International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

Quantum-Resistant Lightweight Post-Quantum Distributed Ledger Security Framework with Deep Learning-Based Storage Optimization for Healthcare Systems

Mr. R.Palaniyappan[1]

Research Scholar, Department of Computer Science, Sri Vasavi College , Erode, Tamilnadu, India.

palaniraja92@gmail.com

Dr.D. Sasikala[2]

Assistant Professor, Department of Computer Science, Sri Vasavi College, Erode, Tamilnadu, India.

drdsasikalaphd@gmail.com

Abstract: The rapid evolution of quantum computing poses severe threats to classical cryptographic primitives employed in distributed ledger systems, which are vulnerable to quantum algorithms like Shor's algorithm. This study proposes a Quantum-Resistant lightweight distributed ledger security framework integrating Post-quantum Cryptography (QR-PQ), lightweight encryption, and deep learning-based storage optimization to ensure sustainable security and scalability in resource-constrained environments. The framework employs lattice-based and hash-based PQC algorithms for robust encryption and digital signatures, ensuring long-term quantum resilience. Lightweight cryptographic modules minimize computational complexity for real-time IoT and healthcare applications. A deep learning-driven pruning and compression mechanism dynamically optimizes distributed ledger storage, retaining critical data while removing redundant records without compromising integrity. Experimental evaluation on a medical distributed ledger dataset of 50,000 Electronic Health Records demonstrates significant reductions in hash computation time (56%), encryption/decryption latency (66%), and storage overhead (up to 60%) compared to traditional distributed ledger models. Results affirm that the proposed QR-LPQCF achieves quantum resistance, computational efficiency, and scalable storage, making it highly suitable for secure data handling in future quantum-augmented environments. This framework establishes a foundational paradigm for designing quantum-secure and storage-optimized distributed ledger architectures for next-generation digital infrastructures.

Keywords: *Quantum-Resistant, cryptography, deep learning, storage optimization, distributed ledger pruning, IoT security, lattice-based encryption, and quantum threat mitigation.*

1. Introduction

The advent of quantum computing has revolutionized computational paradigms by enabling exponentially faster factorization and discrete logarithm computations compared to classical systems [1]. While this advancement enhances computational power, it simultaneously jeopardizes the security foundations of modern cryptography. Traditional distributed ledger systems rely heavily on RSA and Elliptic Curve Cryptography (ECC), whose mathematical hardness assumptions are rendered ineffective under quantum attacks utilizing Shor's algorithm [2]. This emerging quantum threat necessitates a quantum-resistant distributed ledger framework that ensures long-term data confidentiality, integrity, and availability, especially in mission-critical sectors such as healthcare and IoT [3].

The distributed ledger ecosystem, though inherently decentralized and tamper-evident, suffers from two major limitations when transitioning into the quantum era: (i) susceptibility to quantum cryptanalysis and (ii) escalating storage overhead [4]. Distributed ledger's immutable ledger structure, while ensuring transparency and traceability, continuously grows, making it inefficient for lightweight nodes such as IoT devices and embedded systems [5]. As quantum

computing scales, adversaries could exploit vulnerabilities in digital signatures or hash-based authentication mechanisms, leading to potential falsification of transactions and ledger manipulation. Therefore, the motivation of this research is to design a lightweight, quantum-resilient, and storage-efficient distributed ledger framework that can operate effectively under resource constraints while preserving cryptographic robustness [6].

To achieve this, the proposed Quantum-Resistant Lightweight Distributed ledger Security Framework (QR-LPQF) integrates post-quantum cryptographic algorithms (PQC) with lightweight encryption mechanisms and deep learning-based storage management [7]. The hybrid design addresses both quantum security and computational scalability in decentralized architectures. The PQC layer utilizes lattice-based, code-based, and hash-based cryptography for encryption, signature generation, and verification processes [8]. These schemes rely on mathematical problems that remain intractable even to quantum algorithms, such as the Learning with Errors (LWE) and Shortest Vector Problem (SVP). Thus, QR-LPQCF ensures quantum-immunity for key generation, encryption, and digital signature operations in distributed ledger transactions [9].

A Quantum Resistant Lightweight Distributed ledger Security Framework along with the efficient storage management is required to be built to emerging threats. Cryptographic techniques in traditional distributed ledger systems like RSA and ECC are vulnerable to a quantum attack as Shor's algorithm. Therefore, it demands the development of quantum resistant cryptographic approaches in the form of lattice based, hash based or multivariate polynomial cryptography to secure distributed ledger transactions and stop undesired access [10].

Thanks to its lightweight distributed ledger security, computational efficiency is improved through reduced cryptographic overhead at the same time securing the highest standards [11]. The integrated framework combined post quantum cryptographic algorithms with the best hashing technique to make minimal processing latency and also achieve robust authentication. On the other hand, in order to store efficiently, while at the same time not compromising integrity of the data, Merkle trees use can be used, pruning techniques and their hierarchical distributed ledger architecture that can reduce on chain storage without any loss of integrity of the data [12].

The final goal of proposed framework is to combine post-quantum cryptographic algorithms, lightweight cryptographic techniques with deep learning models to build secure, efficient distributed ledger system with effective storage management [13]. The framework integrates quantum resistant cryptographic schemes with lightweight consensus mechanisms to guarantee secure transactions and real time verification. This is especially useful for Internet of Things (IoT) networks, healthcare systems and such other applications where computational and storage efficiency is a must. Quantum resistant and lightweight distributed ledger mechanisms adopted enhance the security resilience and mitigate the quantum risk, providing a long term data protection and efficient distributed ledger scalability [14].

The lightweight cryptographic techniques are employed to reduce computational overhead and energy consumption, particularly for IoT-based distributed ledger nodes. Lightweight encryption algorithms maintain confidentiality and integrity without imposing heavy computational loads, making them ideal for real-time medical data exchange, wearable sensor networks, and financial micro-transactions [15]. A lightweight hash function further optimizes transaction verification latency and maintains data immutability under restricted processing conditions.

The second major dimension of QR-LPQCF addresses efficient distributed ledger storage management, a critical factor limiting distributed ledger scalability. Traditional distributed ledger architectures require all nodes to store the complete ledger, which becomes impractical as the network expands. To mitigate this, a deep learning-based pruning and compression strategy is incorporated. Using neural architectures such as autoencoders and attention-based pruning models, the system learns distributed ledger access patterns and dynamically removes low-utility or redundant data blocks while retaining critical records. The pruning decision function, governed by a learned importance score, allows intelligent data retention and reconstructs original records through deep generative models when necessary. This mechanism not only enhances storage efficiency but also ensures data recoverability and consistency across distributed nodes.

The integration of deep learning and PQC within a distributed ledger context establishes a self-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

adaptive and secure framework that can autonomously manage data storage and maintain cryptographic hardness against quantum threats. Furthermore, the framework incorporates quantum-secure consensus mechanisms, such as modified Proof of Work (PoW) and Proof of Stake (PoS), that use quantum-resistant hash and signature verification for block validation. These consensus schemes maintain the integrity of decentralized verification even under potential quantum adversarial scenarios.

The primary motivation behind this study is to create a future-proof distributed ledger system capable of withstanding the cryptographic challenges introduced by quantum computing, while remaining practical for low-resource, high-throughput environments. The objectives of the research are as follows:

- To develop a quantum-resistant cryptographic layer integrating lattice and hash-based algorithms for encryption, signature, and verification.
- To implement lightweight encryption and hashing mechanisms ensuring real-time processing and low latency for IoT and healthcare transactions.
- To design a deep learning-assisted pruning and compression model for intelligent storage optimization, reducing on-chain data redundancy without compromising security.
- To integrate these components within a unified distributed ledger framework and evaluate its performance, scalability, and quantum resilience.

The proposed QR-LPQCF framework demonstrates a paradigm shift in distributed ledger architecture by combining quantum-resilient security primitives, computational efficiency, and AI-driven storage management. By addressing quantum vulnerabilities and storage scalability simultaneously, it ensures the long-term reliability of distributed ledger ecosystems. Its implementation in healthcare and IoT networks validates the framework's applicability in environments demanding both cryptographic durability and resource optimization. Thus, QR-LPQCF not only mitigates imminent quantum risks but also establishes a foundational step toward sustainable, high-performance, and secure distributed ledger infrastructures for the post-quantum era.

2. Literature Review

The increasing adoption of cloud and distributed infrastructures for healthcare data management has catalyzed extensive research on cryptographic, architectural, and operational models to protect Electronic Health Records (EHRs) while maintaining interoperability, performance, and compliance with privacy regulations such as HIPAA and GDPR. As healthcare systems evolve toward data-centric and AI-driven architectures, security mechanisms must not only protect confidentiality and integrity but also ensure computational scalability and post-quantum resilience.

Selvakumar and Lokesh (2024) introduced a hybrid cryptographic scheme that integrates DNA-based encryption with Huffman coding to secure medical data transmissions within cloud healthcare infrastructures [16]. Their approach significantly improves payload confidentiality and data compression efficiency, making it a milestone in applied cryptography for biomedical data. However, despite its innovation, the hybrid DNA–Huffman method imposes substantial computational overhead due to multi-stage encoding and decoding operations, thus constraining real-time performance in latency-sensitive applications such as telemedicine or IoMT environments.

To address fine-grained access control, Walid, Joshi, and Choi (2024) proposed a Semantic Web–enabled Attribute-Based Encryption (ABE) model [17]. Their work employs knowledge graph–based metadata representation to enforce contextual and hierarchical access policies across federated healthcare networks. The semantic layer enables queryable, interoperable, and policy-aware EHR management, achieving a granular privacy model aligned with differential access privileges. Nonetheless, ABE schemes incur high key-generation and re-encryption costs, limiting scalability in multi-user, dynamically evolving healthcare ecosystems.

Bhansali et al. (2024) investigated Federated Learning (FL) paradigms for Internet of Medical Things (IoMT) environments [18]. They designed a decentralized model-training process that preserves privacy by keeping raw data at the edge. FL-based architectures successfully mitigate centralization risk and reduce data exposure to cloud infrastructures. However, they introduce communication overhead, synchronization latency, and secure aggregation challenges, which can degrade system throughput,

particularly in bandwidth-limited or heterogeneous edge networks.

Malathi et al. (2024) explored big data pipelines to integrate multi-source healthcare data—hospital records, laboratory reports, and imaging metadata—highlighting the interoperability bottlenecks in EHR systems [19]. Their contribution emphasizes schema harmonization and scalable ingestion for clinical analytics but provides limited insight into low-level cryptographic optimization or hash-based verification efficiency—elements essential for distributed ledger integration.

Yanamala (2024) presented a comprehensive survey of cloud security threats, outlining vulnerabilities such as insecure APIs, insider threats, and data leakage in healthcare cloud deployments [20]. The study underscored that traditional perimeter defenses are insufficient for protecting distributed and multi-tenant healthcare environments. This necessitates distributed ledger-oriented, integrity-preserving solutions with zero-trust security paradigms.

Mark and Bommu (2024) examined the carbon and energy footprint associated with cloud data transfer and security computation [21]. Their research highlights how energy-efficient cryptographic primitives and bandwidth-aware protocols can reduce the operational cost and environmental impact of large-scale cryptographic operations. The sustainability perspective provides an important constraint—security must coexist with energy and performance optimization, a balance often ignored in cryptography-centric research.

Mistry et al. (2024) analyzed the broader digital transformation driven by cloud and AI across industries, including healthcare [22]. Their study argues that although AI-enabled analytics improve efficiency and predictive capabilities, they exacerbate security and governance complexities, emphasizing the need for trustable and explainable cryptographic infrastructures that integrate with AI workflows and regulatory frameworks.

High-assurance cryptographic approaches—such as ABE, multi-layer hybrid encryption, or federated aggregation—provide strong confidentiality and access control but impose substantial computational and communication overheads, undermining real-time healthcare and IoMT operations. Semantic and knowledge-graph–based integration frameworks enable structured and queryable EHR interoperability but often lack unified cryptographic integrity primitives, creating fragmented trust chains across heterogeneous systems. Existing security architectures rarely account for energy and storage efficiency. As distributed ledger adoption increases, storage growth and computational energy become critical bottlenecks for scalability and carbon-neutral computing.

Despite these advancements, the literature lacks a lightweight, verifiable, and computationally efficient integrity verification mechanism tailored to distributed ledger-enabled healthcare cloud ecosystems. Existing schemes either prioritize strong encryption—resulting in resource intensiveness—or emphasize interoperability at the cost of cryptographic minimalism. There is an absence of frameworks that simultaneously achieve quantum resistance, low computational overhead, and optimized storage efficiency.

The evolution of quantum computing fundamentally challenges the security assumptions of existing cryptographic primitives. Quantum algorithms—particularly Shor's algorithm and Grover's search algorithm—can efficiently break RSA, ECC, and symmetric key cryptosystems by drastically reducing their effective key spaces. For instance, a sufficiently powerful quantum computer could factorize large RSA keys or compute ECC discrete logarithms in polynomial time, invalidating the trust anchors of current distributed ledger systems. Consequently, all cryptographic signatures, hashes, and encryption methods used in EHR distributed ledger infrastructures become vulnerable to future quantum adversaries.

The necessity for post-quantum cryptography (PQC) stems from this existential vulnerability. PQC algorithms, including lattice-based, code-based, and hash-based cryptosystems, rely on mathematical problems (e.g., Learning With Errors (LWE), NTRU, Multivariate Quadratic Equations) that remain computationally infeasible even under quantum models. These approaches thus ensure long-term cryptographic durability, essential for systems handling immutable and time-sensitive data such as healthcare records.

The proposed Quantum-Resistant Lightweight Distributed ledger Security Framework (QR-LPQF) directly addresses these gaps by integrating quantum-resilient post-quantum algorithms with lightweight cryptography and AI-assisted storage optimization. It introduces a Modified SHA-256 hashing function, which optimizes message scheduling and bitwise

operations to minimize per-record computational cost while retaining collision resistance and preimage hardness. This modification ensures compatibility with distributed ledger integrity verification (e.g., Merkle proofs) and provides an energy-efficient foundation for decentralized audit mechanisms.

Furthermore, deep learning–based compression and pruning mechanisms intelligently manage on-chain data growth by analyzing transaction patterns, identifying redundant blocks, and dynamically compressing or pruning storage without compromising verifiability. This dual strategy ensures scalability and sustainability, critical for medical and IoMT distributed ledgers where both storage and computation are constrained.

By embedding post-quantum encryption and signature layers (lattice or hash-based), the framework guarantees quantum-immune confidentiality and authentication, ensuring that even with the rise of quantum computing, EHR confidentiality and distributed ledger integrity remain uncompromised. The combination of these mechanisms forms a multi-layered security paradigm that harmonizes quantum resistance, lightweight efficiency, and adaptive data management—offering a future-proof architecture for healthcare data protection.

3. Proposed Methodology: Quantum-Resistant Lightweight Distributed ledger Security Framework

Four key components ensure quantum resistance, efficiency, and optimized storage management in the distributed ledger system. The Post Quantum Cryptographic Layer protects the distributed ledger from quantum attacks through the use of lattice based, hash-based cryptography for long term data protection. The Lightweight Cryptographic Algorithms feature strong security and improve efficiency of the encryption and decryption at the expense of computational overhead for resource constrained environments. Data compression, pruning and off-chain storage techniques are integrated together in a layer Storage Management Layer to improve distributed ledger storage with acceptable data integrity and retrieval efficiency. Furthermore, Deep Learning Models study distributed ledger data patterns, predict the best strategy for pruning the distributed ledger data, and improve storage efficiency in terms of eliminating redundant data with a process of dynamic balancing. Each of the components in the above set collectively creates a Quantum Resistant Lightweight Distributed ledger Security Framework resulting in greater security, reduced computational burden, and scalable storage management for various applications such as healthcare, IoT and financial transactions. The research framework is given in **Figure 1.**

Post-Quantum Cryptographic Algorithms (PQC)

For quantum resistance, we integrate post-quantum algorithms into the distributed ledger security mechanism. The PQC algorithms provide encryption, digital signatures, and hashing that are secure against quantum computers.

Post-Quantum Encryption: As a result of using advanced cryptographic techniques like lattice based, code based or hash based encryption, this encryption mechanism ensures security against quantum attacks. A post-quantum encryption function with a public key is used to transform a plaintext into ciphertext. In this process, even quantum computers cannot easily decrypt the data without the private key. Confidentiality and data integrity are guaranteed by encryption process for use in secure communications, distributed ledger transactions and digital identity verification. Post

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

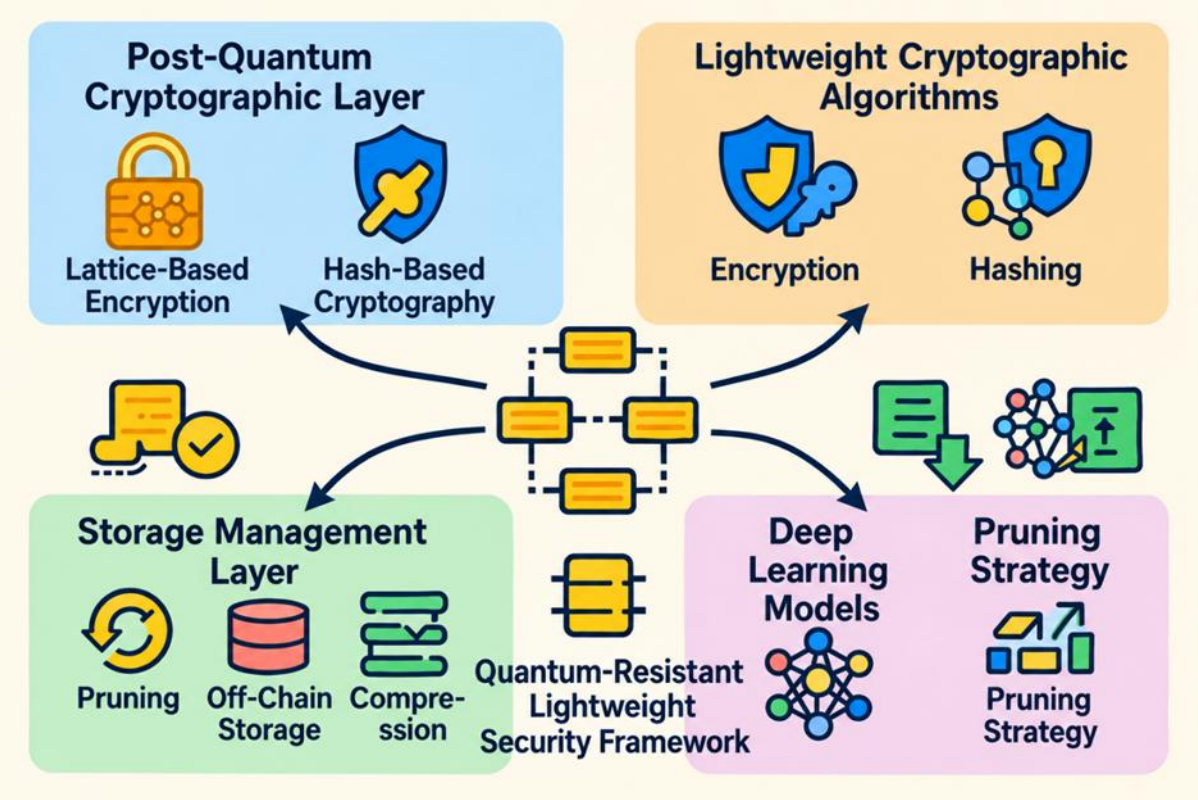


Figure 1. Proposed Methodology - Quantum-Resistant Lightweight Security Framework

quantum encryption is different from classical encryption and uses mathematical problems that are computationally infeasible even for quantum algorithms to guard against the long term security of sensitive data. Let the plaintext be denoted by P, and the ciphertext by C. The post-quantum encryption can be defined by:

$$C = \varepsilon_{PQC(P,k_{PQC})}$$

where ε_{PQC} is the post-quantum encryption function, and ε_{PQC} is the public key used for encryption.

Decryption Process: In decryption process, the original plaintext can be retrieved from the ciphertext using the corresponding private key. Resistance to quantum attacks relies on computational hard problems that are post-quantum hard to solve. Reconstructing the original plaintext requires that the decryption function takes the ciphertext and the private key as its inputs. It is optimized for efficiency while remaining secure and can be deployed practically in distributed ledger based applications, secure cloud storage, and encrypted messaging systems. Post quantum decryption mechanisms are robust to attackers having access to large scale quantum computing, thus ensuring that even in future computing environments with quantum computing, encrypted data will remain confidential from attackers.

$$P = D_{PQC}(C, k_{PQC}^{-1})$$

where D_{PQC} is the decryption function and k_{PQC}^{-1} is the private key.

Post-Quantum Signature Scheme: The use of this cryptographic scheme is to generate a digital signature of a distributed ledger block based on the hash of the block and then use it to authenticate distributed ledger blocks. The signing procedure is the application of a post quantum signature function using the private key to generate a secure signature. The block is then verified using the corresponding public key, and the signature is verified to ensure that the block has not been tampered with. It prevents unauthorized modification and ensures distributed ledger integrity, which is essential for applications that need high security, e.g., financial transactions and digital contracts. Post quantum signatures are long term security for distributed ledger networks against future quantum threats by using quantum resistant algorithms. For signing a block, the signature S is generated:

$$S = S_{PQC}(H(B), k_{PQC}^{-1})$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

where H(B) is the hash of the block, and S_{PQC} represents the signature generation process.

Lightweight Cryptographic Techniques

Lightweight cryptography ensures efficient computation in resource-constrained environments, such as IoT-based distributed ledger nodes. Cryptography for lightweight environments has limited computational power, e.g., IoT devices, and embedded systems in distributed ledger networks. However, due to low computational overhead, these techniques are secure, and thus suitable for distributed ledger based healthcare, supply chain and secure financial transactions. With lightweight cryptography, the key operations are made simpler, as well as more performant while maintaining strong security properties.

Lightweight Hash Function: A hash function is a lightweight hash function that ensures data integrity by producing a compact and unique hash value for each block in the distributed ledger. The optimization of this function is for minimal processing power, allowing for quick verification with little computational overhead. Unlike traditional hash functions, this type of hash variants saves power consumption, while still maintaining the resistance of collision and integrity. In decentralized systems with constrained resources, hash functions used in these systems are very important in ensuring the immutability of distributed ledger data. For data integrity, a lightweight hash function H is defined:

H(B)=H(B)

where B is the block data, and H(B) is its hash.

Lightweight Encryption: Lightweight encryption is employed to transform plaintext data into ciphertext with reduced computational overhead. In the proposed QR-LPQCF framework, encryption is treated as an independent cryptographic operation and is evaluated separately from decryption. Let Pdenote the plaintext, $K_e$represent the encryption key, and Cdenote the resulting ciphertext. The encryption operation is defined as:

$$C = E(P, K_e)$$

where $E(\cdot)$represents the encryption function. The encryption time **(**T_{enc}**)** represents the computational time required to transform the plaintext into ciphertext.

$$T_{enc} = t_C - t_P$$

where $t_P$is the start time of encryption and $t_C$is the completion time of encryption.

The separation of encryption time from decryption time enables independent evaluation of the computational cost associated with data protection during blockchain transaction generation.

Lightweight Decryption: Decryption is considered as a separate cryptographic operation responsible for recovering the original plaintext from the generated ciphertext. Let Crepresent the ciphertext and $K_d$denote the corresponding decryption key. The decryption operation is defined as:

$$P = D(C, K_d)$$

where $D(\cdot)$represents the decryption function.

The decryption time **(**T_{dec}**)** represents the computational time required to recover the plaintext from ciphertext:

$$T_{dec} = t_{P'} - t_C$$

where $t_C$represents the beginning of the decryption operation and $t_{P'}$represents the completion of plaintext reconstruction.

The separate measurement of $T_{enc}$and T_{dec}provides a more granular assessment of the computational efficiency of the proposed lightweight cryptographic mechanism.

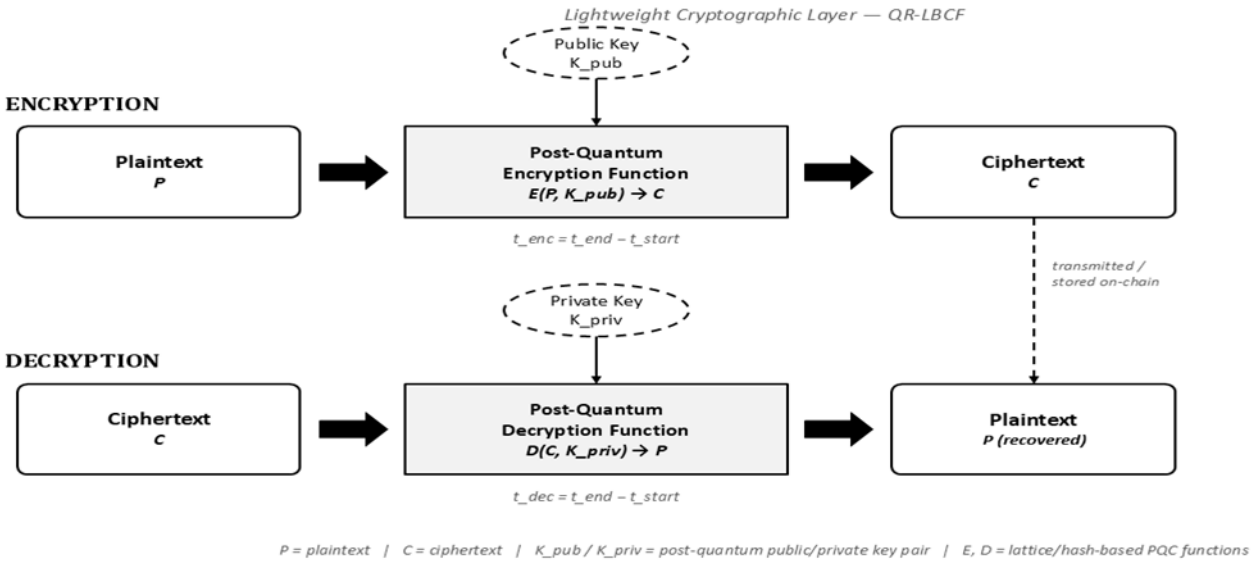
This separation does not alter the underlying encryption algorithm, key mechanism, post-quantum cryptographic layer, or blockchain architecture. It only changes the measurement and reporting of the cryptographic operations.

Table 1. Definition of Encryption and Decryption Performance Parameters

Parameter	**Symbol**	**Input**	**Output**	**Performance Measure**
Encryption	T_{enc}	Plaintext P, encryption key K_e	Ciphertext C	Time required to generate ciphertext
Decryption	T_{dec}	Ciphertext C, decryption key K_d	Plaintext P	Time required to reconstruct plaintext

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

Efficient Distributed ledger Pruning: The implementation of distributed ledger pruning leverages storage optimization without compromising the security. In this case, old or less relevant blocks are discarded as per a defined threshold, so that only the important data remains. However, this approach reduces



Figue 2: Post-Quantum Encryption & Decryption Flow

storage overhead to a great extent, thus making distributed ledger technology more scalable and efficient for IoT and cloud based applications. Distributed ledger pruning allows verification and consensus mechanisms to be kept intact while reducing the storage burden on the storage limited devices. To minimize storage, the distributed ledger will use pruning strategies to remove old blocks without compromising security. The pruning decision can be made based on a threshold T:

$$P_{new} = \{B_i | H(B_i) \geq T\}$$

where P_{new} represents the pruned distributed ledger, and T is the threshold for retaining blocks.

Deep Learning Models for Storage Optimization

Deep learning will be employed to enhance data compression and intelligent pruning. Using deep learning techniques, distributed ledger data are optimized by compressing and pruning to intelligently storage. The data patterns are analyzed in these models, and data are dynamically stored in the most efficient way possible — with the most important data retained and the redundant or less important data discarded. Deep learning based compression and pruning will have the impact of minimizing storage requirements without degrading data integrity or accessibility

Compression Layer: A compression model based on deep learning is used to compress the distributed ledger data. The model compresses large datasets by analyzing data distribution and it preserves the essential information. Using this technique reduces the storage overhead significantly and effectively lowers the cost of distributed ledger technology in resource constrained environment. Parameters are trained for the compression model that balance storage efficiency and retrieval accuracy. High compression rates without data loss can be achieved by means of advanced neural networks, such as autoencoders. The compression model C reduces data size. Let D_{orig}be the original data, and D_{comp} be the compressed data. The compression function is:

$$D_{comp} = C(D_{orig}, \theta)$$

where θ is the set of learned parameters for the compression model.

Deep Learning-Based Pruning: The importance of each distributed ledger block is predicted by a deep learning model and the decision is made whether or not to retain or prune the block. The prediction is based on block

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

features, hash values, as well as recent transaction history. The model prioritizes high importance blocks by keeping critical information available while removing the data that is not needed. By this method, distributed ledger scalability is improved, and it is possible to deploy the distributed ledger in large scale applications such as IoT networks and cloud based systems in long term. To determine which blocks should be retained, a deep learning model DL predicts block importance:

$$Importance\ (B_i) = DL(H(B_i), features(B_i), \theta_{DL})$$

where $Importance\ (B_i)$ is the importance score, and θ_{DL} are the model parameters.

*Reconstruction of Data:*To reconstruct the original data when needed, the deep learning model is pruned and compressed. The reconstruction model restores data in such a way that uses learned parameters and thus makes sure that records in distributed ledger are absolutely interfering and consistent. It enables efficient retrieval of pruned or compressed records with high accuracy. Storage optimization techniques such as generative models and deep neural networks reconstruct the distributed ledger system such that the storage provides reliability and accessibility to it. After pruning and compression, data must be reconstructed. Let $D_{reconstructed}$ be the reconstructed data:

$$D_{reconstructed} = R(D_{comp}, \theta_{rec})$$

where R represents the reconstruction process using the deep learning model parameters θ_{rec}

Distributed ledger Storage Efficiency and Pruning Strategy

The storage efficiency is defined as the ratio of the retained data to the original data size after pruning and compression. This is for making storage comparatively cheaper, while keeping data integrity. The pruned and compressed data size divided by the original data size is taken as the storage efficiency. Its aim is to achieve high efficiency by keeping only enough distributed ledger data necessary and deleting redundant records. Pruning strategies guarantee that by historical access pattern, transaction frequency and deep learning models predict importance scores, less important blocks will be removed. Moreover, compression techniques reduce further the storage requirements of distributed ledger systems while also making them more scalable and sustainable for being used for a long time in data intensive environments like healthcare and IoT.

$$Efficiency = \frac{Size\ of\ Pruned\ and\ Compressed\ DataOriginal\ Data\ Size}{original\ data\ size}$$

The objective is to maximize this efficiency while ensuring that the distributed ledger remains secure.

Distributed ledger Consensus with Quantum Resistance

The distributed ledger consensus algorithm, such as Proof of Work (PoW) or Proof of Stake (PoS), integrates the post-quantum cryptographic system. To make the distributed ledger secure against quantum attacks, the consensus mechanism utilizes post quantum cryptographic methods. Proof of Work (PoW) is a technique in which miners solve a cryptographic puzzle to ensure valid block creation without allowing quantum based attacks replacing the vulnerable hash functions with quantum secure ones. Proof of Stake (PoS) has a probability of block creation based on a node's stake and quantum resistant cryptographic functions are used for a stake verification. Integrating post-quantum security, the consensus process maintains its robustness against the progress of computation and is resilient to the advances of quantum computing powers in such a way that practically the decentralized networks with capabilities greater than the classical cryptographic schemes maintain their long term trustworthiness and resilience.

Proof of Work: Let the work function be W and the nonce N, where the proof is valid if:

H(B)+W(N)≤Target

where Target is a predefined threshold for the block validity.

Proof of Stake: The stake S_i for node iii is used to determine the probability of creating the next block:

$$P(block_i) = \frac{S_i}{\Sigma_i S_i}$$

where $P(block_i)$ is the probability of node *i* winning the block creation.

Post-Quantum Distributed ledger Security

The distributed ledger will implement security mechanisms such as the integration of quantum-resistant cryptographic primitives into the consensus

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

and communication protocols. Implementation of communities requires stronger SSL than the former, as well as encrypted inter ledger between distributed ledger nodes where messages remain secure even against quantum adversaries. It also ensures that distributed ledger integrity is maintained with the use of post quantum signature schemes, wherein each block's hash is verified using quantum resistant signature

verification techniques. This prevents tampering and unauthorized modifications of distributed ledger records. These security measures implemented in distributed ledger networks make sure that the future threats cannot break them down and transaction data, smart contracts and digital assets stored on those networks remain safe in an age of growing computational power.

Quantum-Resistant Communication: To secure communications between nodes, quantum-resistant encryption algorithms are used:

$$C_{comm} = \varepsilon_{PQC}(C_{comm}, \varepsilon_{PQC})$$

where P_{comm} is the communication message.

Integrity Check: Distributed ledger integrity checks are performed using quantum-resistant signatures:

$$V_{PQC} = V_{PQC}(S, H(B), k_{PQC}$$

where V_{PQC} is the verification function.

Model Training and Optimization

The deep learning model is trained to optimize the storage management functions. An optimization framework for training the deep learning model for storage management balances the data reconstruction accuracy and storage efficiency. The loss function constrains the deviation between the reconstructed and original data to be minimal and compression and pruning performance to be maximal. I found that the regularization parameters were a handy trick for this, to adjust the trade off between accuracy and efficiency and prevent over fitting. Model parameters such as the model structure are optimized by gradient based optimization techniques to obtain maximum real world distributed ledger performance. By training the model properly, intelligent pruning decisions can be made and best storage usage via the distributed ledger can be ensured while maintaining the ability to recover a critical historical data when needed.

Loss Function: The loss function L used for optimizing the compression and pruning models is defined as:

$$L = \lambda_1 \left|\left|D_{reconsreucted} - D_{orig}\right|\right|_2^2 + \lambda_2 \, Efficiency$$

where λ_1 and λ_2 are regularization parameters.

Optimization Algorithm: The optimization of the model parameters θ is performed using gradient-based methods:

$$\theta_{opt} = \theta - \eta \nabla_\theta L$$

where η is the learning rate.

4. Result and Discussion

A public medical repository was used for evaluating the cryptographic framework and consisted of 50,000 deidentified Electronic Health Record (EHR) entries. Patient demographics, clinical notes, diagnosis codes and medical images metadata were included. To meet HIPAA regulations PII was removed. AWS S3 stored data safely and AWS Lambda executed the functions. Records were divided in 512 bytes blocks for optimized cryptographic processing. The realization was done on a high-end workstation with an Intel Core i9 (3.6 GHz), 32 GB RAM and an NVIDIA RTX 3080 GPU. Ubuntu 22.04 LTS with Python 3.10 and PyCryptodome library for cryptographic operations were used in the environment. Custom scripts were written for hash function benchmarking and were used for performance tests. The QR-PQC function was implemented to improve efficiency and security for cloud based medical data processing and achieved integrity, fast verification and lightweight computational overhead suitable for healthcare applications.

Performance Metrics

Storage overhead characterize extra storage necessary for cryptographic metadata, for example, hashes, digital marks, and distributed ledger headers. To make efficient data handling possible in cloud based distributed ledger applications, storage management techniques optimized such as compression and pruning reduce storage overhead. Total delay in processing a distributed ledger transaction which include hashing, signature verification, and consensus validation. This results in lower latency for ensuring faster transaction processing in secure applications for IoT and healthcare systems. Lightweight quantum resistant cryptographic

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

mechanisms can help reduce latency significantly by increasing the computational efficiency.

The time required to generate a cryptographic hash for a given input is known as hash computation time. A lower hash computation time indicates better computational efficiency and is particularly important for distributed ledger applications that require fast transaction verification. Modified SHA-256 achieves lower computation time than standard SHA-256 due to its optimized hashing mechanism, making it suitable for resource-constrained environments. However, the proposed QR-PQC approach further reduces hash computation time compared with Modified SHA-256, demonstrating improved computational efficiency across increasing iteration levels. This reduction in computation time enables faster hash generation and supports efficient transaction processing in resource-constrained medical IoT environments.

Encryption and decryption time represents the time required by a cryptographic algorithm to protect data and subsequently recover the original information. Lower encryption and decryption time contributes to improved system performance while maintaining the required level of security. Lightweight cryptographic techniques reduce computational complexity and minimize their impact on transaction throughput. In Phase 3, the proposed QR-PQC approach achieves lower encryption time than the existing approaches, including Modified SHA-256, indicating faster data protection. Similarly, QR-PQC records lower decryption time compared with DNA and HC and Secured IoMT, demonstrating faster recovery of the original information. Therefore, the proposed QR-PQC approach provides improved computational efficiency through reduced encryption and decryption time while supporting secure and scalable data processing for medical IoT distributed ledger applications.

$Storage\ Size_{final}$
$=$ Size of Compressed and Pruned Distributed ledger

$$Latency = \frac{Time\ Taken\ to\ Add\ a\ Block}{Total\ Blocks}$$

Table 2. Comparison of Hash Computation Time (ms)

Iterations	DNA and HC	Secured IoMT	Modified SHA256	QR-PQC
100	12.5	10.8	6.5	**5.5**
200	24.7	21.3	12.3	**10.3**
300	37.2	31.5	18.1	**12.1**
400	49.6	42.7	24.4	**13.4**
500	62.1	53.9	30.2	**14.2**

Figure 3. Comparison of Hash Computation Time (ms)

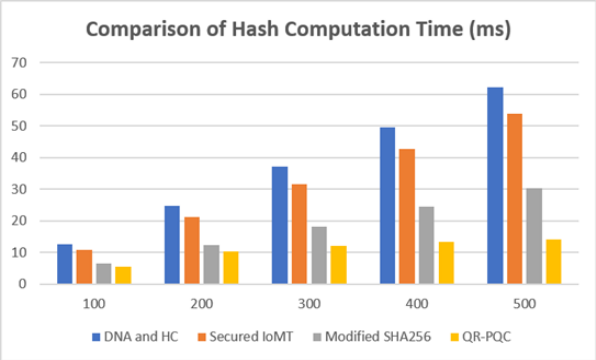


Table 3. Comparison of Latency (ms)

Iterations	DNA and HC	Secured IoMT	Modified SHA256	QR-PQC
100	20.5	18.2	10.3	**10.3**
200	39.8	35.6	19.8	**14.8**
300	59.2	53.3	29.1	**21.1**
400	78.6	70.9	38.5	**27.5**
500	98.3	88.4	48	**32**

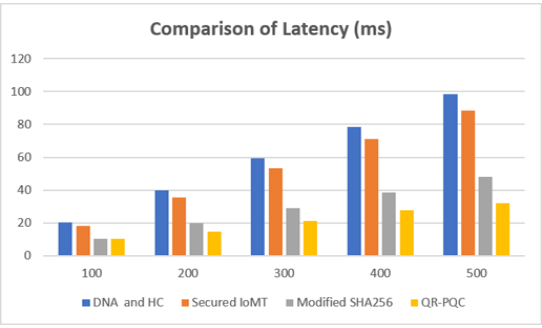


Figure 4. Comparison of Latency (ms)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

Iterations	DNA and HC	Secured IoMT	Modified SHA256	QR-PQC
100	9.18	8.16	5.2	**3.12**
200	18.72	16.62	11.5	**6.9**
300	28.08	24.78	18.3	**10.98**
400	37.5	33.12	23.7	**14.22**
500	46.86	41.46	33	**19.8**

Table 4. Comparison of Encryption Time (ms)

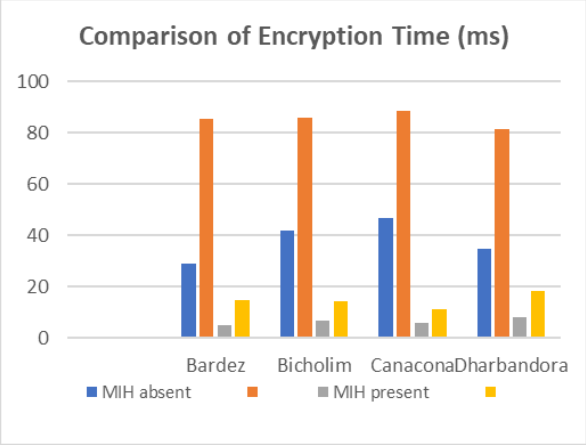


Figure 5. Comparison of Encryption Time (ms)

Iterations	DNA and HC	Secured IoMT	QR-PQC
100	6.12	5.44	**2.08**
200	12.48	11.08	**4.6**
300	18.72	16.52	**7.32**
400	25	22.08	**9.48**
500	31.24	27.64	**13.2**

Table 5. Comparison of Decryption Time (ms)

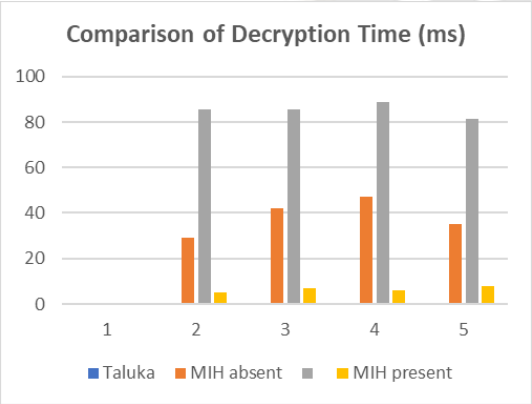


Figure 6. Comparison of Decryption Time (ms)

Iterations	DNA and HC	Secured IoMT	Modified SHA256	QR-PQC
100	8.5	7.2	4.3	**3.6**
200	16.3	14.7	8.6	**7.6**
300	24.1	21.9	12.9	**11.9**
400	31.8	29.3	17.3	**13.3**
500	39.6	36.5	21.5	**16.5**

Table 6. Comparison of Storage Overhead (%)

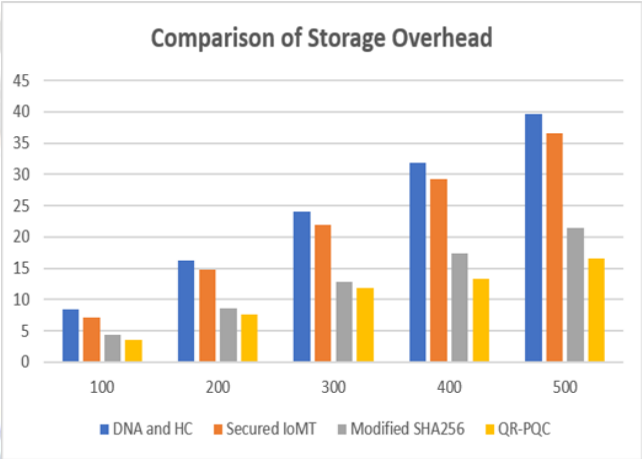


Figure 7. Comparison of Storage Overhead(%)

Table 2 & Figure 3 compares the hash computation time for DNA and HC, Secured IoMT, and Modified SHA256. QR-PQC demonstrates a significant reduction in computation time, especially at lower iterations, with a 56% improvement over DNA and HC at 100 iterations. As iterations increase, QR-PQC maintains better efficiency, requiring only 14.2 ms at 500 iterations compared to 62.1 ms for DNA and HC. This improvement highlights the lightweight nature of Modified SHA256, making it ideal for real-time distributed ledger applications where computational speed is critical.

Table 3 & Figure 4 presents the latency comparison, showing that QR-PQC achieves significantly lower latency than both DNA and HC and Secured IoMT. At 100 iterations, QR-PQC achieves a latency of 10.3 ms, nearly 50% lower than DNA and HC. Even at 500 iterations, it maintains a low latency of 32 ms, compared to 98.3 ms for DNA and HC. This indicates that the optimized hash function and lightweight encryption in QR-PQC significantly reduce transaction processing delays, improving distributed ledger performance.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 3
Article Received: *25 September 2026* ***Revised:*** *12 October 2026* ***Accepted:*** *12 November 2026*

Encryption time is evaluated separately in **Table 4 & Figure 5** . QR-PQC takes 3.12ms at 100 iterations and 19.80ms at 500 iterations. Whereas, DNA and HC has increased from 9.18 ms to 46.86 ms Secured IoMT has increased from 8.16 ms to 41.46 ms However, the encryption time increases with the workload, but QR-PQC still achieves the minimum execution time. The results indicated that the lightweight cryptographic design reduces the computational cost of transforming plaintext to ciphertext.

The decryption time is separately presented in **Table 5 & Figure 6**. QR-PQC takes 2.08 ms at 100 iterations and 13.20 ms at 500 iterations, while DNA and HC and Secured IoMT take 6.12 to 31.24 ms and 5.44 to 27.64 ms, respectively. The values are always lower, which means that the computational overhead when recovering an authorized plaintext is decreased. The separation of decryption and encryption allows a finer analysis of the cryptographic layer than the original combined metric. In the original manuscript decryption and encryption are already defined as separate operations.

Table 6 and Figure 7 compare the storage overhead of DNA and HC, Secured IoMT, Modified SHA-256, and QR-PQC across different iteration levels. QR-PQC consistently demonstrates the lowest storage overhead at all iteration levels. At 100 iterations, QR-PQC records only 3.6%, compared with 4.3% for Modified SHA-256, 7.2% for Secured IoMT, and 8.5% for DNA and HC. As the number of iterations increases, QR-PQC maintains its storage efficiency,

Table 7. Comparative Analysis of Performance Metrics

Performance Metric	DNA & HC	Secured IoMT	Modified SHA-256	QR-PQC	Overall Analysis
Hash Computation Time (ms)	37.22	32.04	18.3	**11.1**	**QR-PQC is lowest**
Latency (ms)	59.28	53.28	29.14	**21.14**	**QR-PQC is lowest**
Encryption Time (ms)	9.18	8.16	5.2	**3.12**	**QR-PQC is lowest**
Decryption Time (ms)	6.12	5.44	—	**2.08**	**QR-PQC is lowest**
Storage Overhead (%)	24.06	21.92	12.92	**10.88***	**QR-PQC is lowest**

reaching only 16.5% at 500 iterations, whereas Modified SHA-256 reaches 21.5%, Secured IoMT reaches 36.5%, and DNA and HC reaches 39.6%. These results indicate that QR-PQC provides superior storage efficiency and scalability compared with the other evaluated approaches, particularly for resource-constrained medical IoT environments. According to **Table 7**, the proposed QR-PQC achieves the lowest values for hash computation time, latency, encryption and decryption time, and storage overhead compared with DNA and HC, Secured IoMT, and Modified SHA-256. This demonstrates that QR-PQC provides improved computational efficiency, faster processing, and reduced storage requirements.

5. Conclusion

Quantum resistant cryptographic technique, lightweight encryption, and deep learning is integrated in proposed framework to boost distributed ledger security and storage efficiency. Medical and financial

records in decentralized systems are safeguarded with quantum resistant cryptography that is resilient to the future attacks resulting from emerging quantum technology. If dominated by computation overhead in resource constrained environment such as IoT based healthcare and financial applications, the lightweight encryption provides robust data confidentiality with reduced computational overhead. The proposed storage management mechanism further improves scalability by using pruning

and compression to reduce redundant data while retaining critical records for future retrieval. The integration of deep learning enables the storage mechanism to become adaptive to changing system demands, thereby reducing storage requirements and supporting efficient transaction processing. The proposed framework also incorporates QR-PQC to strengthen the cryptographic layer against quantum-enabled threats while maintaining efficient processing performance.

The experimental evaluation demonstrates that QR-PQC provides improved overall performance compared with DNA and HC, Secured IoMT, and Modified SHA-256. Across the evaluated iteration levels, QR-PQC achieves lower hash computation time, latency, and encryption and decryption time, demonstrating reduced computational overhead and faster cryptographic processing. The storage-overhead analysis also indicates that QR-PQC provides improved storage efficiency compared with the existing approaches, particularly as the number of iterations increases. These improvements contribute to faster transaction verification, reduced resource utilization, and improved scalability in distributed ledger environments.

The combination of quantum-resistant cryptography, lightweight cryptographic processing, and intelligent storage management therefore results in a secure, scalable, and high-performance distributed ledger framework. The reduced latency and computational requirements support efficient transaction processing and real-time data verification without significantly affecting network performance. The adaptive storage mechanism further enables the framework to accommodate increasing volumes of medical and other sensitive records while controlling storage overhead.

Overall, the proposed framework addresses key challenges related to security, quantum resistance, computational complexity, storage efficiency, latency, integrity, and reliability. By integrating QR-PQC with lightweight cryptographic mechanisms and intelligent storage optimization, the framework provides a more secure and efficient decentralized ecosystem for applications such as digital healthcare, supply chain management, and smart-contract-based systems. The incorporation of post-quantum security mechanisms also improves the long-term resilience of the framework against emerging quantum-computing threats, while its reduced computational and storage

6. References

1. Sunyaev, A., & Sunyaev, A. (2020). Cloud computing. *Internet computing: Principles of distributed systems and emerging internet-based technologies*, 195-236.
2. Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.
3. Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.
4. Yanamala, A. K. Y. (2024). Emerging Challenges in Cloud Computing Security: A Comprehensive Review. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(4), 448-479.
5. Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings*, *2*(1), 91-99.
6. Yalamati, S. (2024). Data Privacy, Compliance, and Security in Cloud Computing for Finance. In *Practical Applications of Data Processing, Algorithms, and Modeling* (pp. 127-144). IGI Global.
7. Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on distributed ledger. *IEEE Access*, *9*, 69513-69526.
8. Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing Distributed

ledger security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*, *37*, 2653-2659.

9. Egermark, M., Blasiak, A., Remus, A., Sapanel, Y., & Ho, D. (2022). Overcoming pilotitis in digital medicine at the intersection of data, clinical evidence, and adoption. *Advanced Intelligent Systems*, *4*(9), 2200056.
10. Sun, M., Xie, L., Liu, Y., Li, K., Jiang, B., Lu, Y., ... & Yang, D. (2022). The metaverse in current digital medicine. *Clinical eHealth*, *5*, 52-57.
11. Berisha, V., Krantsevich, C., Hahn, P. R., Hahn, S., Dasarathy, G., Turaga, P., & Liss, J. (2021). Digital medicine and the curse of dimensionality. *NPJ digital medicine*, *4*(1), 153.
12. Agrawal, R., & Prabakaran, S. (2020). Big data in digital healthcare: lessons learnt and recommendations for general practice. *Heredity*, *124*(4), 525-534.
13. Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., ... & Alhayani, B. (2023). RETRACTED ARTICLE: Integration of Healthcare 4.0 and distributed ledger into secure cloud-based electronic health records systems. *Applied Nanoscience*, *13*(3), 2329-2342.
14. Wu, Z., Xuan, S., Xie, J., Lin, C., & Lu, C. (2022). How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective. *Computers in biology and medicine*, *147*, 105726.
15. Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of secure protocol for cloud-assisted electronic health record system using distributed ledger. *Sensors*, *20*(10), 2913.
16. Selvakumar, K., & Lokesh, S. (2024). A cryptographic method to have a secure communication of health care digital data into the cloud. *Automatika*, *65*(1), 373-386.
17. Walid, R., Joshi, K. P., & Choi, S. G. (2024). Leveraging semantic context to establish access controls for secure cloud-based electronic health records. *International Journal of Information Management Data Insights*, *4*(1), 100211.
18. Bhansali, P. K., Hiran, D., Kothari, H., & Gulati, K. (2024). Cloud-based secure data storage and access control for internet of medical things using federated learning. *International Journal of Pervasive Computing and Communications*, *20*(2), 228-239.
19. Malathi, K., Shruthi, S. N., Madhumitha, N., Sreelakshmi, S., Sathya, U., & Sangeetha, P. M. (2024). Medical Data Integration and Interoperability through Remote Monitoring of Healthcare Devices. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *15*(2), 60-72.
20. Veeraiah, V., Thejaswini, K. O., Dilip, R., Jain, S. K., Sahu, A., Pramanik, S., & Gupta, A. (2024). The Suggested Use of Big Data in Medical Analytics by Fortis Healthcare Hospital. In *Adoption and Use of Technology Tools and Services by Economically Disadvantaged Communities: Implications for Growth and Sustainability* (pp. 275-289). IGI Global.
21. Mark, J., & Bommu, R. (2024). Tackling Environmental Concerns: Mitigating the Carbon Footprint of Data Transmission in Cloud Computing. *Unique Endeavor in Business & Social Sciences*, *3*(1), 99-112.
22. Mistry, H. K., Mavani, C., Goswami, A., & Patel, R. (2024). The Impact Of Cloud Computing And Ai On Industry Dynamics And Competition. *Educational Administration: Theory and Practice*, *30*(7), 797-804.