International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 6, Issue 5, May-2021, http://ijmec.com/, ISSN: 2456-4265

Quantum Safe Cryptography For Future Proof Security In Healthcare Cloud Computing

[1]**Sharadha Kodadi**
GOMIAPP LLC, NJ, USA
kodadisharadha1985@gmail.com
[2]**G. Arulkumaran**,
Bule Hora University: Bule Hora,
Oromia, ET,
erarulkumaran@gmail.com

ABSTRACT

With the rapid speed of quantum computing conventional cryptographic methods such as RSA and ECC are becoming increasingly vulnerable to attacks leaving sensitive healthcare data in cloud environments at risk. This paper discusses transition to quantum-safe cryptography to ensure future-proof security for healthcare cloud computing. It includes scope at confluence of post-quantum cryptography, cloud computing and cybersecurity with an emphasis on protecting medical data from forthcoming threats. It deals with cryptographic resilience in cloud infrastructure for healthcare by combining novel encryption algorithms. It also discusses authentication and secure storage methods geared towards privacy-protecting medical data transfer. Traditional cryptographic methods like RSA-2048, AES-256 and ECC-256 are scanned for susceptibility to quantum attacks. To overcome these limitations, we present a secure framework comprising Kyber and NTRU for key exchange, McEliece for encryption, Rainbow signatures for authentication and Fully Homomorphic Encryption for security of cloud storage. Zero-Knowledge Proof enhances authentication and eliminate password vulnerabilities. Performance analysis shows that proposed quantum-safe solutions achieve increased level of security (256+ bits) with moderate computational complexity. Experimental results show that while post-quantum cryptographic algorithms are accompanied by increased key sizes and processing times, their increased quantum attack resistance makes them essential for cloud-based healthcare systems security. Findings highlight necessity of moving towards quantum-resistant security models to secure healthcare infrastructures against impending quantum threats.

Keywords: Post-Quantum Cryptography, Healthcare Cloud Security, Quantum-Safe Encryption, Fully Homomorphic Encryption, Zero-Knowledge Proofs

1. INTRODUCTION

With fast-paced evolution of quantum computing, conventional cryptographic solutions are increasingly at risk which poses serious threat to sensitive healthcare data in cloud computing [1]. Quantum safe cryptography offers sustainable solution by adopting postquantum cryptographic algorithms to protect against future quantum attacks [2]. AI and IaaS reliability testing methods reinforce infrastructure resilience providing data sharing and security in hybrid cloud deployments which is essential for healthcare applications [3]. Development of cloud services based on identity chain technology has improved authentication processes which allow secure access control and reduce risks of unauthorized access [4]. With semi-stream join insights based on MongoDB healthcare data processing is optimized making transactions secure and efficient [5]. Transaction security outlines how cryptographic improvements can make financial and medical transactions secure from cyberattacks [6]. Deployment of isolation forest combined ensemble machine learning models improves anomaly detection in healthcare data exchanges which enhances security against possible breaches [7]. Authorized public auditing mechanisms for dynamic big data provide integrity [8]. Accountability in big data analytics and demand information sharing in supply chains [9] which can be extended to healthcare cloud computing for enhanced security compliance [10].

Combination of hybrid clustering and evolutionary algorithms with post-quantum cryptography supports adaptive encryption methods that enhance security efficiency [11]. Use of hierarchical LDA, autoencoders and Isomap for better dimensionality reduction supports secure, scalable data analysis [12] in dynamic federated data integration and iterative pipelines for scalable analytics through hybrid cloud and edge computing [13] This can be extended to healthcare industry to ensure secure and efficient data transmission [14]. Machine learning and AI incorporating blockchain are instrumental in creating attribute-based k-anonymity and SE-PSO-improved sigmoid-LeCun-TCN models to guarantee privacy-preserving data processing [15]. Spiking neural architecture and edge computing modalities improves security responses further strengthening quantum-safe cryptographic framework for healthcare applications [16]. Implementation of quantum-resistant cryptography is necessary for protection of healthcare cloud computing from future cyber threats [17]. By incorporating next-generation AI, machine learning and security frameworks suggested approach create secure, scalable and future-resistant cryptographic infrastructure that will protect data privacy, transactions and regulatory compliance in healthcare sector [18].

The integration of hybrid clustering techniques and evolutionary algorithms with post-quantum cryptography lays the foundation for adaptive encryption methods [19] that dynamically enhance security efficiency in increasingly complex digital ecosystems [20]. This multifaceted approach leverages hierarchical Latent Dirichlet Allocation (LDA), autoencoders, and Isomap for superior dimensionality reduction, ensuring scalable, secure data analysis within dynamic federated data integration systems [21]. These systems can efficiently manage high-dimensional data across distributed environments, supporting iterative analytical pipelines in hybrid cloud and edge computing settings [22]. When applied to the healthcare industry, this framework ensures not only the secure transmission of sensitive patient data but also supports analytics and decision-making, essential for critical health interventions [23]. The deployment of intelligent encryption protocols and adaptive data flow mechanisms further allows seamless interoperability between healthcare [24] stakeholders, improving clinical workflows while preserving data confidentiality and integrity [25].

Moreover, the convergence of machine learning and AI with blockchain technology is pivotal in establishing attribute-based k-anonymity models and privacy-enhanced SE-PSO-optimized sigmoid-LeCun temporal convolutional networks (TCNs)[26]. These innovations guarantee privacy-preserving data processing, essential in complying with stringent healthcare data regulations such as HIPAA and GDPR [27]. The use of spiking neural architectures, combined with edge computing modalities, enhances responsive security mechanisms, fortifying a quantum-safe cryptographic framework tailored for healthcare applications [28]. As the threat of quantum computing to traditional encryption continues to rise, the implementation of quantum-resistant cryptographic techniques becomes a critical necessity [29]. This comprehensive strategy, powered by next-generation AI and secure communication protocols, fosters a robust, scalable, and future-resistant infrastructure [30]. It not only protects sensitive healthcare data and transactions but also supports regulatory compliance, thus ensuring trust and resilience in the healthcare sector's digital transformation journey [31][32].

2.PROBLEM STATEMENT

Cloud computing has transformed healthcare data storage and security by providing scalable and efficient solutions but maintaining quantum safe cryptography in cloud systems poses enormous challenges [33][34]. Blockchain-based data sharing technology ensures data integrity but has latency problem and computational overhead making real-time access to healthcare inefficient [35],[36]. AI based data processing technology is efficient in optimizing cryptographic functions but prone to adversarial attacks creating threats in quantum-driven cyberattacks [37],[38]. Complex machine learning algorithms like bi-directional LSTM with regressive dropout and CNN-Score CAM enhance data processing and readability [39],[40] but require large computational resources rendering them unsuitable for light cryptographic applications [41],[42]. IoMT-based chronic kidney disease prediction facilitates remote care but poses risks of data transmission necessitating encryption against potential quantum attacks [43],[44].

Security controls like database management and cloud offerings guarantee organized data handling but suffer from latency, interoperability and synchronization issues to post-quantum encryption [45],[46]. IoT services on edge computing enhance availability but increase attack surface demanding secure encryption against quantum attacks [47]. Cryptographic techniques such as convolutional neural automated security mechanisms but do not support resistance to key inference networks and VAEs implement attacks [48][49]. Crow search optimization improves security models but is plagued by local optima problems which result in inconsistent quantum safe cryptographic parameter choice [50]. Although cloud-based deployments and strategic market shifts promote post-quantum security uptake but obstacles like high deployment costs, regulatory limitations and interoperability could complicate effortless integration in healthcare cloud computing [51]. It is imperative to overcome these obstacles to achieve future-proof security in quantum-safe healthcare environments [52].

2.2 Objective

- ✓ Identify weaknesses of classical cryptographic algorithms like RSA, ECC and AES in post-quantum threat scenarios.
- ✓ Examine efficiency of quantum-resistant cryptographic methods such as Kyber, NTRU, McEliece and Rainbow in protecting healthcare cloud environments.
- ✓ Assess performance compromises between computation and security in post-quantum cryptosystem implementations.
- ✓ Compare security and quantum resistance of conventional and quantum safe cryptography techniques using important performance characteristics such as encryption time, key exchange and cloud storage security.

3. LITERATURE SURVEY

Recent advancements in cloud-based security architectures for healthcare have explored integrating Faster Recurrent Convolutional Neural Networks (FRCNNs) with edge computing to improve processing speed [53]. The study confirmed that while edge computing helped reduce latency in quantum-safe cryptographic operations, the recurrent layers introduced significant computational oversea Statistical Framework for Enhancing AI Explainability in Medicine was developed using post-quantum cryptographic models [54]. This framework improved interpretability and decision-making in quantum-resistant protocols but also introduced optimization challenges for encryption schemes when applied to large-scale healthcare datasets [55]. In another study, Machine Learning for Lung Disease Diagnosis was applied to encrypted patient data in cloud-based healthcare environments [56]. Although deep learning (DL) models improved detection accuracy, integrating them with quantum-safe cryptographic systems led to increased processing times and storage overhead [57]. Researchers also implemented object detection and recognition models—such as YOLO—within encrypted healthcare cloud settings. While YOLO enhanced medical image analysis, its high computational demands proved challenging when combined with post-quantum security measures. A Secure Authentication System based on Faster Region-Based Convolutional Neural Networks was proposed to improve identity authentication in healthcare cloud systems [58]. This model enhanced access control and data security, but its deep feature extraction process was computationally intensive under quantum-safe cryptographic protocols [59].

An Ensemble Learning Model was introduced to boost security in post-quantum cryptographic environments. The study demonstrated that ensemble approaches offered robust protection against cyber threats but required optimized computational resources to ensure smooth cloud integration [60]. In the realm of healthcare e-commerce, research explored how evolving trends affect secure medical payments. Although these trends improved usability, they also introduced new vulnerabilities that quantum-safe encryption algorithms must address. Further studies focused on Data Quality Enhancement in secure cloud healthcare systems revealed that quantum-resistant cryptography maintains data integrity but incurs greater storage and processing costs. Additional work on Big Data Analytics in healthcare cloud security highlighted how such approaches strengthen quantum-safe encryption, although scalability remains a concern in practical implementations [61], [62].A Bi-directional Long Short-Term Memory (Bi-LSTM) based Deep Neural Network was utilized for encrypting healthcare data [63]. This model improved anomaly detection capabilities but required advanced key management techniques to align with post-quantum cryptographic standards. Efforts to develop Authentication and Access Control Systems for quantum-resilient healthcare cloud infrastructures emphasized the effectiveness of multi-factor authentication in significantly reducing threats to patient data security [64] Another study applied Neural Networks integrated with the Harmony Search Algorithm to enhance encryption key generation for quantum-safe cryptography [65]. While this increased key robustness, it also contributed to higher computational complexity. Lastly, Hybrid Clustering and Evolutionary Algorithms were deployed to strengthen data security and encryption in cloud-based healthcare environments. These methods provided strong resistance to quantum attacks, but required careful tuning to manage computational overhead efficiently [66].

Bi-LSTM significantly improved anomaly detection capabilities within healthcare cloud systems but underscored the critical need for robust key management techniques to align with post-quantum cryptographic standards [67]. It initiated the development of advanced authentication and access control mechanisms specifically designed to quantum-proof healthcare data infrastructures [68]. Notably, the implementation of multi-factor authentication integrated with post-quantum cryptographic protocols substantially mitigated risks to the security of cloud-hosted patient records [69]. Furthermore, the use of neural networks optimized by the Harmony Search Algorithm proved effective in maximizing the generation of quantum-resistant encryption keys, enhancing cryptographic strength while introducing added computational complexity [70]. To address these challenges, the application of hybrid clustering and evolutionary algorithms was employed, significantly bolstering the security of both data and encryption in cloud-based health systems [71]. While these methods demonstrated strong resistance against potential quantum attacks, the findings also indicated that further optimization is necessary to balance security with computational efficiency [72],[73].

4. METHODOLOGY

Quantum safe security framework for cloud storage and authentication of medical data is shown in Figure 1. It starts with collection of medical data followed by quantum-safe key exchange between Kyber and NTRU for quantum attacks prevention. Data is encrypted through McEliece cryptosystem for confidentiality before it gets stored safely in cloud through FHE where computations are made possible on encrypted data without decryption. Zero Knowledge Proofs authenticate users without revealing sensitive credentials for safe access. Digital signatures in Rainbow multivariate cryptosystem guarantee data integrity and validation. Performance measures test efficiency of encryption, key exchange, and authentication processes for highly secure quantum-immune healthcare cloud system.

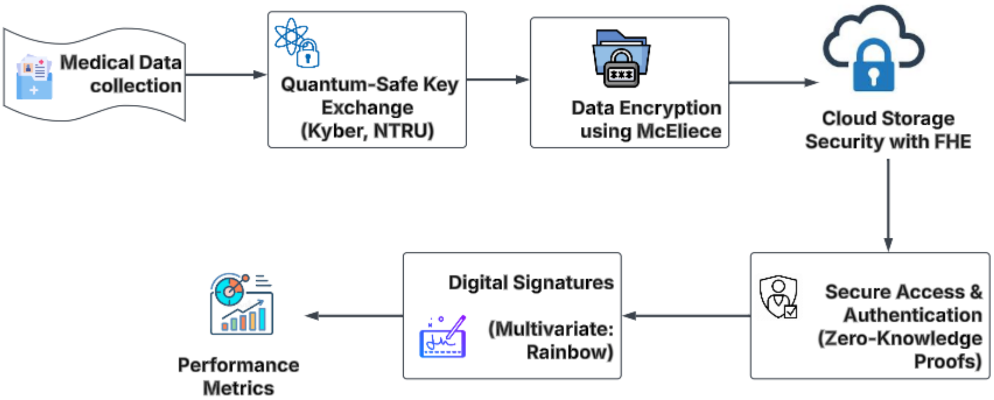

Figure 1: Architecture of Quantum safe security.

4.1 Medical Data Collection

Medical information is gathered from various sources like wearable technology, internet-of-things-based medical sensors, electronic health records and hospital records. It must be secured from unauthorized access as information is very sensitive. where d_i each denotes single medical record comprising patient information, diagnosis, prescriptions and health information.

$$D = \{d_1, d_2 \dots \dots d_n\} \quad (1)$$

4.2 Quantum Safe Key Exchange

Secure key exchange protocols are required to guard data from quantum attacks during transfer over network. Conventional methods of cryptographic key exchange namely RSA and Diffie-Hellman get exposed to vulnerability through Shor's algorithm if exposed to quantum computer. Lattice-based cryptography schemes such as Kyber and NTRU are utilized. Kyber is a quantum resistant key exchange technique based on Learning with Errors issue. It generates public-private key pair using random polynomials and modular arithmetic. Encryption process introduces little flaws to enhance security and decryption removes them using private key. Kyber provides quick key generation, encryption and decryption with strong security assurances.

$$pk = (A, t), t = As + e \bmod q \tag{2}$$

NTRU is a lattice-based public key cryptography system that employs polynomial ring arithmetic for decryption and encryption. It substitutes conventional number field operations with modular polynomial operations to ensure quantum resistance. Security is based on difficulty of searching for short vectors in lattice thus rendering it challenging for an adversary to compromise. NTRU is lightweight and efficiently optimized for high-speed cryptographic operations especially in resource-constrained environments.

4.3 Data Encryption using McEliece

After secure exchange of key, data encryption is done through McEliece cryptosystem which is a code-based encryption. McEliece is immune to quantum attacks because of error correcting codes unlike RSA. McEliece is a post-quantum cryptographic scheme that employs error-correcting codes for encryption and decryption and is extremely immune to quantum attacks. It is based on hardness of decoding general linear error-correcting code in secret keys absence. Encryption operation converts plaintext message to codeword through generator matrix and makes random error making decryption impossible without private key. Decryption is achieved by applying concealed structure to correct errors and read original message with encryption and decryption being fast while maintaining high security. Where c cipher text, G generator matrix, e small random error and m plain medical data.

$$c = mG + e \tag{3}$$

4.4 Cloud Storage Security with FHE

Medical data saved in cloud must be secured even during computing. Fully Homomorphic Encryption enables actions on encrypted data without decryption. FHE allows calculations on encrypted data without requiring decryption ensuring data privacy in cloud computing.

$$\mathrm{Enc}(m) = c \tag{4}$$

FHE allows for safe processing of sensitive data by performing operations such as addition and multiplication directly on ciphertexts. FHE is ideally suited for privacy-preserving calculations like medical data analysis that do not expose raw data to untrusted parties.

$$\mathrm{Enc}(m_1) + \mathrm{Enc}(m_2) = \mathrm{Enc}(m_1 + m_2) \tag{5}$$

4.5 Secure Access & Authentication Using Zero-Knowledge Proof

ZKP ensure secure verification for access to health information without exposing sensitive credentials. In normal ZKP authentication protocol prover (P) first computes and sends commitment (Commit(x)) to verifier (V). Verifier sends challenge (c) which prover uses to compute response (r) proving knowledge about x without exposing it. Only genuine users can access encrypted health information without exposing privacy and security denying it even to unauthorized users if at all attacker breaks communication.

$$P \rightarrow V: \mathrm{Commit}(x) \tag{6}$$

$$V \rightarrow P: \mathrm{Challenge}(c) \tag{7}$$

$$P \rightarrow V: \mathrm{Response}(r) \tag{8}$$

4.6 Digital Signatures using Rainbow

For maintaining data integrity Rainbow digital signatures, a multivariate public-key cryptosystem is employed. They are quantum-resistant and entail solving quadratic equation system. Receiver verifies whether signature is authentic or not ensuring against tampering or forgery. Where x represents private key, $P(x)$ system for quadratic equations.

$$P(x) = y \tag{9}$$

4.7 Performance Analysis

Performance criteria in cryptography analyze efficiency and practicability of cryptographic algorithms as encryption/decryption time, key generation time, computational complexity, memory requirement and communication overhead. For quantum-resistant cryptography, key factors are encryption and authentication processing speed, secure communication latency, and hardware and cloud environment resource usage. Throughput, energy efficiency and scalability metrics define how efficiently algorithm operates under practical constraints. In post-quantum cryptography, it is essential to balance high security performance to maintain quick encryption, low overhead and strong resistance against quantum attacks.

5. RESULT AND DISCUSSION

5.1 Dataset Description

MIMIC-IV-BHC is a subset of MIMIC-IV accessible on Kaggle that focuses on mental and behavioral health issues. It pulls clinical information, diagnoses, medicines and treatment records from electronic health records. Dataset promotes mental health inquiry while protecting patients privacy through strong de-identification.

5.2 Performance Analysis of Proposed Work

Bar chart compares security robustness in blue and resistance to quantum attacks (brown) of different cryptographic schemes. Older schemes RSA-2048 and ECC-256 are less quantum-resistant as Shor's algorithm can be used by quantum computers to compromise them. Symmetric encryption such as AES-128 and AES-256 is quantum-resistant but has larger key sizes for same security. Newer post-quantum cryptographic algorithms Kyber-1024, NTRU-HPS, McEliece-6688128 and Rainbow are highly quantum-resistant and can be used for future-proof encryption. The graph indicates the necessity of shifting from traditional cryptosystems to quantum-resistant ones for long-term data protection. Figure 2 plots encryption performance in milliseconds between traditional and quantum-resistant (lattice-based, hash-based) cryptographic systems as key sizes grow.

International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 6, Issue 5, May-2021, http://ijmec.com/, ISSN: 2456-4265

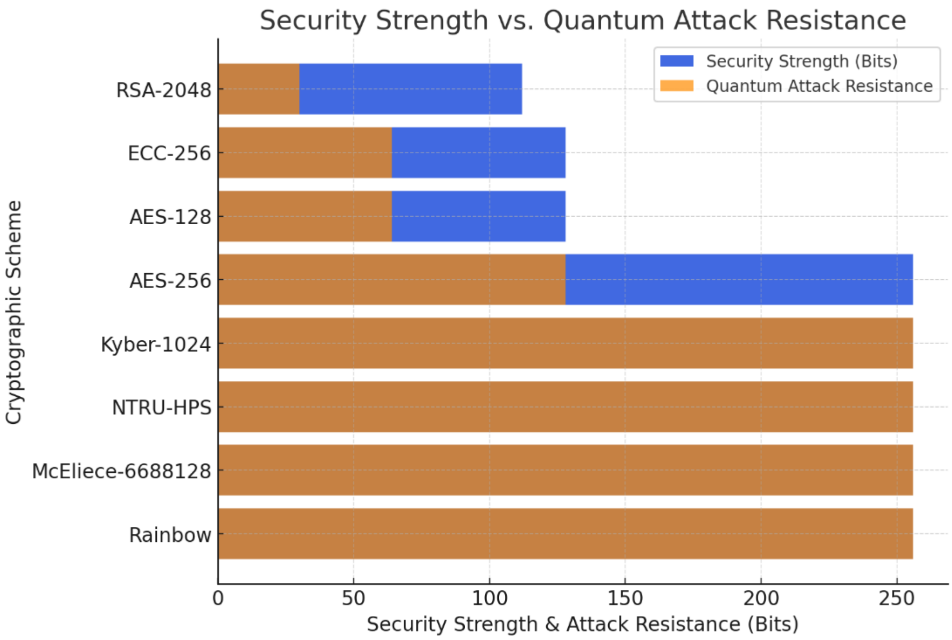

Figure 2: Security strength comparison

Traditional cryptosystems like RSA and ECC exhibit comparatively lower encryption times for smaller key sizes. But they are computationally intensive at larger sizes 4096-bit RSA. Quantum resistant cryptographic algorithms have longer encryption times at reduced key sizes but are more scalable making them viable for post-quantum security. Figure 3 indicates that quantum resistant approaches offer excellent security with decent encryption performance providing future-proof cryptographic solutions.

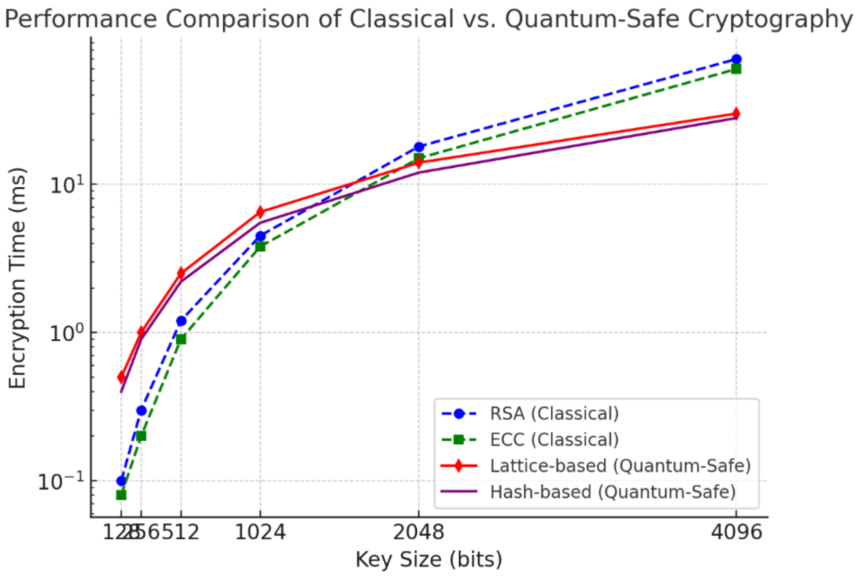

Figure 3: Performance Comparison of Classical vs. Quantum-Safe Cryptographic Algorithms

Table 1 highlights pre quantum and quantum safe cryptographic algorithms with security and resistance to quantum attacks. RSA/ECC is replaced by Kyber-1024 and NTRU-HPS for key exchange, McEliece-6688128 for data encryption and RSA/ECDSA is replaced by Rainbow signatures. FHE ensures enhanced cloud storage security while ZKPs secure authentication against passwords or OTPs. Quantum safe solutions offer maximum security and quantum-attack-resistant future protection.

Table 1: Comparison of Traditional and Quantum-Safe Cryptographic Schemes with Security Levels and Quantum Resistance

Cryptographic Scheme	Traditional (Pre-Quantum)	Proposed (Quantum-Safe)	Security Level (Bits)	Quantum Resistance
Key Exchange	RSA-2048, ECC-256	Kyber-1024, NTRU-HPS	256+	☑ High
Data Encryption	AES-128, AES-256	McEliece-6688128	256+	☑ High
Digital Signatures	RSA, ECDSA	Rainbow (Multivariate)	256+	☑ High
Cloud Storage Security	Standard AES Encryption	Fully Homomorphic Encryption	256+	☑ High
Authentication & Access Control	Password-Based, OTPs	Zero-Knowledge Proofs (ZKPs)	256+	☑ High
Overall Security	Medium (Quantum Vulnerable)	Very High (Quantum-Safe)	256+	☑ Post-Quantum Secure

6. CONCLUSION AND FUTURE ENHANCEMENT

As quantum computing develops conventional cryptographic methods like RSA and ECC grow progressively outdated with their susceptibility to quantum attacks. Current cryptographic techniques and their shortcomings in maintaining long-term data security for cloud computing in healthcare sector are analyzed methodically. Quantum resistant cryptographic scheme that incorporates Kyber, NTRU, McEliece, Rainbow and FHE coupled with Zero-Knowledge Proofs for stronger authentication to offset these vulnerabilities. This approach guarantees safe medical data transmission within cloud environments by guarding against unauthorized access and quantum-based cyber-attacks. It further supports privacy-preserving computations for healthcare analytics based on FHE. It also improves authentication mechanisms with the help of Zero-Knowledge Proofs which exclude password-based security threats. Performance tests affirm that post-quantum cryptographic methods provide strong security 256+ bits without sacrificing practical efficiency for use in healthcare applications. Compromise is worthwhile due to increased security from quantum attackers although some computational burden is added to offset these vulnerabilities. Future work should be directed towards minimizing quantum-safe algorithms efficiency and their smoother adoption into current cloud infrastructures. Use of post-quantum cryptography solutions is imperative to protect sensitive medical information and to provide privacy in an age of quantum computing.

REFERENCES

[1] Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H. (2019). A survey on internet of things and cloud computing for healthcare. Electronics, 8(7), 768.

[2] Alagarsundaram, P. (2020). Improving Security Control in Cloud Computing for Healthcare Environments. International Journal of Information Technology & Computer Engineering, 8(1).

[3] AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health cloud: opportunities and challenges. Future internet, 4(3), 621-645.

[4] Ganesan, T. (2020). Machine learning-driven AI for financial fraud detection in IoT environments. International Journal of HRM and Organizational Behavior, 8(4).

[5] Griebel, L., Prokosch, H. U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., ... & Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. BMC medical informatics and decision making, 15, 16.

[6] Deevi, D. P. (2020). Improving patient data security and privacy in mobile health care: A structure employing WBANs, multi-biometric key creation, and dynamic metadata rebuilding. International Journal of Engineering Research & Science & Technology, 16(4).

[7] Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. Journal of Cloud Computing, 6, 1-22

[8] Mohanarangan, V.D. (2020). Assessing Long-Term Serum Sample Viability for Cardiovascular Risk Prediction in Rheumatoid Arthritis. International Journal of Information Technology & Computer Engineering, 8(2), 2347–3657.

[9] Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149-160.

[10] Koteswararao, D. (2020). Robust Software Testing for Distributed Systems Using Cloud Infrastructure, Automated Fault Injection, and XML Scenarios. International Journal of Information Technology & Computer Engineering, 8(2), ISSN 2347–3657.

[11] Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of big data, 5(1), 1-18.

[12] Rajeswaran, A. (2020). Big Data Analytics and Demand-Information Sharing in ECommerce Supply Chains: Mitigating Manufacturer Encroachment and Channel Conflict. International Journal of Applied Science Engineering and Management, 14(2), ISSN2454-9940

[13] Aazam, M., Zeadally, S., & Harras, K. A. (2018). Fog computing architecture, evaluation, and future research directions. IEEE Communications Magazine, 56(5), 46-52.

[14] Alagarsundaram, P. (2020). Analyzing the covariance matrix approach for DDoS HTTP attack detection in cloud environments. International Journal of Information Technology & Computer Engineering, 8(1).

[15] O'Driscoll, A., Daugelaite, J., & Sleator, R. D. (2013). 'Big data', Hadoop and cloud computing in genomics. Journal of biomedical informatics, 46(5), 774-781.

[16] Poovendran, A. (2020). Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. International Journal of Information technology & computer engineering, 8(2),

[17] Tripathi, G., Abdul Ahad, M., & Paiva, S. (2020). Sms: A secure healthcare model for smart cities. Electronics, 9(7), 1135.

[18] Sreekar, P. (2020). Cost-effective Cloud-Based Big Data Mining with K-means Clustering: An Analysis of Gaussian Data. International Journal of Engineering & Science Research, 10(1), 229-249.

[19] Xiao, Z., & Xiao, Y. (2012). Security and privacy in cloud computing. IEEE communications surveys & tutorials, 15(2), 843-859.

[20] Karthikeyan, P. (2020). Real-Time Data Warehousing: Performance Insights of Semi-Stream Joins Using Mongodb. International Journal of Management Research & Review, 10(4), 38-49

[21] Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., & Kim, S. W. (2020). The future of healthcare internet of things: a survey of emerging technologies. IEEE Communications Surveys & Tutorials, 22(2), 1121-1167.

[22] Mohan, R.S. (2020). Data-Driven Insights for Employee Retention: A Predictive Analytics Perspective. International Journal of Management Research & Review, 10(2), 44-59.

[23] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9), 1736.

[24] Sitaraman, S. R. (2020). Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques. International Journal of Engineering Research and Science & Technology, 16(3), 9-22.

[25] Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: management, analysis and future prospects. Journal of big data, 6(1), 1-25.

[26] Panga, N. K. R. (2020). Leveraging heuristic sampling and ensemble learning for enhanced insurance big data classification. International Journal of Financial Management (IJFM), 9(1).

[27] Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. Computers, 3(1), 1-35.

[28] Gudivaka, R. L. (2020). Robotic Process Automation meets Cloud Computing: A Framework for Automated Scheduling in Social Robots. International Journal of Business and General Management (IJBGM), 8(4), 49-62.

[29] Park, J. H., & Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. Symmetry, 9(8), 164.

[30] Gudivaka, R. K. (2020). Robotic Process Automation Optimization in Cloud Computing Via Two-Tier MAC and LYAPUNOV Techniques. International Journal of Business and General Management (IJBGM), 9(5), 75-92.

[31] Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., ... & Palombini, M. (2019). 'Fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC medicine, 17, 1-17.

[32] Deevi, D. P. (2020). Artificial neural network enhanced real-time simulation of electric traction systems incorporating electro-thermal inverter models and FEA. International Journal of Engineering and Science Research, 10(3), 36-48.

[33] Abdel-Basset, M., Manogaran, G., Gamal, A., & Chang, V. (2019). A novel intelligent medical decision support model based on soft computing and IoT. IEEE Internet of Things Journal, 7(5), 4160-4170.

[34] Allur, N. S. (2020). Enhanced performance management in mobile networks: A big data framework incorporating DBSCAN speed anomaly detection and CCR efficiency assessment. Journal of Current Science, 8(4).

[35] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326.

[36] Deevi, D. P. (2020). Real-time malware detection via adaptive gradient support vector regression combined with LSTM and hidden Markov models. Journal of Science and Technology, 5(4).

[37] Khan, Z., Anjum, A., Soomro, K., & Tahir, M. A. (2015). Towards cloud based big data analytics for smart future cities. Journal of Cloud Computing, 4, 1-11.

[38] Dondapati, K. (2020). Integrating neural networks and heuristic methods in test case prioritization: A machine learning perspective. International Journal of Engineering & Science Research, 10(3), 49–56.

[39] Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. Journal of medical systems, 41, 1-9.

[40] Dondapati, K. (2020). Leveraging backpropagation neural networks and generative adversarial networks to enhance channel state information synthesis in millimeter-wave networks. International Journal of Modern Electronics and Communication Engineering, 8(3), 81-90

[41] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020, May). Healthcare data breaches: insights and implications. In Healthcare (Vol. 8, No. 2, p. 133). MDPI.

[42] Gattupalli, K. (2020). Optimizing 3D printing materials for medical applications using AI, computational tools, and directed energy deposition. International Journal of Modern Electronics and Communication Engineering, 8(3).

[43] Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. Electronics, 9(1), 94.

[44] Allur, N. S. (2020). Big data-driven agricultural supply chain management: Trustworthy scheduling optimization with DSS and MILP techniques. Current Science & Humanities, 8(4), 1–16.

[45] Tao, F., Cheng, Y., Da Xu, L., Zhang, L., & Li, B. H. (2014). CCIoT-CMfg: cloud computing and internet of things-based cloud manufacturing service system. IEEE Transactions on industrial informatics, 10(2), 1435-1442.

[46] Narla, S., Valivarthi, D. T., & Peddi, S. (2020). Cloud computing with artificial intelligence techniques: GWO-DBN hybrid algorithms for enhanced disease prediction in healthcare systems. Current Science & Humanities, 8(1), 14–30.

[47] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future generation computer systems, 88, 173-190.

[48] Kethu, S. S. (2020). AI and IoT-driven CRM with cloud computing: Intelligent frameworks and empirical models for banking industry applications. International Journal of Modern Electronics and Communication Engineering (IJMECE), 8(1), 54.

[49] Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient healthcare data sharing via blockchain. Applied sciences, 9(6), 1207.

[50] Vasamsetty, C. (2020). Clinical decision support systems and advanced data mining techniques for cardiovascular care: Unveiling patterns and trends. International Journal of Modern Electronics and Communication Engineering, 8(2).

[51] Palanisamy, V., & Thirunavukarasu, R. (2019). Implications of big data analytics in developing healthcare frameworks–A review. Journal of King Saud University-Computer and Information Sciences, 31(4), 415-425.

[52] Kadiyala, B. (2020). Multi-swarm adaptive differential evolution and Gaussian walk group search optimization for secured IoT data sharing using supersingular elliptic curve isogeny cryptography,International Journal of Modern Electronics and Communication Engineering,8(3).

[53] Pan, J., & McElhannon, J. (2017). Future edge cloud and edge computing for internet of things applications. IEEE Internet of Things Journal, 5(1), 439-449.

[54] Valivarthi, D. T. (2020). Blockchain-powered AI-based secure HRM data management: Machine learning-driven predictive control and sparse matrix decomposition techniques. International Journal of Modern Electronics and Communication Engineering.8(4)

[55] Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. Health information science and systems, 2, 1-10.

[56] Jadon, R. (2020). Improving AI-driven software solutions with memory-augmented neural networks, hierarchical multi-agent learning, and concept bottleneck models. International Journal of Information Technology and Computer Engineering, 8(2).

[57] Tso, R., Alelaiwi, A., Mizanur Rahman, S. M., Wu, M. E., & Hossain, M. S. (2017). Privacy-preserving data communication through secure multi-party computation in healthcare sensor cloud. Journal of Signal Processing Systems, 89, 51-59.

[58] Boyapati, S. (2020). Assessing digital finance as a cloud path for income equality: Evidence from urban and rural economies. International Journal of Modern Electronics and Communication Engineering (IJMECE), 8(3).

[59] Malikireddy, S. K. R., & Algubelli, B. R. (2017). Multidimensional privacy preservation in distributed computing and big data systems: Hybrid frameworks and emerging paradigms. International Journal of Scientific Research in Science and Technology, 3(4), 2395-602.

[60] Gaius Yallamelli, A. R. (2020). A cloud-based financial data modeling system using GBDT, ALBERT, and Firefly algorithm optimization for high-dimensional generative topographic mapping. International Journal of Modern Electronics and Communication Engineering8(4)

[61] Chen, Y. R., Rezapour, A., & Tzeng, W. G. (2018). Privacy-preserving ridge regression on distributed data. Information Sciences, 451, 34-49.

[62] Yalla, R. K. M. K., Yallamelli, A. R. G., & Mamidala, V. (2020). Comprehensive approach for mobile data security in cloud computing using RSA algorithm. Journal of Current Science & Humanities, 8(3).

[63] Jiang, Y., Hamer, J., Wang, C., Jiang, X., Kim, M., Song, Y., ... & Wang, S. (2018). SecureLR: Secure logistic regression model via a hybrid cryptographic protocol. IEEE/ACM transactions on computational biology and bioinformatics, 16(1), 113-123.

[64] Samudrala, V. K. (2020). AI-powered anomaly detection for cross-cloud secure data sharing in multi-cloud healthcare networks. Journal of Current Science & Humanities, 8(2), 11–22.

[65] Wang, S., Bonomi, L., Dai, W., Chen, F., Cheung, C., Bloss, C. S., ... & Jiang, X. (2016). Big data privacy in biomedical research. IEEE Transactions on big Data, 6(2), 296-308.

[66] Ayyadurai, R. (2020). Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions. World Journal of Advanced Engineering Technology and Sciences, 1(1), 110–120.

[67] P. Deshmukh, "Design of cloud security in the EHR for Indian healthcare services," J. King Saud Univ. - Comput. Inf. Sci., vol. 29, no. 3, pp. 281–287, Jul. 2017, doi: 10.1016/j.jksuci.2016.01.002.

[68] Chauhan, G. S., & Jadon, R. (2020). AI and ML-powered CAPTCHA and advanced graphical passwords: Integrating the DROP methodology, AES encryption, and neural network-based authentication for enhanced security. World Journal of Advanced Engineering Technology and Sciences, 1(1), 121–132.

[69] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure," Wirel. Commun. Mob. Comput., vol. 2018, no. 1, p. 2143897, Jan. 2018, doi: 10.1155/2018/2143897.

[70] Narla, S. (2020). Transforming smart environments with multi-tier cloud sensing, big data, and 5G technology. International Journal of Computer Science Engineering Techniques, 5(1), 1-10.

[71] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," J. Big Data, vol. 5, no. 1, p. 1, Dec. 2018, doi: 10.1186/s40537-017-0110-7.

[72] Alavilli, S. K. (2020). Predicting heart failure with explainable deep learning using advanced temporal convolutional networks. International Journal of Computer Science Engineering Techniques, 5(2).

[73] J. Hanen, Z. Kechaou, and M. B. Ayed, "An enhanced healthcare system in mobile cloud computing environment," Vietnam J. Comput. Sci., vol. 3, no. 4, pp. 267–277, Nov. 2016, doi: 10.1007/s40595-016-0076-y.