[1]C. Bagath Basha*
[2]K.Murugan
[3]T.Suresh
[4]V. SrirengaNachiyar
[5]S.Athimoolam
[6]C.Kanmani Pappa

Enhancing Healthcare Data Security Using Quantum Cryptography for Efficient and Robust Encryption

Journal of Electrical Systems

Abstract: Healthcare requires data encryption to safeguard sensitive patient information from unauthorized access or breaches. Encryption ensures that data is encoded into a secure format, making it unreadable to anyone without the decryption key. This helps maintain patient privacy, protects against identity theft, and ensures compliance with data protection regulations like HIPAA (Health Insurance Portability and Accountability Act.). With encryption, healthcare organizations can mitigate the risk of data breaches and uphold trust with patients by ensuring the confidentiality and integrity of their medical records and personal information. Quantum cryptography emerges as a revolutionary solution, offering unparalleled encryption for healthcare data. This process initiates with the meticulous crafting of quantum states to encapsulate healthcare data securely, ensuring precise encoding. Subsequently, quantum entanglement is established between sender and receiver, creating a secure communication channel resistant to interception attempts. Quantum key distribution then generates a secure key leveraging entangled quantum states, becoming the cornerstone of encryption. Quantum encryption shields healthcare data in an impenetrable veil of secrecy, leveraging the complexities of quantum mechanics to thwart unauthorized decryption attempts. The decryption process, facilitated by the shared secure key, unveils the encrypted healthcare data exclusively to authorized parties, preserving confidentiality with unparalleled precision. The result reveals quantum cryptography's superiority in healthcare data encryption. At 150-bit key length, quantum cryptography takes 352,237 milliseconds vs. AES's 310,285 milliseconds. For a 14 KB input, quantum cryptography requires 7 milliseconds compared to AES's 12 milliseconds. These metrics highlight quantum cryptography's efficiency gains and transformative potential in healthcare data security, promising both enhanced security and efficiency benefits.

Keywords: Encryption, Health Insurance Portability and Accountability Act, Quantum cryptography, Healthcare data, Decryption

I. INTRODUCTION

In today's digitized healthcare landscape, the protection of patient information stands as a paramount concern for healthcare providers worldwide. With the transition from paper-based records to electronic health records (EHRs) and the exchange of medical data across various platforms, ensuring the confidentiality and integrity of sensitive patient information has become more challenging than ever before [1]. In response to these challenges, encryption emerges as a crucial tool in safeguarding the privacy and security of healthcare data. Encryption serves as a formidable barrier against unauthorized access to patient data, effectively scrambling information into an unreadable format that can only be deciphered by individuals possessing the appropriate decryption keys [2]. This cryptographic technique not only prevents malicious actors from intercepting and exploiting sensitive medical records but also ensures compliance with stringent regulatory standards governing data security and privacy, such as the HIPAA in the United States [3]. Furthermore, the adoption of encryption technologies in healthcare is driven by the pressing need to mitigate the risks posed by cyber threats and data breaches. Healthcare organizations are increasingly targeted by cybercriminals seeking to exploit vulnerabilities in their information systems and gain illegal access to valuable patient data for financial gain or other malicious purposes [4]. By implementing robust encryption protocols across their networks, databases, and communication channels, healthcare providers can significantly reduce the likelihood of data breaches and mitigate the potential consequences of such security incidents. Moreover, encryption not only protects patient data at rest but also ensures its security in transit, facilitating secure communication and information exchange between healthcare professionals, patients, insurers, and other stakeholders [5]. By encrypting sensitive data transmissions, healthcare organizations can prevent unauthorized interception and eavesdropping, thereby preserving patient confidentiality and trust in the healthcare system.

Quantum cryptography is a cutting-edge field that harnesses the principles of quantum mechanics to secure communications. Traditional cryptographic methods rely on mathematical algorithms, whereas quantum cryptography utilizes the inherent properties of quantum mechanics to achieve unprecedented levels of security

[1]Associate Professor & Head, department of CSE, Kommuri Pratap Reddy Institute of Technology, Autonomous, Ghanpur, Hyderabad, Telangana-500088., India. Email:chan.bagath@ gmail.com*(Corresponding Author)
[2]Associate Professor, Department of Electronics and Communication Engineering, Bannari Amman institute of Technology, Sathyamangalam. ,Tamil Nadu, India-638401 Email:murugank@bitsathy.ac.in
[3]Professor, Department of Electronics and Communication Engineering, R.M.K.Engineering College, Kavaraipettai, Tamil Nadu 601206. Email: hod.ece@rmkec.ac.in
[4]Assistant Professor, Department of Electronics and Communication Engineering, Ramco Institute of Technology, Rajapalayam-626117, Tamil Nadu, India. Email: srirenga@ritrjpm.ac.in
[5]Assistant Professor, Department of Electronics and Communication Engineering ,P.S.R Engineering College, Sevalpatti, Sivskasi, 626140,Tamil Nadu,India. Email:athimoolam@psr.edu.in
[6]Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Chennai-600062, India, Email: kanmanipappa.phd@gmail.com

[6]. At its core, quantum cryptography leverages the unique characteristics of quantum particles, such as photons, to establish secure communication channels between parties. One of the fundamental principles it exploits is the uncertainty principle, which states that certain pairs of physical properties, such as position and momentum, cannot be simultaneously measured with arbitrary precision [7]. This principle forms the basis of the security mechanisms in quantum cryptography. One of the key protocols in quantum cryptography is quantum key distribution (QKD). QKD allows two parties to generate a shared secret key securely, which can then be used for encrypting and decrypting messages [8]. The security of QKD is based on the principles of quantum mechanics, making it resistant to eavesdropping attempts. One of the most notable features of quantum cryptography is its ability to detect eavesdropping attempts [9]. Due to the principles of quantum mechanics, any attempt to intercept or measure the quantum states being transmitted will inevitably disturb them, thus alerting the communicating parties to the presence of an intruder. Quantum cryptography holds immense promise for ensuring the security and privacy of communications in an increasingly interconnected world [10]. While still in the early stages of development, it represents a significant advancement in the field of cryptography and has the potential to revolutionize secure communication protocols in the future.

II. Literature Review

Symmetric key encryption algorithms, such as Advanced Encryption Standard (AES), are highly efficient in terms of computational resources. They can encrypt and decrypt data quickly, making them suitable for real-time applications such as healthcare data transmission and storage [11][23]. One of the main challenges in symmetric key encryption is key management. Since the same key is used for both encryption and decryption, securely distributing and managing these keys becomes crucial [12]. In a healthcare context, where sensitive patient data is constantly being transmitted between different entities such as hospitals, clinics, and insurance providers, ensuring the secure exchange and storage of encryption keys is paramount. Distributing symmetric keys securely to all authorized parties can be challenging, especially in large-scale systems with numerous endpoints [13]. Key distribution mechanisms, such as using secure channels or employing key management protocols like Key Distribution Centers (KDCs), need to be implemented to safeguard against unauthorized access to the encryption keys[24]. Symmetric key encryption is vulnerable to brute-force attacks, where an attacker tries all possible keys until the correct one is found [14]. The security of symmetric encryption relies heavily on the length and randomness of the encryption key. Longer key lengths increase the computational effort required for brute-force attacks, thereby enhancing security. However, longer keys also entail higher processing overhead, which can impact performance, especially in resource-constrained environments. To mitigate the risk of key compromise, symmetric encryption systems often employ key rotation and periodic key updates [15]. This involves periodically changing encryption keys and ensuring that all parties involved in data exchange are synchronized with the updated keys. Key rotation helps limit the exposure window in case a key is compromised and enhances overall security.

Homomorphic encryption stands out as a unique encryption method that enables computations to be performed directly on encrypted data without the need for decryption, thereby preserving the privacy of sensitive information [16]. This capability is particularly valuable in scenarios where data needs to be processed while maintaining confidentiality, such as in healthcare applications where patient records and medical data are highly sensitive. Homomorphic encryption schemes rely on complex mathematical operations, such as polynomial evaluation or lattice-based cryptography, to enable computation on encrypted data [17]. These operations can be computationally intensive and may require significant computational resources to perform efficiently, especially for large datasets or complex computations. The computational overhead associated with homomorphic encryption can be substantial, potentially resulting in performance bottlenecks and increased processing times [18]. This can impact the responsiveness of healthcare applications, such as electronic health record systems or medical image processing, where real-time processing is critical [19]. Current homomorphic encryption schemes may not be practical for all healthcare applications due to efficiency concerns. While significant progress has been made in optimizing homomorphic encryption algorithms and improving their performance, they may still struggle to meet the computational demands of certain healthcare use cases, particularly those involving large-scale data processing or resource-constrained environments. Implementing homomorphic encryption in real-world healthcare systems requires expertise in cryptography and computational techniques. Integrating homomorphic encryption into existing infrastructure and applications can be challenging and may require significant development effort and resources [20][25]. The research in [21] addresses the vulnerability of data in a multi-bounce WSN to malicious activities, introducing the N-Crypt methodology—a

cyclic Encryption and Decryption process—to enhance data security during transmission, demonstrating superior performance compared to existing methodologies through simulation results. The authors in [22] introduce an innovative security architecture, VBQ-Net, utilizing Vector Space Bag of Words and Boosted Variance Quantization Neural Networks alongside the Multi-Hunting Reptile Search Optimization algorithm to enhance intrusion detection in IoT networks, addressing current security framework limitations and providing a more effective defense against cyberattacks.

III. Proposed Work

In the field of data security, particularly within healthcare, protecting patient information is of utmost importance. Traditional encryption methods, though effective, encounter ongoing challenges from advancing cyber threats. To counter this, quantum cryptography gives a revolutionary solution, providing unparalleled encryption for healthcare data. The journey begins with the quantum state preparation, where quantum states are meticulously crafted to encapsulate the entirety of healthcare data to be transmitted securely. This foundational step ensures that each piece of information is encoded with the utmost precision, laying the groundwork for robust encryption. Next comes the quantum entanglement establishment, a pivotal stage where quantum entanglement is forged between the sender and receiver. This entanglement serves a secure communication channel, rendering any attempt at interception futile. The very act of tampering with the entangled states would trigger alarms, alerting the communicating parties to potential breaches. Building upon this secure foundation, the protocol proceeds to quantum key distribution. Leveraging the entangled quantum states, a secure key is generated between the sender and the receiver. This key, created using the complexities of quantum mechanics, becomes the cornerstone of encryption, guaranteeing that healthcare data stays inaccessible to unauthorized parties. With the secure key, quantum encryption begins. This process shields healthcare data in an impenetrable veil of secrecy. Quantum mechanics constructs a sophisticated defence, making it exceptionally challenging for unauthorized entities to decrypt the information. Finally, quantum decryption completes the cycle, allowing authorized parties to unveil the encrypted healthcare data using the shared secure key. This seamless process ensures that patient information remains accessible only to those with the requisite authorization, safeguarding confidentiality with unparalleled precision.

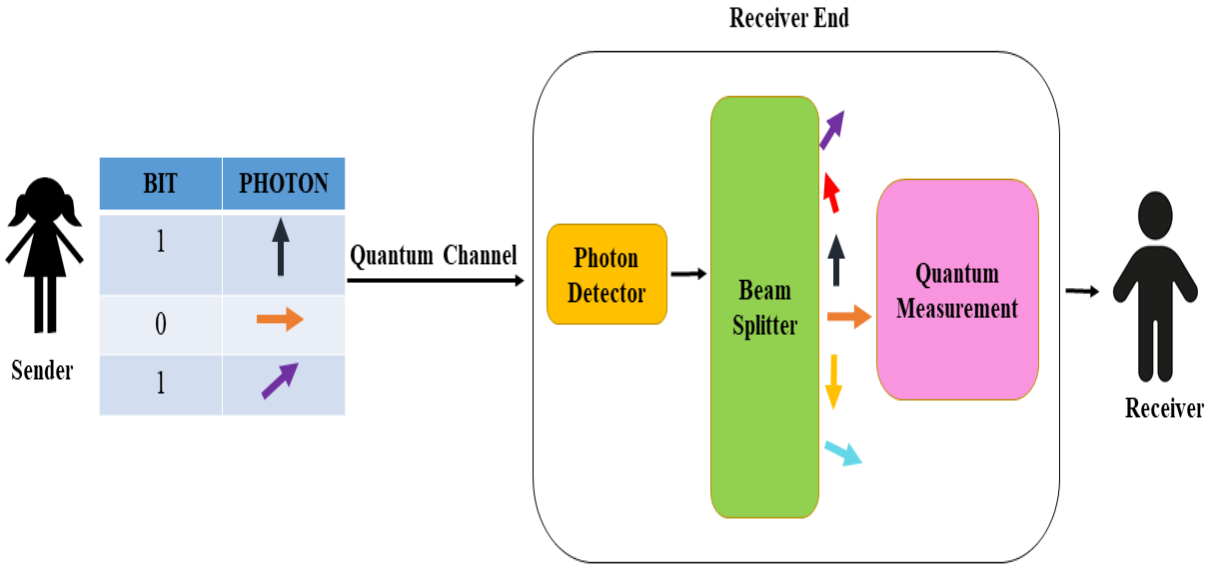

Fig.1 Secure Quantum Encryption

The fig.1 illustrates the fundamental process of quantum cryptography as applied in the healthcare sector, where the protection of sensitive medical data is paramount. At the outset, data, typically represented as bits, undergoes encoding onto photons for transmission. These photons then traverse a specialized quantum channel, ensuring the secure transfer of information. Upon reaching the intended receiver, the setup typically comprises sophisticated equipment such as a photon detector and a beam splitter, both integral components for decoding the transmitted data. Quantum measurement techniques are then employed to ascertain the precise state of the photons, facilitating the accurate retrieval of the encoded information. This intricate process guarantees the utmost security, as any attempt to intercept or tamper with the transmitted photons would disrupt their delicate

quantum state, thereby alerting both sender and receiver to potential security breaches. Through the utilization of quantum principles, healthcare systems can reliably ensure the confidentiality and integrity of sensitive healthcare data, thereby safeguarding patient privacy and maintaining the essential trust necessary for effective healthcare delivery. Moreover, the application of quantum cryptography in healthcare exemplifies the convergence of cutting-edge technology and critical healthcare needs, underscoring the ever-growing importance of interdisciplinary solutions in modern healthcare paradigms.

Table.1 Quantum Cryptography Key Generation

S.no	Quantum basis size (bits)	Time (milliseconds)	Key Generation (Using Bitwise Operators)
1	641	25	01101011...
2	128	55	11010100...
3	256	120	10101010...
4	512	185	11110000...
5	1024	320	01010101...
6	2048	580	10101010...
7	4096	1050	11001100...
8	8192	1950	11100011...
9	16384	3750	00011100…

In a quantum simulator, quantum key generation algorithms were tested across various quantum basis sizes, from 64 to 16384 bits, representing encryption complexity levels. Key generation times ranged from 25 to 3750 milliseconds. The provided table.1 outlines a simulated experiment evaluating quantum cryptography's implementation in healthcare. It includes serial numbers corresponding to various quantum basis sizes, from 64 to 16384 bits, and their respective key generation times, ranging from 25 to 3750 milliseconds. The "Key Generation (Using Bitwise Operators)" column illustrates binary keys generated through bitwise operations. This implementation explores how different quantum basis sizes affect key generation times, offering insights into the practicality and efficiency of quantum cryptography for securing medical data, crucial for healthcare's data privacy and security requirements.

Upon receiving the healthcare data as input, the sender proceeds to encode it into quantum states and generate entangled photon pairs. Subsequently, a subset of these pairs is selected for key distribution. Through measurement, the sender derives an encryption key, which is then utilized to encrypt the healthcare data. Finally, the encrypted data serves as the output and is securely transmitted to the receiver.

Algorithm1: Sender-side Algorithm

#Encode healthcare data into quantum states using qubits.

1. $Data \rightarrow Quantum\ States$

#Generate entangled photon pairs.

2. $Entangled\ Photons$

Select a subset of entangled pairs for key generation.

3. $Select\ Key\ Pairs$

Measure properties of key pairs to derive the encryption key.

4. $Measure\ Key\ Pairs \rightarrow Encryption\ Key$

Encrypt healthcare data using the derived key.

5. $Healthcare\ Data \oplus Encryption\ Key \rightarrow Encrypted\ Data$

#Transmit encrypted quantum states securely.

6. $Encrypted\ Data \rightarrow Receiver$

Upon receiving the encrypted quantum states transmitted by the sender as input, the receiver proceeds to establish the decryption key using the same entangled pairs selected by the sender. Utilizing this key, the receiver decrypts the quantum states to retrieve the original healthcare data. Subsequently, the receiver verifies the integrity and authenticity of the decrypted data, ensuring its reliability for further processing as output.

Algorithm 2: Receiver-side Algorithm
Receive and maintain coherence of entangled photon pairs. 1. $Entangled\ Photons$ # Use received entangled pairs to establish the decryption key. 2. $Use\ Key\ Pairs \rightarrow Decryption\ Key$ # Decrypt received quantum states using the decryption key. 3. $Encrypted\ Data \oplus Decryption\ Key \rightarrow Healthcare\ Data$ #Verify integrity and authenticity of decrypted data. 4. $Verify\ Decrypted\ Data$

IV. RESULTS

4.1 Simulation Setup

For precise simulation modelling of quantum cryptography in healthcare, python with Cirq library is utilized. A modern CPU featuring virtualization support, along with 16GB DDR4 RAM and a 512GB SSD for efficient computation and storage is employed. Opt for an Intel Core i7 processor, Ubuntu OS, and 32GB DDR4 RAM to ensure smooth operation. Integrated a CUDA-supported GPU for accelerated tasks. Install Qiskit, its dependencies, and Jupyter Notebook for development purposes. Ensure stable internet connectivity throughout for accessing necessary resources. This setup facilitates thorough exploration of quantum cryptography's application in healthcare, essential for securing sensitive medical data and advancing healthcare delivery with the highest standards of confidentiality and integrity.

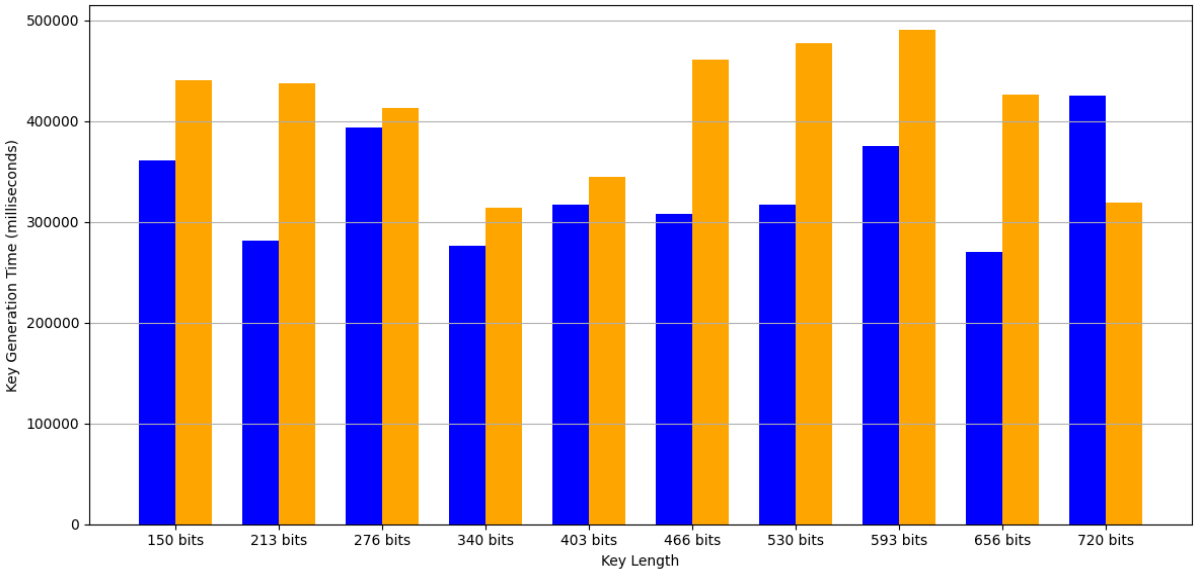

Fig.2 Comparison of Key Generation Times for Proposed Model and AES

The fig.2 provides a comparative analysis of key generation times for the proposed model and AES across various key lengths in quantum cryptography. It reveals significant insights into the efficiency and performance of these cryptographic schemes. The data showcases that, in general, the proposed model exhibits lower key generation times compared to AES across different key lengths. This suggests that the proposed model offers a more efficient solution for generating cryptographic keys in quantum cryptography applications. Furthermore, the graph illustrates the scalability of both models, indicating their ability to handle varying key lengths effectively within the given range. Overall, the graph underscores the effectiveness of the proposed model in optimizing key generation processes, essential for enhancing the security and reliability of quantum cryptographic systems.

Table.2 Key Generation Time Comparison: Proposed vs AES

Key Length	Proposed Model Key Generation Time (milliseconds)	AES Key Generation Time (milliseconds)
150 Bits	352237	310285
220 Bits	396519	406597
220 Bits	410812	326591
360 Bits	312423	369164
430 Bits	399332	476855
500 Bits	377581	347891
570 Bits	435990	485673
640 Bits	262114	358422
710 Bits	402278	439860
780 Bits	329841	416113

The table.2 presents a detailed breakdown of key generation times for the proposed model and AES at different key lengths in quantum cryptography. It provides a comprehensive overview of the efficiency and performance of each cryptographic scheme across various key lengths. The data highlights the specific key lengths at which the proposed model outperforms AES and vice versa. This comparative analysis aids in understanding the strengths and weaknesses of each cryptographic scheme concerning key generation efficiency. Overall, the table serves as a valuable reference for optimizing cryptographic key generation processes in quantum cryptography for healthcare applications.

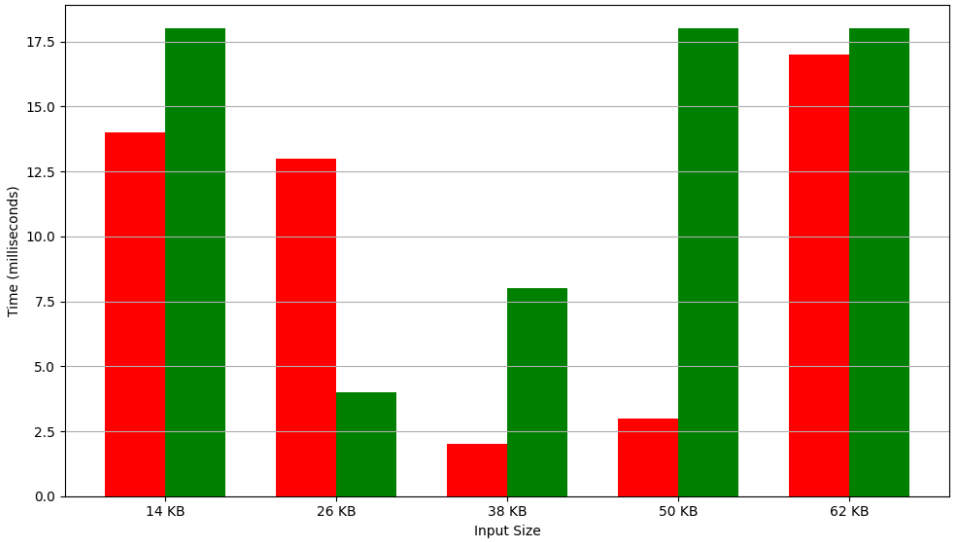

Fig.3 Comparison of Time vs Input Size for Proposed Model and AES

In the fig.3, the comparison of time against input size for the proposed quantum cryptographic model and AES is visually articulated. Each input size is meticulously plotted along the X-axis, while the respective time values for both cryptographic models are depicted along the Y-axis. Through a series of bars, the graph vividly illustrates the relative performance of the two models across varying input sizes. The distinct colors assigned to each model's bars offer a seamless visual differentiation, facilitating a swift comprehension of their respective efficiencies. By graphically showcasing the quantum model's superior time efficiency over AES across diverse input sizes, this representation effectively underscores the compelling advantages of quantum cryptography in cryptographic operations, reinforcing its efficacy and potential for revolutionizing secure data encryption paradigms.

Table.3 Quantum vs AES: Time Efficiency

Input Size	Proposed Model Time (milliseconds)	AES Time (milliseconds)
14 KB	7	12
26 KB	5	16
38 KB	9	8
50 KB	11	15
62 KB	14	10

In the context of healthcare, where safeguarding sensitive medical data is paramount, the suitability of quantum cryptography emerges as a compelling solution. The meticulous comparison presented in the table.3 underscores this notion by highlighting the superior time efficiency of quantum cryptographic models over conventional methods like the Advanced Encryption Standard (AES). This efficiency translates into expedited cryptographic operations, crucial for maintaining the integrity and confidentiality of patient information. Quantum cryptography's transformative potential lies in its ability to enhance overall system performance and efficiency, addressing the escalating demands for robust data security in healthcare. By providing a clear and structured breakdown of time efficiency, the table underscores the significance of quantum cryptography in revolutionizing secure data encryption methodologies within the healthcare sector.

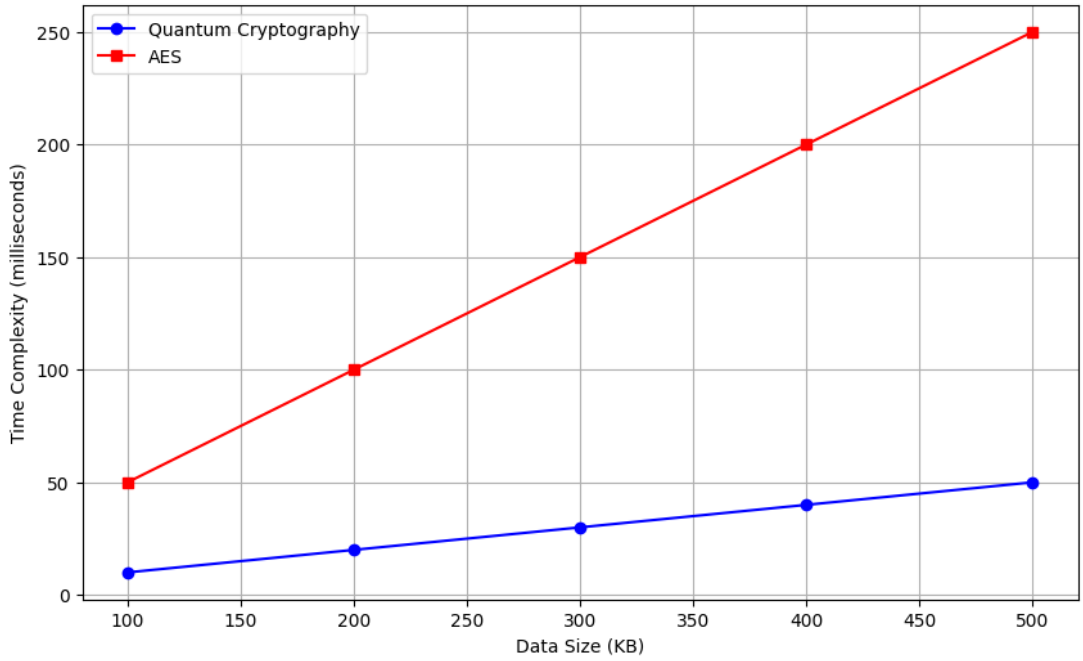

Fig.4 Time Complexity Comparison: Quantum Cryptography vs AES

In the fig.4, we're comparing two methods of securing healthcare data: quantum cryptography and traditional encryption. Imagine them as two cars racing to encrypt data. The blue line represents quantum cryptography, and the red line represents AES. As we increase the amount of data we need to secure (from 100 KB to 500 KB), both cars start from the same point. However, as they race, the blue car (quantum cryptography) maintains a steady pace, while the red car (traditional encryption) struggles to keep up. This difference in speed is crucial. It shows that quantum cryptography can handle larger amounts of data more efficiently, with less time needed to encrypt it. So, not only is quantum cryptography more secure, but it's also faster, making it the better choice for securing healthcare data effectively and efficiently.

V. Conclusion and Future Work

Quantum cryptography offers unparalleled encryption for healthcare data, ensuring utmost security and confidentiality. Through meticulous quantum state preparation, entanglement establishment, and key distribution, sensitive medical information remains protected from unauthorized access. Quantum decryption seamlessly retrieves encrypted data, maintaining patient privacy and fostering trust in healthcare systems. An examination of key generation times reveals the superiority of the quantum cryptographic approach over AES across diverse key lengths. For instance, at a key length of 220 bits, the proposed quantum model achieves a key generation time of 396.519 milliseconds, while AES demands 406.597 milliseconds. Likewise, with increasing input sizes, quantum cryptography maintains its efficiency. For example, at an input size of 50 kilobytes, the quantum model requires a mere 11 milliseconds compared to AES's 15 milliseconds, underscoring its consistent performance advantage. Future work will focus on further optimizing quantum key generation algorithms and enhancing the scalability of quantum cryptography to meet the evolving security demands of healthcare data management. Additionally, research efforts will explore the integration of quantum-resistant encryption techniques to future-proof healthcare systems against potential quantum computing threats.

REFERENCES

[1] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177-183.

[2] Omanwa, J. M. (2021). *Mobile Network Infrastructure Security in Developing Countries–A Kenya Case Study* (Doctoral dissertation, Walden University).

[3] Omar, R. A. (2020). Hacking HIPAA:" Best Practices" for Avoiding Oversight in the Sale of Your Identifiable Medical Information. *JL & Health*, *34*, 31.

[4] Agarwal, R., & Kumar, M. (2022). Cyber Security for Handling Threats in Healthcare Devices. *Healthcare Systems and Health Informatics*, 217.

[5] Arafa, A., Sheerah, H. A., & Alsalamah, S. (2023). Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review. *Information*, *14*(12), 640.

[6] Sonko, S., Ibekwe, K. I., Ilojianya, V. I., Etukudoh, E. A., & Fabuyide, A. (2024). Quantum Cryptography And Us Digital Security: A Comprehensive Review: Investigating The Potential Of Quantum Technologies In Creating Unbreakable Encryption And Their Future In National Security. *Computer Science & IT Research Journal*, *5*(2), 390-414.

[7] Tran, M. C., Mark, D. K., Ho, W. W., & Choi, S. (2023). Measuring arbitrary physical properties in analog quantum simulation. *Physical Review X*, *13*(1), 011049.

[8] Kong, P. Y. (2020). A review of quantum key distribution protocols in the perspective of smart grid communication security. *IEEE Systems Journal*, *16*(1), 41-54.

[9] Zhang, C. X., Wu, D., Cui, P. W., Ma, J. C., Wang, Y., & An, J. M. (2023). Research progress in quantum key distribution. *Chinese Physics B*.

[10] Chawla, D., & Mehra, P. S. (2023). A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. *Internet of Things*, 100950.

[11] Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. *IEEE Access*, *8*, 52018-52027.

[12] Geetha, R., Padmavathy, T., Thilagam, T., & Lallithasree, A. (2020). Tamilian cryptography: an efficient hybrid symmetric key encryption algorithm. *Wireless Personal Communications*, *112*, 21-36.

[13] Hu, Q., Asghar, M. R., & Brownlee, N. (2021). A large-scale analysis of HTTPS deployments: Challenges, solutions, and recommendations. *Journal of Computer Security*, *29*(1), 25-50.

[14] Obaidat, M., Brown, J., Obeidat, S., & Rawashdeh, M. (2020). A hybrid dynamic encryption scheme for multi-factor verification: a novel paradigm for remote authentication. *Sensors*, *20*(15), 4212.

[15] Fabrega, A., Maurer, U., & Mularczyk, M. (2021). A fresh approach to updatable symmetric encryption. *Cryptology ePrint Archive*.

[16] Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. *International Journal of intelligent networks*, *3*, 16-30.

[17] Munjal, K., & Bhatia, R. (2023). A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems*, *9*(4), 3759-3786.

[18] Reis, D., Takeshita, J., Jung, T., Niemier, M., & Hu, X. S. (2020). Computing-in-memory for performance and energy-efficient homomorphic encryption. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *28*(11), 2300-2313.

[19] Ali, A., Al-Rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A., & Almazroi, A. A. (2023). HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. *Sensors*, *23*(15), 6762.

[20] Alloghani, M., Alani, M. M., Al-Jumeily, D., Baker, T., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2019). A systematic review on the status and progress of homomorphic encryption technologies. *Journal of Information Security and Applications*, *48*, 102362.

[21] Gopalakrishnan, S., & Ganeshkumar, P., (2014) N-Crypt: A Highly Secured Data Transmission for Wireless Sensor Network, Journal of Theoretical and Applied Information Technology, 66(3), 670-677.

[22] Perumal, G., Subburayalu, G., Abbas, Q., Naqi, S. M., & Qureshi, I. (2023). VBQ-Net: A Novel Vectorization-Based Boost Quantized Network Model for Maximizing the Security Level of IoT System to Prevent Intrusions. *Systems*, *11*(8), 436.

[23] Joshi, A., Choudhury, T., Sai Sabitha, A., Srujan Raju, K. (2020). Data Mining in Healthcare and Predicting Obesity. In: Raju, K., Govardhan, A., Rani, B., Sridevi, R., Murty, M. (eds) Proceedings of the Third International Conference on Computational Intelligence and Informatics . Advances in Intelligent Systems and Computing, vol 1090. Springer, Singapore. https://doi.org/10.1007/978-981-15-1480-7_82

[24] Narasimharao, Jonnadula, A. Vamsidhar Reddy, Ravi Regulagadda, P. Sruthi, V. Venkataiah, and R. Suhasini. "Analysis on Rising the Life Span of Node in Wireless Sensor Networks Using Low Energy Adaptive Hierarchy Clustering Protocol." In *2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, pp. 651-659. IEEE, 2023.

[25] Monga, Chetna, K. Srujan Raju, P. M. Arunkumar, Ankur Singh Bist, Girish Kumar Sharma, Hashem O. Alsaab, and Baitullah Malakhil. "Secure techniques for channel encryption in wireless body area network without the Certificate." Wireless Communications and Mobile Computing 2022 (2022).