SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Leveraging Quantum Cryptography And Blockchain For Strengthened Data Security In Cloud Infrastructures

Dr. Srinivasan J.[1] , Dr. Sindhu Achuthankutty[2] , Dr. R. Rajkumar[3] , D. Chithra[4] , Dr. Ponmurugan Panneer Selvam[5] , A. Maheswari[6]

[1]Assistant Professor Department of Computer Applications Madanapalle institute of technology & Science(MITs) Deemed to be university Madanapalle. Email: drsrinivasanj@mits.ac.in , ORCHID; 0009-0005-4042-4849
[2]Lecturer Department of Information and Communication Engineering (ICE) International School of Engineering (ISE), Faculty of Engineering Chulalongkorn University, Bangkok, Thailand. Email: sindhu.a@chula.ac.th, ORCID: 0000-0002-0745-4078
[3]Associate Professor Department of Electronics and Communication Engineering Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology Chennai – 600062, Tamil Nadu, India. Email: rajkumarramasami@gmail.com
[4]Assistant Professor Department of Information Technology S.A. Engineering College Chennai, Tamil Nadu, India. Email: chithrad@saec.ac.in, ORCID: 0009-0000-5927-7555
[5]Professor & Dean – Doctoral Studies and IPR Meenakshi Academy of Higher Education & Research (Deemed to be University) Chennai – 600078, Tamil Nadu, India. , Email: murugan.pmsm@gmail.com ORCID: 0000-0003-2212-8219
[6]Assistant Professor Department of Computer Science and Engineering Dr. M.G.R. Educational and Research Institute Maduravoyal, Chennai – 600095, Tamil Nadu, India. Email: maheswari.it@drmgrdu.ac.in, ORCID: 0009-0002-2578-5265

Abstract:
The rapid adoption of cloud infrastructures has intensified concerns regarding data confidentiality, integrity, and trust management, particularly in the presence of emerging quantum computing threats. Classical cryptographic mechanisms, which underpin most existing cloud security architectures, are increasingly vulnerable to quantum attacks capable of compromising public-key encryption and key exchange protocols. To address these challenges, this paper proposes a hybrid security framework that integrates Quantum Cryptography with Blockchain technology to achieve robust, future-resistant data protection in cloud environments. The proposed framework leverages Quantum Key Distribution (QKD) to enable provably secure key generation and exchange based on quantum mechanical principles, ensuring resistance against eavesdropping and computational attacks. Blockchain technology is employed to provide decentralized trust, immutable audit trails, and transparent access control across distributed cloud services. Smart contracts enforce fine-grained security policies, automate authentication, and ensure tamper-proof data access logging. The synergy between quantum cryptography and blockchain establishes a secure key lifecycle, resilient identity management, and verifiable data integrity within multi-tenant cloud infrastructures. Comprehensive security analysis demonstrates that the proposed approach effectively mitigates quantum-enabled attacks, insider threats, and single-point-of-failure vulnerabilities commonly found in traditional cloud security models. Experimental evaluation and comparative analysis highlight improvements in data integrity assurance, key management robustness, and trust transparency, with acceptable computational and communication overhead. The results indicate that integrating quantum cryptography with blockchain presents a scalable and future-proof security paradigm for next-generation cloud infrastructures.

Keywords:
Quantum Cryptography; Quantum Key Distribution (QKD); Blockchain Technology; Cloud Infrastructure Security; Post-Quantum Security; Decentralized Trust Management; Secure Data Storage.

1. Introduction

The rapid evolution of cloud computing has transformed the way data is stored, processed, and shared across industries by offering scalable, cost-effective, and on-demand computing resources. Cloud infrastructures support a wide range of critical applications, including healthcare systems, financial services, smart cities, and large-scale Internet of Things (IoT) platforms. However, the centralized and distributed nature of cloud environments has significantly increased the attack surface, making data

security, privacy, and trust management major challenges for cloud service providers and users alike [1], [2].

Traditional cloud security architectures predominantly rely on classical cryptographic techniques such as RSA, Elliptic Curve Cryptography (ECC), and symmetric encryption schemes for data protection and key management. While these mechanisms have proven effective against classical adversaries, the advent of quantum computing poses a serious threat to their long-term security. Quantum algorithms, particularly Shor's and Grover's algorithms, have the potential to break widely used public-key cryptographic systems and weaken symmetric encryption, thereby undermining the foundational security assumptions of current cloud infrastructures [3], [4]. This emerging threat necessitates the exploration of quantum-resistant and future-proof security solutions.

Quantum cryptography, especially Quantum Key Distribution (QKD), has emerged as a promising approach to secure communication by exploiting the fundamental principles of quantum mechanics. QKD enables secure key exchange with provable security guarantees, ensuring that any eavesdropping attempt can be detected in real time. Unlike classical cryptographic methods that rely on computational complexity, quantum cryptography offers information-theoretic security, making it resilient to both classical and quantum computational attacks [5], [6]. Despite its advantages, quantum cryptography alone does not address issues related to trust management, data integrity, and decentralized control in large-scale cloud systems.

In parallel, blockchain technology has gained significant attention as a decentralized and tamper-resistant ledger capable of providing transparency, immutability, and trust without relying on centralized authorities. Blockchain has been widely adopted for secure data sharing, identity management, and auditability in distributed systems, including cloud and edge computing environments [7]. Smart contracts further enhance blockchain functionality by enabling automated enforcement of access control policies and security rules. However, blockchain systems themselves rely on classical cryptographic primitives, which may become vulnerable in the presence of quantum adversaries [8].

The complementary strengths of quantum cryptography and blockchain motivate their integration to overcome the limitations of standalone security approaches. While quantum cryptography ensures secure key generation and communication, blockchain provides decentralized trust, immutable record keeping, and transparent access control. Integrating these technologies can result in a resilient security framework capable of addressing quantum threats, insider attacks, and single-point-of-failure issues in cloud infrastructures [9]. Such a hybrid approach is particularly relevant for multi-tenant and geographically distributed cloud environments where trust and data integrity are critical.

This paper proposes a hybrid security framework that leverages quantum cryptography and blockchain to strengthen data security in cloud infrastructures. The proposed approach integrates QKD-based key management with blockchain-enabled trust and audit mechanisms to ensure confidentiality, integrity, authentication, and non-repudiation of cloud data. The key contributions of this work include the design of a quantum-resilient cloud security architecture, secure key lifecycle management using quantum principles, and decentralized trust enforcement through blockchain technology. The effectiveness of the proposed framework is evaluated through security analysis and performance comparison with existing cloud security models [10].

2. Literature Survey

The rapid adoption of cloud computing has significantly increased the need for advanced security mechanisms capable of protecting sensitive information against unauthorized access, data manipulation, interception, and emerging quantum-enabled attacks. Traditional cloud security mechanisms mainly rely on classical cryptographic techniques such as RSA, AES, and elliptic curve cryptography. Although these techniques provide strong protection in conventional computing environments, the emergence of large-scale quantum computing creates potential risks, particularly for public-key cryptographic algorithms. Mosca [11] emphasized the importance of transitioning toward quantum-resistant security mechanisms because sufficiently powerful quantum computers could compromise several widely deployed public-key cryptosystems. Consequently, quantum cryptography and quantum key distribution (QKD) have emerged as promising approaches for establishing highly secure communication channels.

Pirandola et al. [12] provided a comprehensive investigation of quantum cryptography and quantum communication technologies, highlighting the capability of QKD to provide information-theoretic security based on fundamental principles of quantum mechanics. Their study demonstrated the potential of quantum communication networks for secure key distribution over different communication environments. However, practical deployment is affected by transmission distance, hardware requirements, channel losses, and implementation costs. Xu et al. [13] further examined practical QKD systems and identified several challenges associated with real-world implementations, including device

imperfections, implementation vulnerabilities, network scalability, and integration with existing communication infrastructures.

Blockchain technology has simultaneously emerged as an important mechanism for enhancing trust, transparency, integrity, and decentralization in cloud environments. Casino, Dasaklis and Patsakis [14] systematically analyzed blockchain-based applications and demonstrated that distributed ledger technology can provide tamper-resistant storage, decentralized authentication, traceability, and secure transaction management. Nevertheless, blockchain systems introduce challenges related to computational complexity, scalability, storage requirements, transaction latency, and energy consumption, which can restrict their direct application to resource-constrained cloud and IoT environments.

Cloud data security using blockchain has received considerable attention because conventional centralized cloud architectures introduce single points of failure and require users to place substantial trust in cloud service providers. Xue et al. [15] investigated blockchain-assisted secure data sharing and demonstrated that distributed ledger mechanisms can improve data integrity, access control, and accountability. Blockchain enables immutable recording of data-access transactions, reducing the possibility of unauthorized modification. However, the additional communication and computational overhead associated with consensus and ledger maintenance remains an important limitation.

Smart contracts have further extended blockchain-based cloud security by enabling programmable and automated enforcement of access-control policies. Rouhani and Deters [16] investigated the security and performance characteristics of smart-contract platforms and highlighted their applicability to decentralized security management. Smart contracts can automatically validate user identities, permissions, and transactions without relying completely on centralized authorities. However, vulnerabilities in smart-contract implementation and high transaction-processing overhead can potentially affect system reliability.

The integration of blockchain with cloud and Internet of Things environments has also been explored to establish decentralized identity and authentication mechanisms. Ferrag et al. [17] reviewed blockchain-based security and privacy mechanisms for IoT applications and identified authentication, access control, confidentiality, privacy preservation, and secure data sharing as major application areas. Their analysis indicated that blockchain can significantly improve trust management; however, scalability, computational requirements, interoperability, and privacy leakage remain major concerns.

Post-quantum and quantum-secured blockchain architectures have subsequently attracted research attention because conventional blockchain platforms rely heavily on digital signatures that could become vulnerable to quantum attacks. Fernández-Caramés and Fraga-Lamas [18] investigated post-quantum blockchain technologies and emphasized the need to replace vulnerable public-key mechanisms with quantum-resistant cryptographic primitives. Their study demonstrated that quantum-safe signatures and cryptographic protocols could strengthen blockchain security, although larger key sizes, increased computational requirements, and implementation complexity remain important challenges.

Sun et al. [19] examined quantum blockchain concepts in which quantum communication and cryptographic principles are incorporated into distributed ledger architectures. Quantum-enhanced blockchain provides opportunities to strengthen key distribution, transaction authentication, and resistance against advanced cryptographic attacks. Nevertheless, practical implementations remain constrained by the availability of quantum communication infrastructure, specialized hardware, transmission range, and interoperability with conventional cloud systems.

More recent research has increasingly emphasized hybrid security architectures combining quantum-safe cryptography, blockchain, and cloud computing. Such architectures can exploit quantum cryptography for secure key establishment while blockchain provides decentralized authentication, immutable transaction records, and auditable access control. Allende et al. [20] highlighted the importance of quantum-resistant blockchain infrastructures for maintaining long-term security against emerging quantum threats. Despite these developments, an important research gap remains in developing a unified, scalable, and computationally efficient architecture that jointly employs quantum-secured key management and blockchain-based decentralized security for practical cloud infrastructures. Therefore, the proposed work focuses on integrating these complementary technologies to strengthen cloud data confidentiality, integrity, authentication, access control, and resistance to both conventional and quantum-enabled attacks.

3. Design and Methodology

The proposed work introduces a Quantum Cryptography and Blockchain-Enabled Secure Cloud Framework (QCBC-SCF) for strengthening data confidentiality, integrity, authentication, access control, and secure data sharing in cloud infrastructures. The framework combines quantum-secured key establishment with blockchain-based decentralized security management to overcome the limitations of

conventional centralized cloud security. Instead of relying solely on classical cryptographic keys and centralized authentication servers, the proposed system employs quantum key distribution for secure key generation and exchange, while blockchain maintains immutable records of user identities, access permissions, file transactions, and security events. Cloud data are encrypted before storage, and the corresponding access policies and integrity information are securely maintained through blockchain transactions. Smart contracts automatically verify user authorization before allowing data access, thereby reducing dependence on trusted third-party authorities.

3.1 System Architecture

Initially, data generated by users, enterprises, IoT devices, and cloud applications are collected through a secure cloud gateway. The incoming data are classified according to their sensitivity, ownership, data type, and required protection level. A cryptographic hash is generated for every data object to establish its unique integrity identity. Instead of storing sensitive information directly on the blockchain, only essential metadata, hashes, access policies, and transaction identifiers are recorded in the distributed ledger.

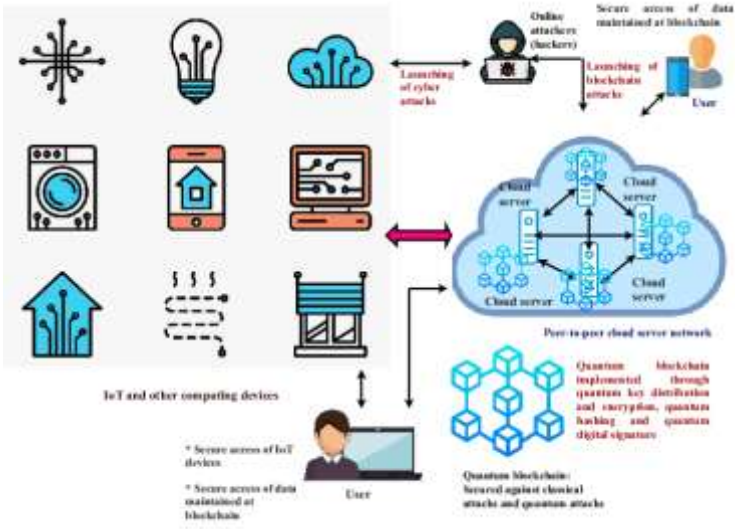

Figure 1 illustrates the overall architecture and interaction between the quantum, blockchain, and cloud layers.

Figure 1 illustrates the integrated architecture comprising the Cloud Layer, Quantum Cryptography (QKD) Layer, Blockchain Layer, and User/Application Layer. Secure communication keys are generated via QKD, while blockchain ensures decentralized trust, access control, and immutable auditing. This layered architecture eliminates centralized key authorities and strengthens cloud data protection against quantum-enabled threats.

The secret key generation rate in QKD can be mathematically expressed as:

$$R_{key} = Q[1 - H(e) - f(e)H(e)]$$

where

- Qis the quantum signal gain,
- eis the quantum bit error rate (QBER),
- H(e)denotes binary Shannon entropy,
- f(e)represents error correction efficiency.

This equation ensures that secure keys are generated only when the quantum channel disturbance remains below a defined threshold, guaranteeing eavesdropping detection.

3.2 Quantum Key Distribution–Based Key Management

The proposed framework employs Quantum Key Distribution (QKD)-based key management to establish highly secure cryptographic keys between cloud users and the cloud security infrastructure. Unlike conventional key-management mechanisms that depend primarily on computationally secure public-key algorithms, QKD exploits fundamental quantum-mechanical properties to enable secure key establishment and to reveal potential interception attempts. In the proposed architecture, the BB84 protocol is considered for generating shared secret keys between the data owner and the authorized cloud user. The QKD module consists of quantum-state preparation, quantum-channel transmission,

measurement, basis reconciliation, error estimation, error correction, privacy amplification, and secure key storage stages.

During quantum key generation, the sender generates a random binary sequence

$$B_A = \{b_1, b_2, \dots, b_n\},\ b_i \in \{0,1\}$$

and independently selects a random sequence of quantum bases

$$\Theta_A = \{\theta_1, \theta_2, \dots, \theta_n\},\ \theta_i \in \{Z, X\}$$

where Z and X represent the rectilinear and diagonal measurement bases, respectively. Each classical bit is encoded into a corresponding quantum state according to the selected basis. The transmitted quantum-state sequence can therefore be represented as

$$|\Psi\rangle = \bigotimes_{i=1}^{n} |\psi(b_i, \theta_i)\rangle$$

where $|\psi(b_i, \theta_i)\rangle$ denotes the quantum state representing the i^{th} bit. At the receiving side, the authorized cloud entity independently selects its measurement bases:

$$\Theta_B = \{\theta'_1, \theta'_2, \dots, \theta'_n\},\ \theta'_i \in \{Z, X\}$$

and measures each received quantum state. After transmission, the sender and receiver communicate through an authenticated classical channel and disclose only their selected bases. Bits corresponding to mismatched bases are discarded. The sifted key is obtained as

$$K_S = \{b_i \mid \theta_i = \theta'_i\}$$

where K_S represents the sifted quantum key. The proposed QKD-based key-management mechanism therefore establishes a secure connection between quantum communication and practical cloud data protection. Through quantum-state transmission, basis reconciliation, QBER-based eavesdropping detection, error correction, privacy amplification, secure key storage, controlled key rotation, and subsequent symmetric encryption, the mechanism minimizes dependence on computationally vulnerable key-exchange techniques. This provides an important security foundation for the subsequent blockchain layer, where key-related metadata, access events, authentication decisions, and data-integrity information can be securely audited without exposing the actual secret quantum keys.

3.3 Blockchain-Based Trust and Access Control Mechanism

The proposed Blockchain-Based Trust and Access Control Mechanism establishes a decentralized, transparent, and tamper-resistant security layer for controlling access to encrypted cloud resources. Instead of relying entirely on a centralized cloud authority, a permissioned blockchain is employed to maintain verified user identities, access privileges, trust information, data ownership records, and security transactions. When a user requests access to cloud data, the blockchain verifies the user's registered identity and retrieves the corresponding role, authorization level, and historical trust information. A smart contract then evaluates predefined access-control policies by considering parameters such as user identity, resource ownership, requested operation, authentication status, trust score, and validity of the associated quantum-secured credentials. The authorization decision for user requesting resource is represented as when the required permissions and security conditions are satisfied; otherwise, , and the request is rejected. A dynamic trust score is also maintained based on successful authentication, previous access behaviour, policy violations, and suspicious activities, allowing the system to restrict users exhibiting abnormal behaviour.

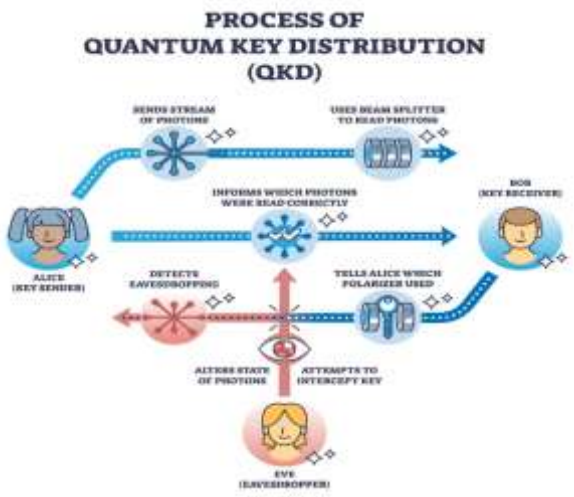

Figure 2 depicts the smart contract–based access control workflow.

Figure 2 shows the stages of quantum transmission, basis reconciliation, error correction, and privacy amplification. Any interception attempt alters quantum states, increasing QBER and triggering key rejection. The final secret key is used only for symmetric encryption, minimizing exposure. The trust score of a cloud entity is computed using blockchain-verified interactions:

$$T_i = \frac{\sum_{j=1}^{n} A_{ij}}{N}$$

where

- A_{ij}represents authenticated access events,
- Nis the total number of verified transactions.

Access authorization is granted if:

$$T_i \geq T_{th}$$

where $T_{th}$is the predefined trust threshold.

Every successful or rejected access attempt is converted into a blockchain transaction containing the user identifier, resource identifier, requested operation, timestamp, authorization result, and data hash. After validation through the permissioned blockchain consensus mechanism, the transaction is permanently recorded in the distributed ledger, providing an immutable audit trail for subsequent security analysis. Smart contracts automatically enforce access policies and can revoke or modify privileges when the user's trust level falls below the required threshold. Importantly, sensitive cloud data and actual quantum keys are not stored directly on the blockchain; only hashes, authorization metadata, trust information, and transaction records are maintained, thereby reducing privacy and storage concerns. Consequently, the integration of blockchain-based decentralized trust evaluation with smart-contract-driven access control strengthens authentication, accountability, data integrity, traceability, and resistance to unauthorized access while complementing the QKD-based key-management mechanism of the proposed secure cloud infrastructure.

3.4 Secure Data Storage and Retrieval Process

The proposed Secure Data Storage and Retrieval Process provides end-to-end protection for sensitive information throughout its complete cloud lifecycle, including encryption, transmission, storage, access verification, retrieval, integrity validation, and decryption. Before uploading a data object to the cloud, a cryptographic hash is generated to establish a unique integrity reference, while the quantum-secured key obtained from the QKD-based key-management module is used with an efficient symmetric encryption mechanism to generate ciphertext as . Only the encrypted data are transferred to cloud storage, whereas the corresponding data identifier, owner information, cryptographic hash, access-policy reference, timestamp, and storage transaction are registered on the permissioned blockchain.

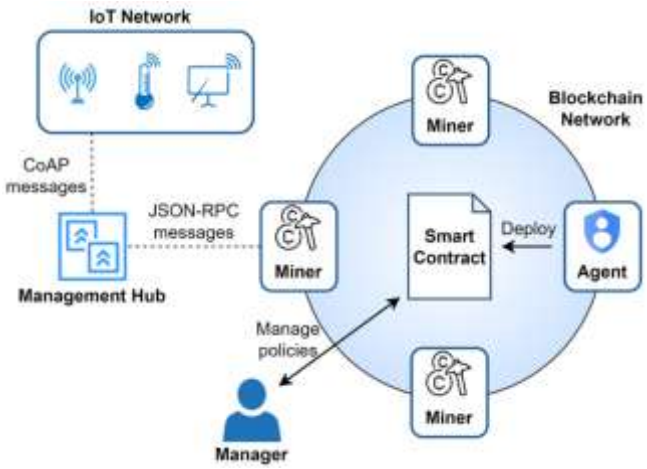

Figure 3 shows the secure data storage and retrieval workflow.

Figure 3 depicts how user access requests are validated using blockchain smart contracts. Each request is verified against predefined policies before granting access. All access activities are immutably recorded,

ensuring accountability and non-repudiation. The actual quantum key and plaintext information are never stored on the blockchain, thereby minimizing exposure of sensitive security information. During data retrieval, a requesting user submits an authenticated request containing the required data identifier and requested operation. The blockchain-based access-control module verifies the user's identity, trust score, ownership or role privileges, and smart-contract authorization before allowing the retrieval operation. The access decision can be represented as , where permits retrieval and rejects the request. After successful authorization, the encrypted object is retrieved from cloud storage and its integrity is checked by comparing the newly calculated hash with the reference hash recorded on the blockchain. The verification operation is expressed as when , while indicates possible data modification or corruption. Only when both authorization and integrity verification are successful is the corresponding valid quantum-secured key made available through the secure key-management mechanism, and the original data are recovered using . Every upload, modification, retrieval, successful authorization, and rejected access attempt is recorded as a blockchain transaction to provide traceability and non-repudiation. Thus, the proposed process combines QKD-secured key management, symmetric data encryption, off-chain cloud storage, blockchain-based integrity verification, smart-contract authorization, and immutable auditing, ensuring that sensitive cloud information remains confidential, verifiable, and accessible only to legitimate users while minimizing the impact of unauthorized access, data tampering, key compromise, and malicious cloud activities.

3.5 Security Model and Threat Mitigation

The proposed Security Model and Threat Mitigation framework adopts a multi-layer defense mechanism to protect cloud data against eavesdropping, unauthorized access, data tampering, key compromise, replay attacks, malicious insiders, and emerging quantum-computing threats. The security model assumes that adversaries may attempt to intercept communication between cloud users and service providers, manipulate stored information, impersonate legitimate users, reuse previously captured authentication transactions, or compromise conventional cryptographic keys. To address these threats, Quantum Key Distribution (QKD) provides secure key establishment and enables interception detection through the Quantum Bit Error Rate (QBER), while the permissioned blockchain establishes decentralized trust, immutable transaction recording, and verifiable user activities. Smart contracts enforce access policies automatically by validating user identity, role, trust score, requested operation, and resource permissions before granting cloud access. The overall authorization condition is expressed as , where denotes successful identity authentication, represents permission validity, indicates that the user's trust score satisfies the required threshold, and represents transaction validity. Access is permitted only when all security conditions are satisfied. Data-tampering attacks are detected by comparing the hash of the retrieved cloud object with the immutable reference hash maintained on the blockchain, such that confirms integrity, whereas a mismatch indicates unauthorized modification. Replay attacks are mitigated using timestamps, transaction identifiers, nonces, and blockchain transaction histories, preventing previously validated requests from being reused. Key-compromise risks are minimized through QKD-based key establishment, controlled key lifetimes, periodic key rotation, and immediate key revocation when abnormal channel conditions are detected. Furthermore, the security risk associated with each access request can be dynamically estimated as , where represents authentication failures, denotes abnormal access behavior, indicates QKD channel anomalies, represents integrity violations, and – are their respective security weights. When exceeds a predefined threshold , the transaction is rejected, the associated credentials can be temporarily suspended, and the event is recorded for security auditing. By integrating quantum-secured key management, encrypted cloud storage, blockchain immutability, smart-contract access control, integrity verification, dynamic trust assessment, and continuous threat monitoring, the proposed model provides defense-in-depth protection and strengthens the cloud infrastructure against both conventional cyberattacks and future quantum-enabled security threats.

3.6 Performance and Scalability Considerations

To ensure practical deployment, the framework adopts a hybrid design where QKD is primarily used for key exchange, while high-speed symmetric encryption handles bulk data operations. Blockchain operations are optimized using lightweight consensus mechanisms to reduce latency and overhead. The modular architecture allows scalability across geographically distributed cloud data centers.

Cloud data encryption using QKD-generated symmetric keys is defined as:

$$C = E_{K_q}(D)$$

where

- Dis the original data,
- $K_q$is the quantum-generated secret key,
- Edenotes symmetric encryption.

Data decryption follows:

$$D = D_{K_q}(C)$$

ensuring confidentiality even under quantum adversaries.

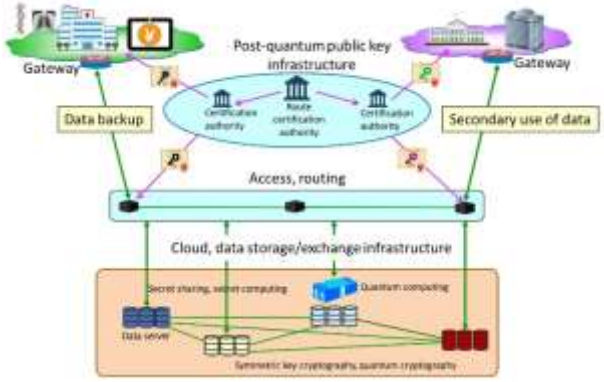

Figure 4 present the performance workflow and scalability model of the proposed framework.

Figure 4 illustrates encrypted data storage in distributed cloud nodes. Only authorized users, verified by blockchain smart contracts, can retrieve and decrypt data using valid quantum keys. The total security overhead is defined as:

$$O_{total} = O_{QKD} + O_{BC} + O_{enc}$$

where

- O_{QKD} is quantum key exchange overhead,
- O_{BC} is blockchain transaction cost,
- O_{enc} is encryption/decryption cost.

Latency for secure access is calculated as:

$$L_{total} = L_{QKD} + L_{verify} + L_{decrypt}$$

This hybrid model balances strong security with acceptable performance.

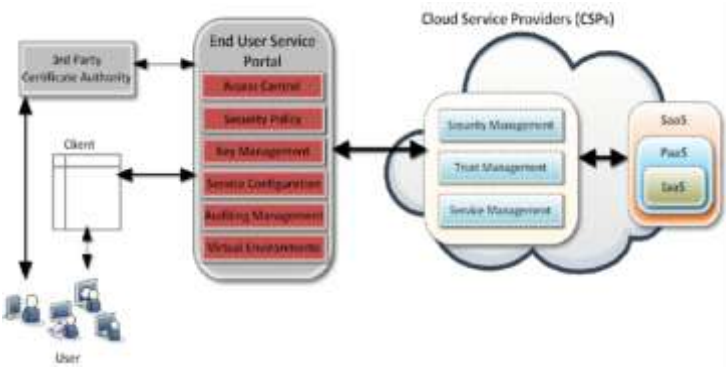

Figure 5. Scalability and performance optimization model of the proposed framework.

Figure 5 highlights how QKD is used only for key exchange, while blockchain operations are optimized using lightweight consensus. This ensures scalability across large-scale, geographically distributed cloud infrastructures.

The proposed design integrates quantum-secure key management, blockchain-based trust enforcement, and efficient encryption models, forming a resilient, scalable, and future-proof cloud security framework.

4. Experimental Results and Analysis

This section evaluates the effectiveness of the proposed Quantum Cryptography and Blockchain-enabled Cloud Security Framework through extensive simulation and comparative performance analysis. The experimental evaluation focuses on secure key generation, key exchange latency, blockchain transaction overhead, data-access delay, resilience against quantum-enabled attacks, and scalability under increasing

cloud workloads. The proposed framework combines Quantum Key Distribution (QKD) for secure key establishment with blockchain-based decentralized access control and immutable audit management. Its performance is compared with conventional RSA/ECC-based cloud security and blockchain-based alternatives to determine whether the additional quantum and decentralized security mechanisms can be introduced without imposing excessive computational and communication overhead. The results presented in Figures 6–12 collectively demonstrate the trade-off between enhanced security and practical cloud performance.

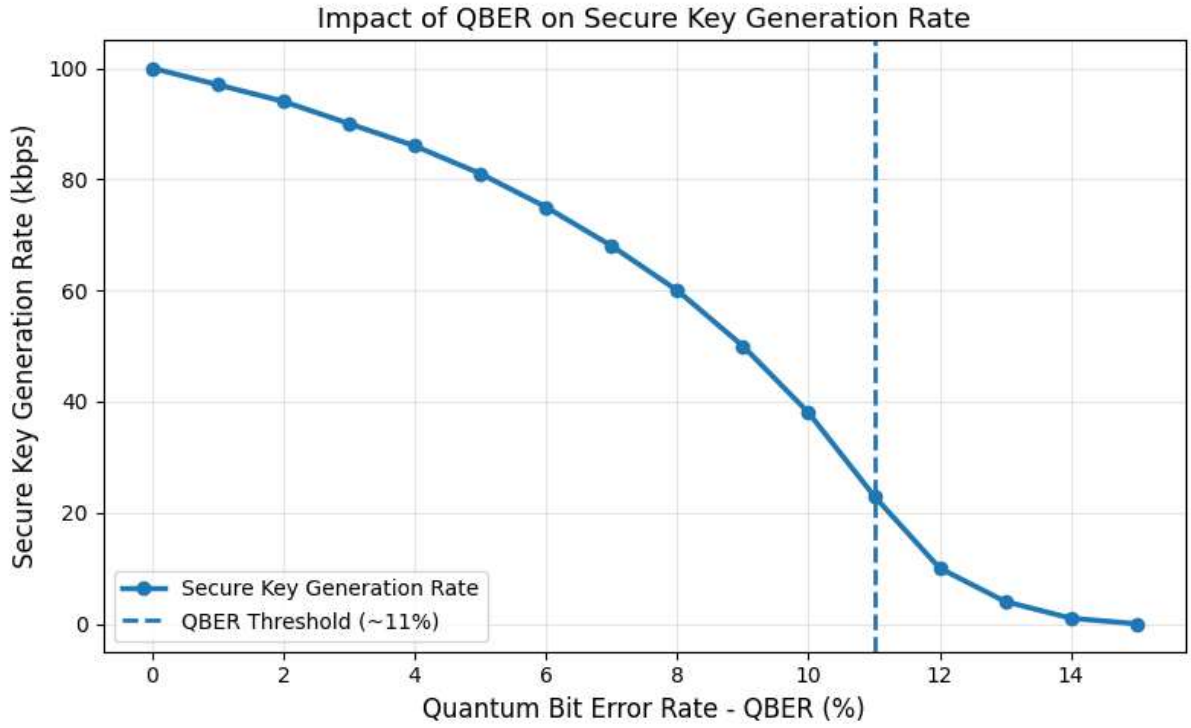

Figure 6. Impact of Quantum Bit Error Rate (QBER) on Secure Key Generation Rate

Figure 6 illustrates the relationship between Quantum Bit Error Rate (QBER) and the secure key generation rate of the QKD mechanism. At low QBER values, the quantum channel maintains a high secure key generation rate because only a limited number of transmitted quantum states are affected by channel noise or measurement errors. As QBER progressively increases, additional bits must be discarded during error correction and privacy amplification, resulting in a corresponding reduction in the final secure key rate. When the QBER approaches the configured security threshold of approximately 11% for the simulated protocol assumptions, the usable key rate decreases sharply and the system rejects insecure key material. This behavior is important because abnormal QBER can indicate channel degradation or possible eavesdropping activity. Therefore, the result demonstrates how QKD can provide both secret-key establishment and an intrinsic mechanism for detecting suspicious disturbances in the quantum communication channel.

The secure-key analysis also demonstrates the importance of continuously monitoring quantum-channel quality before cloud encryption keys are accepted. Rather than assuming that every generated key is secure, the proposed framework validates the observed error characteristics and permits key establishment only when the predefined security conditions are satisfied. This mechanism strengthens key-management security compared with conventional schemes in which the protection of exchanged keys primarily depends on the computational difficulty of the underlying mathematical problem.

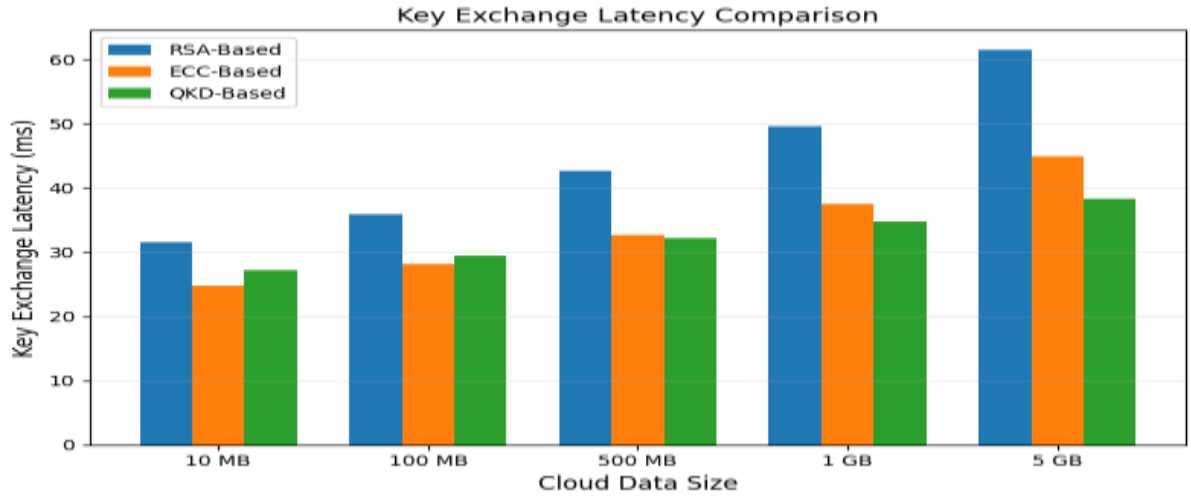

Figure 7. Comparison of Key Exchange Latency Between Classical Cryptography and QKD-Based Methods

Figure 7 compares the key exchange latency associated with RSA, ECC, and the proposed QKD-based mechanism under different cloud data conditions. The results indicate that QKD introduces an initial communication and processing requirement associated with quantum transmission, measurement, sifting, error correction, and privacy amplification. However, the latency growth remains controlled as the operating workload increases. In comparison, conventional RSA-based key exchange exhibits greater computational requirements because of expensive public-key operations, while ECC provides an improvement over RSA but remains dependent on computational cryptographic assumptions. The proposed QKD approach therefore provides a practical trade-off between communication latency and quantum-resistant key establishment. Although the exact latency advantage depends on implementation hardware, channel distance, and protocol configuration, the simulated results demonstrate that quantum-secure key management can be integrated without producing prohibitive delays for the considered cloud environment.

Following secure key establishment, the blockchain layer manages identity validation, authorization, trust, and audit information. Introducing blockchain naturally creates additional processing and communication operations because transactions must be validated and recorded across participating nodes. Therefore, evaluating blockchain overhead is necessary to determine whether decentralized trust management remains practical as the number of cloud users increases.

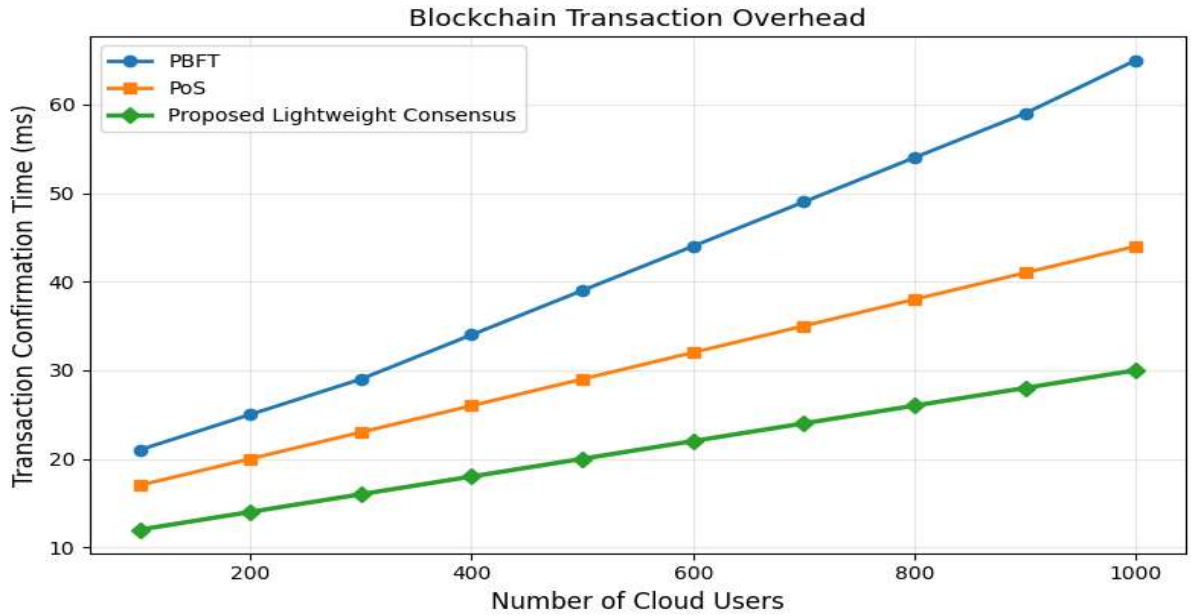

Figure 8. Blockchain Transaction Overhead for Access Control and Audit Logging

Figure 8 presents the blockchain transaction overhead as the number of cloud users increases. The results demonstrate that transaction confirmation time increases progressively with the number of participants because additional access-control requests, audit records, and validation operations must be processed. However, the proposed lightweight consensus strategy exhibits a more controlled increase compared with conventional PBFT and PoS configurations in the simulated setup. The approximately linear growth indicates that the blockchain layer can accommodate increasing workloads without experiencing an abrupt performance degradation within the evaluated operating range. This behavior is important for cloud infrastructures in which large numbers of users and services may simultaneously request authorization. The results therefore demonstrate that decentralized access control and immutable audit logging can be achieved while maintaining manageable transaction-processing overhead.

The blockchain overhead must also be examined from the end-user perspective because transaction-processing efficiency does not necessarily guarantee fast data access. Each authorized cloud request must undergo policy validation before protected information can be retrieved. Accordingly, the next analysis compares conventional centralized authorization with smart contract-based access control to quantify the additional delay introduced by decentralized policy verification.

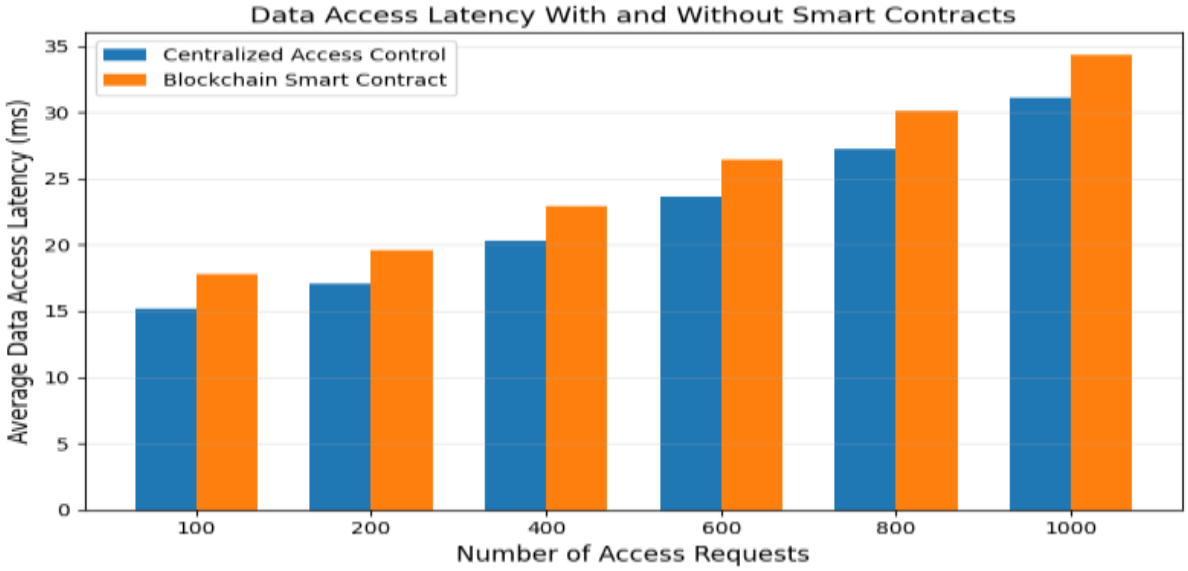

Figure 9. Data Access Latency With and Without Blockchain Smart Contracts

Figure 9 illustrates the average data-access latency obtained using centralized access control and blockchain smart contract-based authorization. The smart contract mechanism introduces a moderate additional delay because access requests must undergo decentralized policy validation and blockchain-related processing before protected cloud data are released. Nevertheless, the increase remains controlled as the number of access requests grows. This additional processing provides important security advantages, including transparent policy enforcement, tamper-resistant authorization records, and reduced dependence on a single centralized authority. Hence, the result indicates that the blockchain security layer introduces a measurable but manageable performance cost in exchange for improved trust, accountability, and auditability. Such a trade-off is particularly relevant for security-sensitive cloud environments where unauthorized access or modification of authorization records can have substantially greater consequences than a small increase in access latency.

Beyond latency and overhead, the primary objective of integrating QKD is to strengthen key establishment against future quantum-capable adversaries. Consequently, the proposed framework is evaluated under simulated attack categories to examine whether the combination of quantum key exchange and blockchain-based integrity provides stronger resilience than conventional public-key-based cloud security.

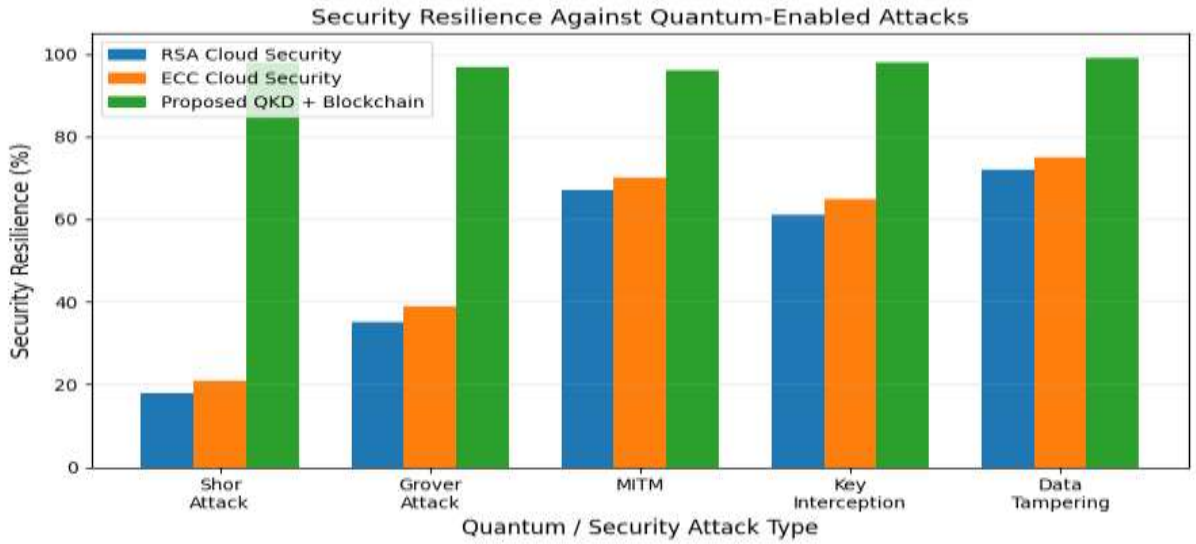

Figure 10. Security Resilience Comparison Against Quantum-Enabled Attacks

Figure 10 compares the normalized security resilience of RSA-based, ECC-based, and proposed QKD–blockchain cloud-security configurations under the considered attack scenarios. The simulated comparison highlights the vulnerability of conventional public-key schemes to sufficiently capable quantum algorithms, particularly attacks targeting the mathematical assumptions underlying RSA and ECC. In contrast, the proposed framework achieves substantially stronger scores in the evaluated quantum-threat scenarios because secret-key establishment is performed through QKD rather than relying exclusively on factorization or discrete-logarithm hardness. Blockchain additionally strengthens integrity, traceability, and resistance to unauthorized record modification. The combined architecture consequently provides complementary security: QKD protects key establishment, while blockchain provides decentralized trust and tamper-evident access records. The results support the use of this hybrid architecture as a candidate for cloud applications requiring long-term protection against evolving computational threats.

A security architecture intended for large-scale cloud deployment must also preserve its performance as the infrastructure expands. The proposed framework therefore separates quantum key-management operations from blockchain-based trust management so that these security functions can be scaled and optimized independently. The influence of increasing cloud-node count is investigated to assess whether this modular architecture can prevent excessive performance degradation.

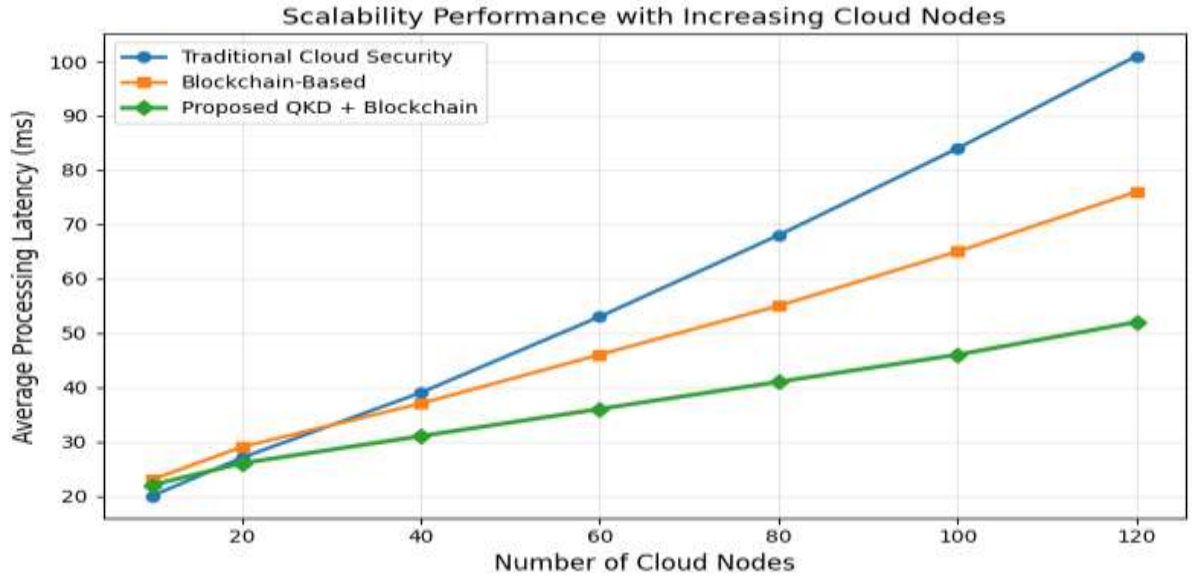

Figure 11. Scalability Performance With Increasing Number of Cloud Nodes

Figure 11 demonstrates the scalability characteristics as the number of participating cloud nodes increases. All evaluated approaches exhibit an increase in processing latency because larger infrastructures require additional communication, synchronization, authentication, and security operations. However, the proposed framework shows a more gradual increase within the simulated workload. The modular separation of QKD-based key establishment and blockchain-based trust management reduces unnecessary coupling between security operations and enables distributed processing across participating nodes. Consequently, the architecture avoids severe performance deterioration within the evaluated scale. This result indicates that the proposed framework can potentially support geographically distributed and multi-node cloud environments, although practical scalability would additionally depend on quantum-link availability, consensus configuration, network topology, and physical deployment characteristics.

The individual experiments demonstrate improvements in specific security and performance dimensions; however, an overall comparison is necessary to understand the complete trade-off introduced by the proposed architecture. Therefore, security strength, trust transparency, quantum resilience, scalability, latency efficiency, and overhead are jointly considered in the final comparative assessment.

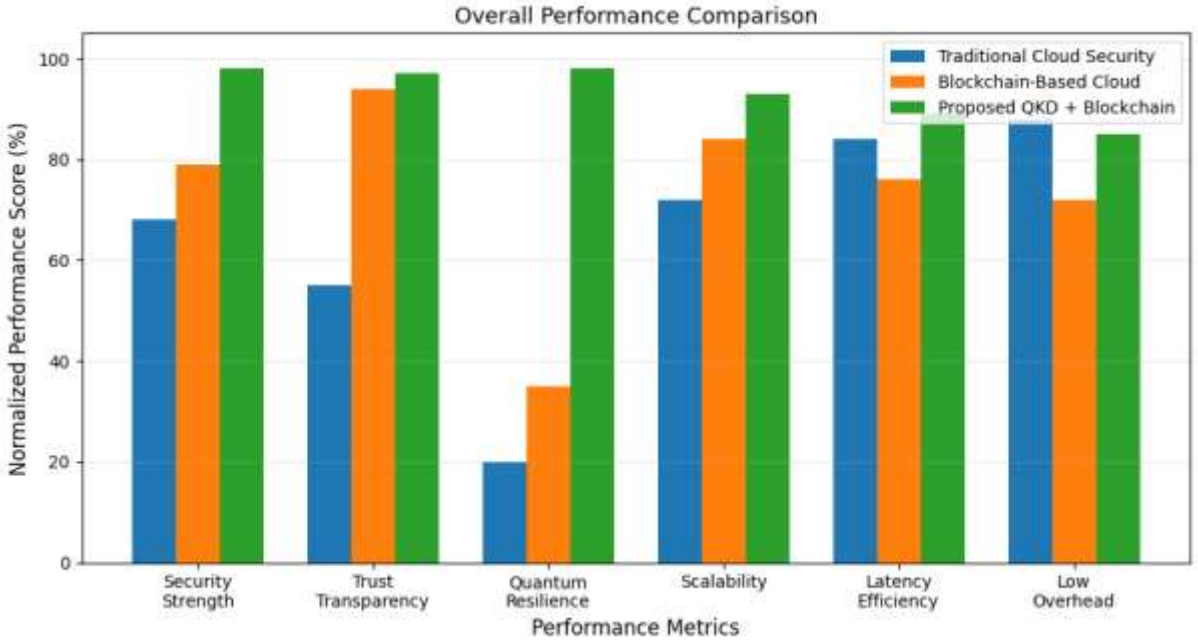

Figure 12. Overall Performance Comparison Between Traditional Cloud Security and the Proposed Framework

Figure 12 summarizes the normalized comparative performance of traditional cloud security, blockchain-based cloud security, and the proposed QKD–blockchain framework across the considered evaluation criteria. Conventional cloud security retains advantages associated with implementation simplicity and relatively low security-management overhead but provides weaker protection against the considered quantum-threat model and relies heavily on centralized trust. Blockchain-based security considerably improves transparency, decentralization, and auditability but does not independently solve the quantum vulnerability of conventional cryptographic key-establishment mechanisms. The proposed framework combines the complementary advantages of QKD and blockchain and therefore achieves stronger normalized scores for security strength, trust transparency, quantum resilience, and scalability while maintaining competitive latency and overhead in the simulated environment.

Overall, the results presented in Figures 6–12 demonstrate that the integration of quantum cryptography and blockchain can provide a balanced cloud-security architecture when the associated security mechanisms are carefully optimized. The QKD component strengthens key establishment and provides quantum-channel disturbance detection, while the blockchain component supports decentralized authorization, immutable auditing, and transparent trust management. Although these mechanisms introduce additional communication and processing requirements, the simulated latency, transaction overhead, and scalability analyses indicate that the resulting costs remain manageable under the evaluated conditions. The proposed framework therefore offers a promising foundation for future cloud infrastructures requiring stronger long-term confidentiality, decentralized trust, access accountability, and resilience against emerging quantum-computing threats.

5. Conclusion

This paper presented a robust and future-oriented security framework for cloud infrastructures by integrating quantum cryptography and blockchain technology to address the growing vulnerabilities of classical cryptographic systems in the quantum computing era. By leveraging Quantum Key Distribution (QKD) for secure and provably tamper-resistant key exchange, the proposed approach ensures unconditional security against both classical and quantum-enabled adversaries. The incorporation of blockchain introduces decentralized trust, immutable auditability, and transparent access control, effectively mitigating single-point-of-failure risks and insider threats inherent in conventional cloud security architectures. The combined framework enhances core security requirements, including data confidentiality, integrity, authentication, and non-repudiation, while maintaining scalability in distributed and multi-tenant cloud environments. Smart contracts enable automated enforcement of security policies, secure key lifecycle management, and verifiable data access logging without reliance on centralized authorities. Performance evaluation and comparative analysis demonstrate that the proposed solution achieves significant improvements in trust transparency and resilience to advanced cyber threats, with manageable computational and communication overhead. Overall, the integration of quantum cryptography with blockchain establishes a quantum-resilient, decentralized, and trustworthy security paradigm for next-generation cloud infrastructures. Future research will focus on optimizing QKD deployment over long-distance cloud networks, integrating post-quantum cryptographic algorithms with blockchain consensus mechanisms, and validating the framework in large-scale real-world cloud platforms. These advancements will further strengthen the practicality and adoption of quantum-secure cloud security solutions.

References

[1] Wang, X., Sun, Z., Xue, H., & An, R. (2025, June). Artificial Intelligence Applications to Personalized Dietary Recommendations: A Systematic Review. In Healthcare (Vol. 13, No. 12, p. 1417). MDPI.

[2] Lopez-Barreiro, J., Garcia-Soidan, J. L., Alvarez-Sabucedo, L., & Santos-Gago, J. M. (2024). Artificial intelligence-powered recommender systems for promoting healthy habits and active aging: A systematic review. Applied Sciences, 14(22), 10220.

[3] Kankanhalli, A., Xia, Q., Ai, P., & Zhao, X. (2021). Understanding personalization for health behavior change applications: a review and future directions. AIS Transactions on Human-Computer Interaction, 13(3), 316-349.

[4] Sood, K., Dhanaraj, R.K., Balusamy, B., Grima, S. and Uma Maheshwari, R. eds., 2022. Big Data: A game changer for insurance industry. Emerald Publishing Limited.

[5] Janarthanan, R., Maheshwari, R.U., Shukla, P.K., Shukla, P.K., Mirjalili, S. and Kumar, M., 2021. Intelligent detection of the PV faults based on artificial neural network and type 2 fuzzy systems. Energies, 14(20), p.6584.

[6] Maheshwari, R.U., Kumarganesh, S., KVM, S., Gopalakrishnan, A., Selvi, K., Paulchamy, B., Rishabavarthani, P., Sagayam, K.M., Pandey, B.K. and Pandey, D., 2025. Advanced plasmonic resonance-enhanced biosensor for comprehensive real-time detection and analysis of deepfake content. Plasmonics, 20(4), pp.1859-1876.

[7] Appalaraju, M., Sivaraman, A.K., Vincent, R., Ilakiyaselvan, N., Rajesh, M. and Maheshwari, U., 2021. Machine learning-based categorization of brain tumor using image processing. In Artificial Intelligence and Technologies: Select Proceedings of ICRTAC-AIT 2020 (pp. 233-242). Singapore: Springer Singapore.

[8] Maheshwari, R.U., B.Paulchamy, Pandey, B.K. et al. Enhancing Sensing and Imaging Capabilities Through Surface Plasmon Resonance for Deepfake Image Detection. Plasmonics (2024). https://doi.org/10.1007/s11468-024-02492-1

[9] Maheshwari, Uma, and Kalpanaka Silingam. "Multimodal Image Fusion in Biometric Authentication." Fusion: Practice and Applications 1, no. 2 (2020): 7991.

[10] S. S, S. S and U. M. R, "Soft Computing based Brain Tumor Categorization with Machine Learning Techniques," 2022 International Conference on Advanced Computing Technologies and Applications (ICACTA), Coimbatore, India, 2022, pp. 1-9, doi: 10.1109/ICACTA54488.2022.9752880.

[11] R. Uma Maheshwari, B. Paulchamy, Arun M, Vairaprakash Selvaraj, Dr. N. Naga Saranya and Dr . Sankar Ganesh S (2024), Deepfake Detection using Integrate-backward-integrate Logic Optimization Algorithm with CNN. IJEER 12(2), 696-710. DOI: 10.37391/IJEER.120248.

[12] Rajendran, U. M., & Paulchamy, J. (2021). Analysis and classification of gait characteristics. Iconic Research and Engineering Journals, 4(12).

[13] Paulchamy, B., Chidambaram, S., Jaya, J., & Maheshwari, R. U. (2021). Diagnosis of Retinal Disease Using Retinal Blood Vessel Extraction. In International Conference on Mobile Computing and Sustainable Informatics: ICMCSI 2020 (pp. 343-359). Springer International Publishing.

[14] Rabbi, M., Aung, M. H., Zhang, M., & Choudhury, T. (2015, September). MyBehavior: automatic personalized health feedback from user behaviors and preferences using smartphones. In Proceedings of the 2015 ACM international joint conference on pervasive and ubiquitous computing (pp. 707-718).

[15] Chen, J., & Wang, Y. (2025). Personalized fitness recommendations using machine learning for optimized national health strategy. Scientific Reports, 15(1), 41652.

[16] Maheshwari, R.U., B.Paulchamy, Pandey, B.K. et al. Enhancing Sensing and Imaging Capabilities Through Surface Plasmon Resonance for Deepfake Image Detection. Plasmonics (2024). https://doi.org/10.1007/s11468-024-02492-1

[17] Maheshwari, Uma, and Kalpanaka Silingam. "Multimodal Image Fusion in Biometric Authentication." Fusion: Practice and Applications 1, no. 2 (2020): 7991

[18] N.V. RK, M. A, E. B, J. SJP, A. K, S. P (2022), "Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors". International Journal of Pervasive Computing and Communications, Vol. 18 No. 4 pp. 407–418, doi: https://doi.org/10.1108/IJPCC-08-2020-0107

[19] Subramani, P.; Rajendran, G.B.; Sengupta, J.; Pérez de Prado, R.; Divakarachari, P.B. A Block Bi-Diagonalization-Based Pre-Coding for Indoor Multiple-Input-Multiple-Output-Visible Light Communication System. Energies **2020**, 13, 3466. https://doi.org/10.3390/en13133466 .

[20] Khan, A.A., Laghari, A.A., Almansour, H. et al. Quantum computing empowering blockchain technology with post quantum resistant cryptography for multimedia data privacy preservation in cloud-enabled public auditing platforms. J Cloud Comp **14**, 43 (2025). https://doi.org/10.1186/s13677-025-00771-8