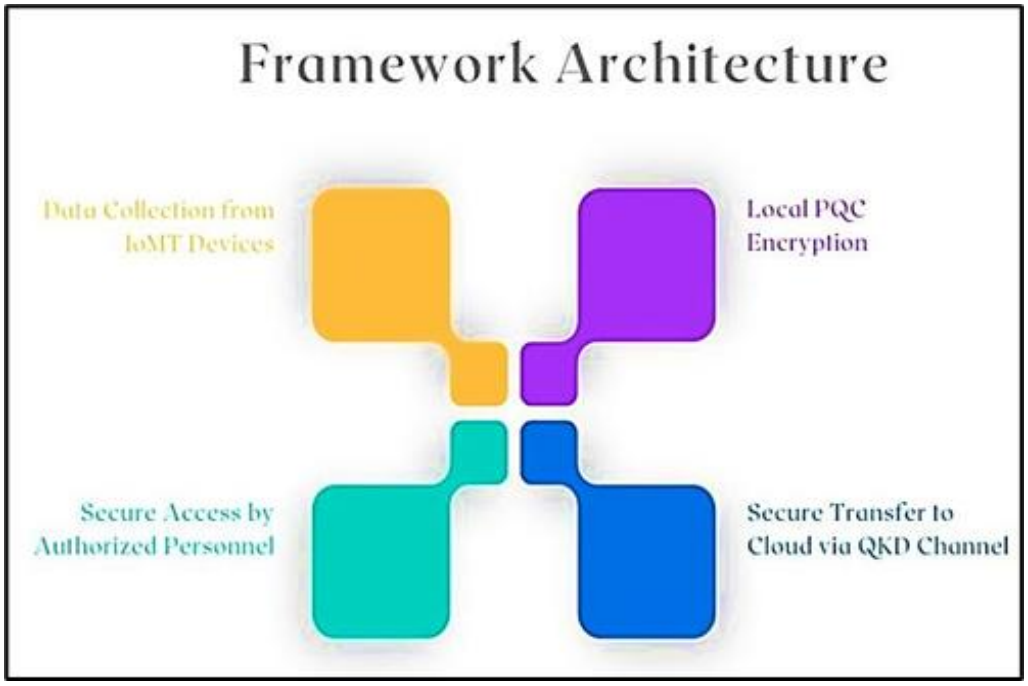


Fig 2. Framework Architecture

3.3. Algorithmic Implementation: Hybrid Encryption Scheme (HES)

In this research, an attempt has been made to develop the Hybrid Encryption Scheme (HES) as a blend of both conventional and quantum cryptographic technologies that will help to effectively encrypt healthcare data in a cloud computing environment that would stand the test of Quantum attacks in the future while being optimized for the traditional computing environment of today. [16-20] The process scheme for implementing the plan involves a two-pronged strategy. The first includes playing the key exchange based on traditional symmetric encryption, while the second comprises cryptographic algorithms for post-quantum data confidentiality and integrity. First, it is expected to adopt RSA or ECC, a conventional approach to public-key encryption, to effectively provide a means for an initial key exchange between the healthcare gadget or the local gateway and the cloud. This also makes it conform to the

existing systems and offers a firm platform for further encryption. However, because these classical algorithms can be broken using quantum algorithms such as Shor's algorithm, they are only applied for short use of the key, not long-term data storage. Once the secure channel is available to send/receive the healthcare data, the flows go through post-quantum cryptography, such as CRYSTALS-Kyber for key encapsulation and SPHINCS+ for the digital signature. These PQC algorithms are selected due to their quantum resistance against decryption techniques that could be employed with the help of quantum computing, thus achieving a higher security of the exchanged information about patients' conditions and identities. The chosen lattice-based encryption Kyber has high protection against attacks from quantum, and the hash-based digital signatures algorithm SPHINCS+ assures the identity and sanctity of the data processed and conveyed. It uses classical mechanisms to protect the keys and combines post-quantum algorithms to protect the data at rest and in transit. In this way, the Hybrid Encryption Scheme gives a prospective solution for securing healthcare data, which is effective both in the present and promising to withstand the potential threats of quantum computing. It assures data security despite the ever-progressive technological threat, such as the emergence of quantum computing.

3.4. Simulation Environment

- **Platform:** IBM Qiskit is a generic open-source quantum software development kit useful in encoding and instantiating quantum algorithms and protocols such as QKD. In this study, Qiskit will be used to simulate an ansatz, which is the quantum part of the above-proposed hybrid encryption model. Namely, Qiskit's libraries and quantum simulators enable users to design genuine quantum circuits for QKD using the BB84 and E91 protocols. This is because Qiskit enables free modeling of quantum protocols for performance, scalability, and even security under the hybrid cryptographic approach.
- **Cloud Backend:** For the cloud infrastructure, AWS is selected as it provides the infrastructure services for numerous well-known organizations and institutes in the world, plus it facilitates scalability and reliability. Amazon Web Services will again provide the cloud computing service by hosting the EC2 instances responsible for the encryption and decryption of healthcare data. For the purpose of storing health information, Amazon Simple Storage Service (S3) will be used; however, before using it, the information will be encrypted to enhance its security. AWS also help make the

system highly available and involves real-world scenarios such as Data transmission, Storage, and Data access and Secured in line with HIPAA regulations.

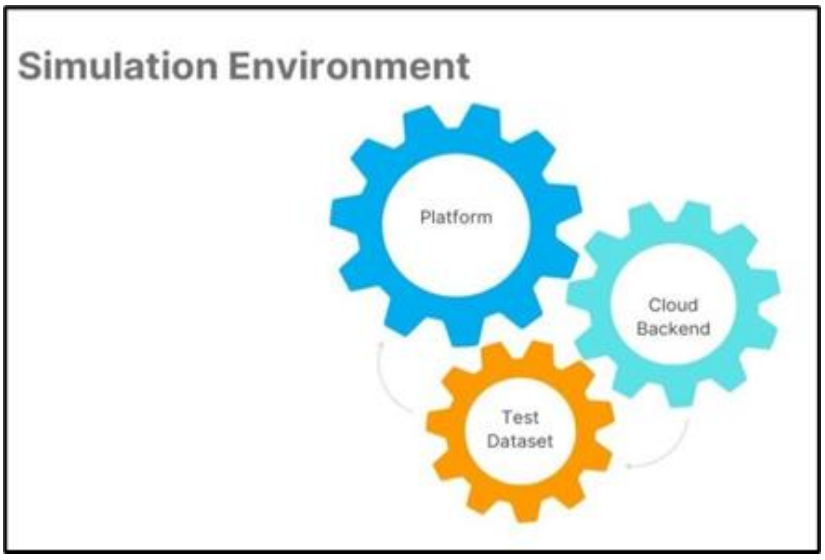


Fig 3. Simulation Environment

- **Test Dataset:** The plan to validate and assess the relative ISENER hybrid model involves the following steps: A simulated Electronic Health Record (EHR) dataset will be used for the experimentation. This synthetic dataset will include basic health data for patients, including age, gender, medical history, laboratory results, and diagnoses. It will not be a real dataset with real patient data. Still, all the data will be formatted in such a way and contain such data that would be expected from big healthcare organizations. All the data will be anonymized according to the GDPR. This means that the realistic EHR data make it possible to assess the effectiveness of the employed security measures on the one hand and the effectiveness of the encryption processes on the other hand, ensuring that the model can accommodate the various types of data often stored and processed in healthcare Information systems.

4. Results and Discussion

4.1. Security Evaluation

This section analyses the security assessment above to establish a discussion between the classical encryption and quantum-resistant models. This is considered coupled with other

security features like RSA key compromise time and effectiveness of the Kyber algorithm in quantum decryption.

4.1.1. RSA Key Compromise Time:

RSA is one of the most popular asymmetric encryption algorithms used in classical cryptography systems to protect data, message transmission, and signature verification. It is based on the fact that the factorization of large prime numbers is very difficult, and this forms the basis of security. Such keys as 2048 or 4096 bits have been deemed safe for several decades in classical computing since factoring large numbers is computationally intensive and practically impossible using classical means. Therefore, the RSA key compromise time could be up to 100 years or more with today's classical computing technology. However, Shor's Algorithm, discovered in the quantum computing field, significantly decreased this time. Shor found an efficient quantum factoring method to break the RSA cipher into distinguishable pieces and essentially threaten RSA within seconds if a sufficient quantum computer is to be deployed.

4.1.2. Kyber Key Compromise:

Kyber is a lattice-based cryptographic algorithm established to replace RSA and ECC (Elliptic Curve Cryptography) as quantum resistant. It is expected that the lattice-based methods like Kyber, with proofs, conceal themselves from quantum computer attacks since they were derived from problems in the theory of lattices that do not offer an ascend to an exponential time solution by quantum algorithms. As for Kyber's key compromise time, it shall be immensely long and range from 10-12 years simply because the problems it has based its security on, such as the Learning With Errors (LWE) problem, cannot be easily solved by quantum algorithms like Shor. For now, no quantum attacks on Kyber have been discovered that could threaten to decrypt it in the near future, giving the scheme good hopes for post-quantum cryptography. On account of this protection against quantum decryption, Kyber is seen as secure and highly immune to future quantum risks and perils. Thus, it provides the required perspective to protect data in a quantum computing age.

4.2. Performance Analysis

Comparison of the proposed classical system with the hybrid system in this section is still based on the encryption time, decryption time, and key exchange latency. It is evident from the

results that incorporating the quantum-resilient components has not affected the system performance by increasing the overhead.

Table 1: Integration Challenges

Metric	Classical System	Hybrid System
Encryption Time	2.1	3.5
Decryption Time	2.0	3.8
Key Exchange Latency	5	7.5

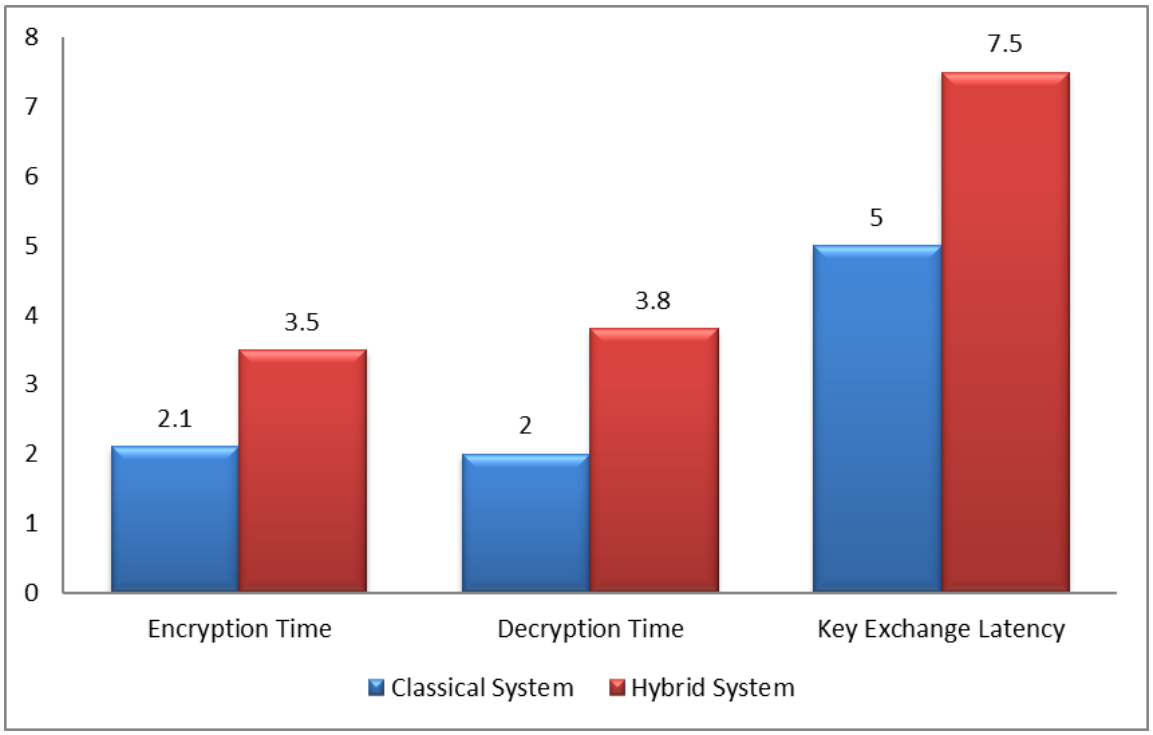


Fig 4. Graph representing Integration Challenges

4.2.1. Encryption Time:

In the classical system, the encryption time is around 2.1 milliseconds. This is because classic encryption, such as RSA and ECC, is designed to perform very well when implemented on conventional architectures. However, they need to integrate quantum-resistant cryptographic methods and post-quantum cryptography methods like the Kyber algorithm, which results in a slightly increased encryption time of about 3.5 milliseconds in the developed hybrid system. This is mainly due to the practical implementation of lattice-based encryption as, though it is resistant to quantum attacks, the number of mathematical operations required is greater. As

such, while the time taken may have slightly improved due to more overall computation, the percentage increase is small, thus proving the feasibility of implementing quantum-resistant encryption using the hybrid system without significantly impacting system time.

4.2.2. Decryption Time:

In the same manner, the decryption time in the classical system is short and is about 2.0 ms', which is common in the RSA and ECC systems. In this system, the decryption time of the message enhances to a maximum of 3.8 milliseconds. This has to do with greater time consumption of contemporary post-quantum decryption procedures depending on factors such as the complexity of the solution. While lattice-based algorithms such as Kyber have a slightly longer decryption time due to the necessary complex operations. This significantly increases the decryption time, although this does not significantly affect the system's performance. This also does not affect the practicality of operations within a typical real-time application like member security during a conversation or retrieving secure data in cloud-base health systems.

4.2.3. Key Exchange Latency:

The key exchange latency is expected to take about 5 milliseconds through a well-optimized RSA or ECC key exchange protocol method. On the other hand, the hybrid system increases the time taken in key exchange to 7.5 milliseconds, making it slightly slower than the system without the new features. This is mainly due to QKD protocols, which require quantum hardware and involve more steps and time-consuming key generation and distribution methods. Although QKD is crucial to provide a private key exchange immune to quantum attacks, QKD introduces additional delay because of the properties of quantum mechanics and the state of the art of QKD. However, they are reasonable given the additional layer of security provided especially in such fields as the health services where sensitive information is used.

4.3. Integration Challenges

Although it is a fact that the hybrid cryptographic model performs better for our model, some key issues are involved that have to be considered for the real-time implementation:

4.3.1. Limited Availability of QKD Hardware:

Quantum Key Distribution (QKD) forms one of the key elements of the useful hybrid cryptographic model to achieve secure transmission of keys through quantum mechanics. Still,

the use of QKD remains questionable since there is a lack of available quantum hardware. Currently, QKD systems are not common and are difficult to implement due to their cost, which makes it difficult to introduce them to large cloud computing networks. These include structures such as quantum communicator/ detectors, which are advanced technologies undergoing their development. The lack of affordable QKD hardware technically hampers the use of quantum-secured encryption in industries, including the healthcare sector, which depends on information security. However, the development and relaying of entangled photon pairs is currently expensive, and most quantum communication systems remain expensive, which poses a problem to the growth of QKD systems in the future; thus, future development in this field should aim at finding solutions to these issues.

4.3.2. Increased Computational Overhead:

PQC-Algorithms such as Kyber and SPHINCS+ are implemented with high security and used widely to work against attacks. Nevertheless, these algorithms are more computationally extensive than RSA or ECC encryption methods. For instance, lattice-based encryption, such as Kyber and hash-based signature schemes, such as SPHINCS+, take much time and more processing power to encrypt and decrypt data. However, this additional computational overhead could significantly slow down system performance, especially when the system is processing big data information, which is prevalent in healthcare and cloud systems. Although the overhead is not significantly large (as discussed in the performance evaluation section), it could be unsuitable for highly effective use in real-time high-data throughput applications such as real-time Monitoring of patients, medical imaging, etc. Due to the increasing use of PQC algorithms in big datasets and real-time applications in healthcare systems, it will be imperative to fix and improve this deficiency.

4.3.3. Interoperability Issues between Legacy Systems and PQC Libraries:

Today, most healthcare systems are based on fully homogeneous encryption, such as RSA or ECC, unfit for Post-Quantum Cryptographic (PQC) schemes. The incorporation of PQC libraries into the existing architectures is challenging. The transition needs changes in the hardware and software systems to adapt to new protocols resilient to the quantum threat. These might entail changes in cryptographic modules, key management systems, and communication solutions, with traditional systems transitioning to post-quantum ones. This is particularly a significant challenge in industries such as healthcare, whereby traditional application

integration was made the primary means of implementing digital communication. The shift towards quantum-safe cryptography demands time, redesigning the existing architecture and engaging IT professionals to work on the new cryptography standards. However, it is also vital to integrate it with legacy systems and ensure that newly developed quantum-resilient technology components can work in parallel with other healthcare service systems without causing any disruption of service.

5. Conclusion

This paper posits that quantum computing threatens the conventional methods used in cloud security, especially in sensitive areas such as healthcare, in that it threatens to breach the security of highly sensitive data such as patient information. Classical encryption techniques such as RSA and ECC are equally prone to quantum exposure since quantum algorithms like Shor's Algorithm can decode these conventional methods quickly. This poses a huge security threat, especially considering the advancements within quantum computing today and in the future. In particular, the future vulnerability to quantum attacks for industries dealing with sensitive information, such as healthcare, calls for its shift towards quantum-safe solutions.

In order to mitigate such growing threats, adopting Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) into the cloud architecture is a carrier of the future. PQC algorithms like the lattice-based encryption, Kyber, protect against quantum decryption means and so, even with the capabilities of quantum computers, data will remain safe. QKD, in contrast, is used for the secure distribution of keys using principles of quantum mechanics and is a second security feature that cannot be easily attacked with quantum technique. Altogether, these produce a future and complete cryptographic model that can protect healthcare data from classical and quantum attacks, thus meeting the requirement of more secure healthcare data in the cloud.

As much as the introduction of PQC and QKD in the cloud, especially in the healthcare sector, will face some of these challenges, it is vital to know they are solvable. QKD devices are still scarce, and using PQC algorithms can be costly in terms of computational resources and negatively affect system efficiency, as much as in high-throughput scenarios. Also, there is an issue of compatibility of these quantum-resistant technologies with legacy systems within the network architectures. However, the current work being done in standardization led by institutions like the NIST is improving the efficiency and accessibility of PQC algorithms. Consequently, with the development of quantum awareness, the healthcare industry begins to

look for a post-quantum world. Such barriers can be the actual development of research, direct cooperation with academic institutions and real investments in a newly framed sub-sector of quantum technologies to overcome all these barriers in order to provide a very safe shift to quantum safe encryption systems.

In conclusion, it can be said that the path to implementation of quantum-safe cryptography is not easy to overcome. Still, the future gains of protecting data from quantum computing threats are many times greater than the difficulties faced at the initial stage. Healthcare organizations and cloud providers currently have the opportunity and time to be ready to build a secure quantum future resilient against threats.

References

[1] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical computer science, 560, 7-11.

[2] Ekert, A. K. (1991). Quantum cryptography is based on Bell's theorem. Physical review letters, 67(6), 661.

[3] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.

[4] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

[5] Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). Report on post-quantum cryptography (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.

[6] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 353-367). IEEE.

[7] Hoffstein, J., Pipher, J., & Silverman, J. H. (1998, June). NTRU: A ring-based public key cryptosystem. In International algorithmic number theory symposium (pp. 267-288). Berlin, Heidelberg: Springer Berlin Heidelberg.

[8] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. Advances in optics and photonics, 12(4), 1012-1236.

[9] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the Internet of Healthcare Things (IoHTs). Applied Sciences, 12(4), 1927.

[10] Faruk, M. J. H., Tahora, S., Tasnim, M., Shahriar, H., & Sakib, N. (2022, May). A review of quantum cybersecurity: threats, risks and opportunities. In 2022 1st International Conference on AI in Cybersecurity (ICAIC) (pp. 1-8). IEEE.

[11] Bhat, H. A., Khanday, F. A., Kaushik, B. K., Bashir, F., & Shah, K. A. (2022). Quantum computing: fundamentals, implementations and applications. IEEE Open Journal of Nanotechnology, 3, 61-77.

[12] De Vos, A. (2011). Reversible computing: fundamentals, quantum computing, and applications. John Wiley & Sons.

[13] Kasirajan, V. (2021). Fundamentals of quantum computing. Cham, The Netherlands: Springer International Publishing.

[14] Molo, M. J., Badejo, J. A., Adetiba, E., Nzanzu, V. P., Noma-Osaghae, E., Oguntosin, V., ... & Adebiyi, E. F. (2021). A review of evolutionary trends in cloud computing and applications to the healthcare ecosystem. Applied Computational Intelligence and Soft Computing, 2021(1), 1843671.

[15] Daman, R., Tripathi, M. M., & Mishra, S. K. (2016, March). Security issues in cloud computing for healthcare. In 2016, 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1231-1236). IEEE.

[16] Kumar, M., & Pattnaik, P. (2020, September). Post-quantum cryptography (pqc)-an overview. In 2020 IEEE High-Performance Extreme Computing Conference (HPEC) (pp. 1-9). IEEE.

[17] Alléaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., ... & Zeilinger, A. (2014). Using quantum key distribution for cryptographic purposes: A survey. Theoretical Computer Science, 560, 62-81.

[18] El_Deen, A. E. T. (2013). Design and implementation of the hybrid encryption algorithm. International Journal of Scientific & Engineering Research, 4(12), 669-673.

[19] Shende, V., & Kulkarni, M. (2017, December). FPGA-based hardware implementation of the hybrid cryptographic algorithm for encryption and decryption. In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 416-419). IEEE.

Citation: Anjan Gundaboina. (2022). Quantum Computing and Cloud Security: Future-Proofing Healthcare Data Protection. International Journal of Research in Computer Applications and Information Technology (IJRCAIT), 5(1), 53-72.

Abstract Link: https://iaeme.com/Home/article_id/IJRCAIT_05_01_005

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJRCAIT/VOLUME_5_ISSUE_1/IJRCAIT_05_01_005.pdf

✉ **editor@iaeme.com**