I.J. Information Engineering and Electronic Business, **2025, 6, 99-111**
Published Online on December 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2025.06.08

Hybrid Security Models for Cloud Systems: Blockchain and Quantum Cryptographic Integration

Neethu V. A.
Department of Computer Science & Engineering, Madhav University, Abu Road, Rajasthan, India
E-mail: arunchandranneethu@gmail.com
ORCID ID: https://orcid.org/0000-0002-9462-3182

Arun Vaishnav*
Faculty of Computing and Informatics, Sir Padampat Singhania University, Udaipur, India
E-mail: a.vaishnav2155@gmail.com
ORCID ID: https://orcid.org/0000-0003-3352-1382

Mohammad Akram Khan
Department of Computer Science & Application, Madhav University, Abu Road, Rajasthan, India
E-mail: staryan23@gmail.com
ORCID ID: https://orcid.org/0009-0009-7372-8987

Received: 15 December, 2024; Revised: 22 March, 2025; Accepted: 25 June, 2025; Published: 08 December, 2025

Abstract: The introduction of cloud technology changes the face of data management by eliminating tedious concerns with regards to proper storage and accessibility as it can done from any location, therefore, it can be said that the emergence of this technology came with a number of challenges related to data confidentiality, integrity, and authentication as well. As a resolution to certain weaknesses presented in this case, the authors in this paper suggest a hybrid security model which integrates both quantum cryptography and blockchain technology, and improves security flaws on cloud and quantum models. There are three characteristics of data that are crucial to its safety and security; confidentiality, integrity, and availability, and cloud technology has been known to be accompanied with plenty of challenges concerning these aspects, however, with the use of Blockchain technology, data becomes immutable, decentralized, and transparent thereby reducing the risk of unauthorized access. The combination of strategies proposed in this paper, helps to eliminate a number of drawbacks like key loss, data loss, and man in the middle attacks that are common in cloud infrastructure. This study shows the structural design, data transmission and processes of the architecture for the hybrid model, looking forward to achieve better data security. The analysis of the model suggests its advantages over conventional encryption model and a purely constructed model of blockchain. Performance benchmarks are also included, demonstrating that the model is resilient to cyber threats during the quantum age. The architecture is seamless with the current cloud stature, takes cloud security a notch higher by solving the considerable challenges and is poised to be deployed on a larger scale The directional works will include improving the system's computational efficiency and extending the model to multiple cloud infrastructures to achieve higher security in today's complex cloud systems.

Index Terms: Blockchain Technology, Quantum Cryptography, Hybrid Security Model, Cloud Security, Quantum Key Distribution (QKD), Data Integrity and Scalability, Post-Quantum Cryptography, Post-Quantum Quasi-Monoalphabetic cryptography (PQQM)

1. Introduction

Cloud Computing has been the mainstay of modern Internet architecture that showcases data storage, processing, and data retrieval capabilities. On the other hand, the increasing prevalence of cloud systems has come with serious security issues such as data leakage, excessive system access, and cracking of keys. As quantum computers improve, existing mechanisms of encryption are becoming less reliable, which highlights the need to implement strong protocols

that would protect valuable data stored in the cloud. To mitigate these challenges, this paper offers a hybrid security paradigm which integrates blockchain technology with quantum encryption. The use of Blockchain facilitates a distributed ledger system that is tamper-proof and assures validation and verification of records, additionally QKD makes use of the principles of quantum mechanics and guarantees secure key management and transfer. Such an approach helps develop methods to protect computers from threats occurring in the classical era as well as during the quantum era, thereby ensuring that those methods are suitable for several circumstances and requirements set in the future. [1] in this regard point out how quantum computing changes the infrastructure and its need for appropriate security in the quantum age. [2] also consider security problems and security solution for cloud computing applications by recommending a distributed blockchain SDN architecture for IoT networks. The evolving threat landscape, coupled with the disruptive advent of quantum computing, requires strong and future-proof security architectures. Traditional encryption models can no longer provide strong assurances of cloud data integrity and user trust. The proposed hybrid model provides a defensive model and answers to the anticipated concerns while maintaining cloud computing principles of confidentiality, integrity, and availability even when faced with both classical and quantum adversaries.

Blockchain nodes and quantum key distribution nodes are aligned withinside the model`s multi-layered protection structure to offer a unified, impenetrable environment. This takes a look at simulates each traditional and quantum risk scenarios, makes use of benchmark datasets to check the advised structure, and measures overall performance metrics consisting of assault resistance, power efficiency, latency, and key protection. The closing goal is to create an intensive and bendy cloud protection structure which can shield data and sports in a destiny this is turning into extra unpredictable and technologically sophisticated. The hybrid model is proposed to improve the recovery of the cloud system by taking advantage of the forces of blockchain and quantum code. It is related to the main security goals - security, integrity and usability - while ensuring expansion capacity, incident tolerance and effective locking. In addition, it promotes the ability to interact in multi -slop environment and support essential monitoring and verification mechanisms for high insurance systems.

2. Literature Survey

Even with the evolution of cloud systems, the protective measures that have been put in place are not comprehensive enough to prevent the data from the threats posed by sophisticated cyber-attacks, particularly now that quantum computers are on the rise, frightening the principles of encryption long held. [3] The entanglement and overlapping are two concepts that allow IT quantum to perform much more complicated calculations than computers made by regular computers. This study emphasized the multidisciplinary nature of the region by highlighting important ideas, especially the calculation of Qubit, parallel to quantum and backward computer science. Quantum computers can regenerate any physical system, which can lead to progress in artificial intelligence and sophisticated approach to solve the problem.[4] discuss challenges and benefits of blockchain for cloud computing in depth. [5] propose a solution for problems of data sharing in public clouds while ensuring security and data integrity through the use of blockchain technology. [6] dual features of quantum computerization and blockchain technology have been analysed .While quantum computing plunges its fangs into the established blockchain systems with a rabid thirst for security risks, on the flip side are new prospects to upgrade computational power and design frameworks that are resistant to quantum errors. [7] examine the scope of concern and opportunity at the intersection of blockchain and quantum computation. consider post quantum security measures and in the context of this PQQM federation performance block chained federated learning. The research conducted within the last couple of years has focused greatly on the combination of blockchain and quantum cryptography with hybrid security models of cloud systems.[8] cover the chronological spatiotemporal gapping of security services associated with blockchains and hint at new and old developments afterward. [9] explain computational aspects of quantum encryption security, which is critical in devising secure quantum cryptographic systems. [10] have accomplished the task of explaining applications of quantum blockchain in the medical sector with examples.

New changes enhance even more the importance of this connection. For example, [11] implements post quantum cryptographic security along with blockchain technology in a IoT cloud computing system that was built to be reliable. In addition, [12] designed a cloud computing application where Multi Party Data Outsourcing was introduced and Quantum Key Distribution was used to prevent international attacks. [13] Quantum computers threaten common cryptographic algorithms like RSA and ECC by effectively breaking them by using quantum algorithms like short. To combat this, researchers are developing code after health and distributing quantum locks such as safe alternative options. [14] securing blockchain systems with quantum immunity has convincing benefits for the longer run, as the running costs can be justified by the ensure of safety and robustness of cloud services leveraging blockchain in the forthcoming future. By employing cloud computing and blockchain technology in IoT, the authors in [15] introduced SH-Block CC, a successful, enhanced and secure smart home architecture. [16] Presents a systematic review of blockchain-based communication systems for UAVs. Using Blockchain technology in the industry, they demonstrate increased safety with UAS communications through possible solutions for some conflicts in the field.

[17] the authors discussed edge-assisted vehicular networks security issues and how edge computing can improve vehicular communication systems for both security and performance concerns. Their research highlights key security issues and finds new ways to ensure data integrity and confidentiality in these networks. [18] investigated the

convergence between blockchain and edge computing to improve the security, scalability, and reliability of operators and services for IoT critical infrastructures in Industry 4.0. [19] presented detailed review on blockchain security and involved techniques and challenges to maintain blockchain secure. The paper also signifies potential future work in blockchain security, indicating what aspects require more research and development. [20] This paper provides a systematic taxonomy and review on blockchain-based trust management in cloud computing system, discussing the major techniques and their challenges. It also discusses the future possibilities of blockchain technology being integrated with cloud infrastructures to enhance reliability, security and transparency of such companions. This paper provides a systematic taxonomy and review on blockchain-based trust management in cloud computing system, discussing the major techniques and their challenges. It also discusses the future possibilities of blockchain technology being integrated with cloud infrastructures to enhance reliability, security and transparency of such companions.[21] explain quantum computing quite thoroughly, outlining its core ideas (superposition, entanglement) and what these ideas mean for speed and complexity of computation. They also present state-of-the-art, challenges for quantum hardware and the future impact on cryptography, optimization and machine learning.[22] introduce a quantum walk based algorithm on determining subgame perfect equilibrium in finite two-player sequential games. They show that quantum algorithms can in some cases offer a computational advantage for game theory, with a better equilibrium computation efficiency than classic approaches.[23] Quantum Computing as a Service (QCaaS) and explore to what extent, if at all it is theoretically possible, or even practically feasible. Conversing the basic design, possible advantages, and open challenges, they argue that despite its great potential, QCaaS requires further technological maturity for being widely available and useful.[24] apply quantum computing and optimization strategies in their quantum based cuckoo search algorithm. Their performance outperforms Man-and-Machine based on classical solvers and FQT on both solution quality and convergence rate, indicating the prospective applications of hybrid quantum-classical approaches in combinatorial optimization.[25] quantum mechanics inspired analysis, by simulating the model and simulating some simple quantum systems. [26] areas like sequence alignment, protein folding, and systems biology, where quantum computer can potentially provide revolutionary computational improvements over the classical one. [27] Introduces key concepts such as quantum error correction codes and threshold theorems, which are essential for building scalable and stable quantum computing systems.[28] emphasizes both the opportunities and current challenges in adopting quantum technologies for complex healthcare problems, suggesting a promising future with continued research and development. [29] how quantum computing can outperform classical approaches in specific problem domains such as optimization, cryptography, and complex simulations, while also discussing the current barriers to widespread quantum adoption.[30] present enhanced security proofs for the SIGMA and TLS 1.3 key exchange protocols, offering tighter bounds and more precise cryptographic guarantees. Their work strengthens the theoretical foundations of these widely used protocols, ensuring improved confidence in their security against advanced adversarial models.

The above works in concert show the transformation of hybrid models of security with regard to the growing integration of blockchain and quantum safe cryptography to newly discovered security challenges in cloud systems.

3. Problem Statement and Proposed Hybrid Approach

The decentralized, immutable nature of blockchain combined with secure key exchange capabilities provided by quantum cryptography can offer a new way to develop security protocols that are resilient to classical and quantum threats.

3.1 Significance of the Study

The Union of both Blockchain and Quantum Cryptography presents a new strategy for Cloud protection overcoming the vulnerabilities that currently exist, and also providing a strong mechanism that is likely to withstand the quantum era cyber-attacks. This study improves the resilience of the system while also providing the basis for the robust cloud environment multi-cloud infrastructure. The combination of blockchain and quantum cryptography is strategically motivated by their complementary strengths. Blockchain offers tamper-resistance and decentralized record-keeping, while QKD ensures unbreakable key exchanges. Together, they form a robust, future-proof defenses for cloud infrastructures.

3.2 Objectives

- To determine and examine the weaknesses of contemporary cloud security models regarding quantum assaults.
- Construct a mixed secure architecture amalgamating blockchain and quantum cryptography.
- Foster secure data transport and storage through QKD.
- Determine the performance and the scalability of the hybrid model.
- Research and analyse the performances of the classical and quantum cyber assailants with respect to the model.
- Investigate and analyse the practicality of applying the hybrid model within the range of real cloud environments.
- Explore optimization and future research opportunities.

3.3 Overview of the Hybrid Model

The hybrid approach of blockchain and quantum cryptography is fundamentally process-driven because these technologies each afford distributed approaches for secure cloud systems. Blockchain can maintain decentralized and tamper-proof record-keeping, which underpins accountability in the event of an information breach; but even though the integrity of blockchain is preserved, it still relies on traditional cryptography, which is mainly vulnerable to attacks from quantum computers. Conversely, quantum cryptography through QKD offers theoretically unbreakable key exchanges, but lacks the characteristics of distributed data management and public verification supported by blockchain. The hybrid approach integrates both technologies so that blockchain can maintain decentralized, auditable status while quantum technologies support the encryption and management of keys. Together they offer a comprehensive framework that mitigates contemporary and emerging threats by ensuring the hybrid system is resilient to sophisticated quantum-enabled attacks but also incorporates traditional cyber threats.

4. Dataset

This research utilizes Hybrid Security Evaluation Dataset (HSED) to assess hybrid models that integrate blockchain and quantum cryptography into the cloud systems. The dataset covers Blockchain transaction, quantum cryptography datasets (key exchange logs, error rates and bit rates), cloud system logs (user IDs, control events, traffic amount), and artificially generated attack data (man-in-the-middle and quantum attacks). Fig. 1. outlines the hierarchical structure of the set. These components assist in evaluating the security feature's resistance to a range of attacks. It also employs ISOT Cloud IDS (ISOT CID) dataset, which is a real-world cloud dataset with traffic, system logs and performance data to analyse the hybrid model's effectiveness for cloud intrusion detection. The dataset includes components that allow the mechanisms to be tested on a wide scope. The ISOT Cloud IDS dataset went through some preprocessing (normalization, time alignment for simulating blockchain, removing redundant records, and creating synthetic examples of quantum attacks). This will ensure robust security assessment and reproducibility.

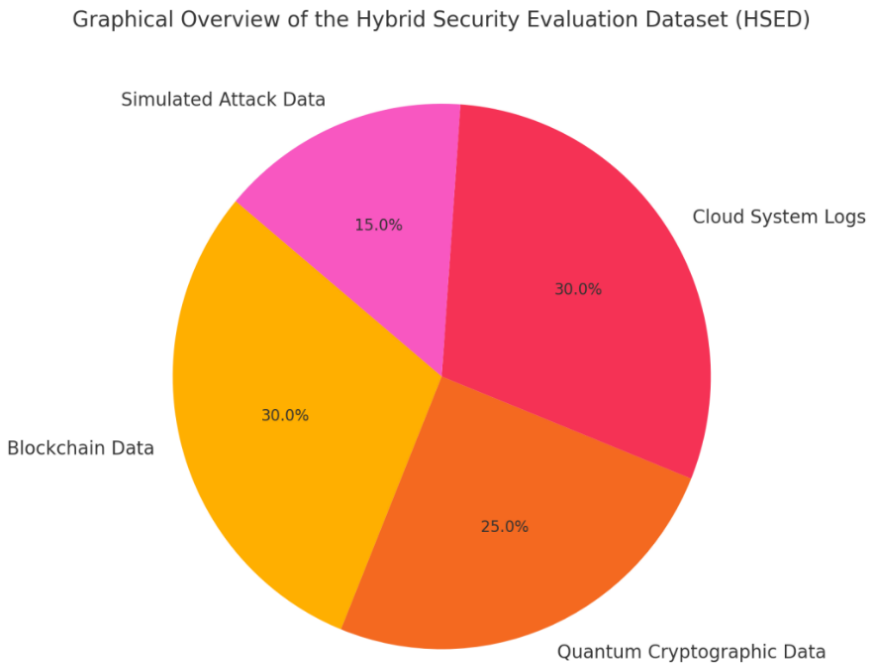

Fig. 1. The distribution of data components in the Hybrid Security Evaluation Dataset

Table 1. Dataset Component

Dataset Component	Details
Blockchain Data (30%)	Transaction IDs, Timestamps, Hash Values
Quantum Cryptographic Data (25%)	Key Exchange Logs, Error Rates, Bit Rates
Cloud System Logs (30%)	User IDs, Access Control Events, Data Integrity Checks, Traffic Volume
Simulated Attack Data (15%)	Man-in-the-Middle Scenarios, Quantum Attack Simulations

This table summarizes the key components of the HSED. Prior to assessing model performance, the ISOT Cloud IDS dataset was preprocessed by normalizing the network traffic features, removing duplicates, adjusting timestamps to simulate blockchain transactions, and generating synthetic data to emulate quantum-specific attacks. The dataset was then divided into 70% training and 30% testing data and used to test the hybrid model's resilience. Multiple attack simulations were included throughout the dataset that included both classical and quantum attack vectors, thus allowing

a complete assessment of the performance of the hybrid model. The completed preprocessing will allow for the experiments to be replicated increasing the validity of the security analysis.

The datasets not only encompass a very broad swath of normal operations in the cloud, but also model real-world cyber threats directly geared towards quantum-enabled attackers. The hybrid evaluation was implemented using attack models developed to capture quantum capabilities to ensure that the hybrid model keeps the proposed evaluation resilient to developing threat spaces.

5. Proposed Methodology

The suggested hybrid security framework integrates the use of quantum cryptography with blockchain technology to cater for the shifting security requirements of cloud systems in todays and tomorrow's computing scenario. Due to the decentralized and unchangeable form of its record, Blockchain provides guaranteed data integrity and ability to audit transactions. Its rate of transactions per second is stated as:

$$\mathrm{TPS} = \frac{\mathrm{T_t} \cdot \mathrm{N_n}}{\mathrm{T_b}} \tag{1}$$

Where T_t is the number of transactions per block, N_n is the number of nodes involved in the consensus process, and T_b is the block timeIn order to bolster the level of security, QKD protocol is now included for key exchanges. The key generation rate is determined as:

$$\mathrm{R_k} = \mathrm{P_s} \cdot \eta \cdot (1 - \mathrm{QBER}) \tag{2}$$

Where P_s is the photon generation rate, η represents system efficiency, and $QBER$ is the Quantum Bit Error Rate. Data encryption is performed using AES-256, with the ciphertext expressed as:

$$\mathrm{C} = \mathrm{E}(\mathrm{K}, \mathrm{P}) \tag{3}$$

Where K is the QKD-generated key and P is the plaintext. The model's layered architecture synchronizes blockchain nodes with QKD systems as shown in Fig .2, ensuring seamless integration for secure data storage and communication. Performance evaluations simulate potential threats to measure metrics such as data integrity, scalability, latency, and energy consumption, demonstrating the hybrid model's robust and efficient approach to modern cloud security challenges.

5.1 Challenges and Limitations of QKD in Cloud Environments

While QKD has strong theoretical foundations, practical deployment across large cloud systems will have various challenges. First, QKD systems rely on dedicated quantum channels, which can be fibre-optic or free-space, that may have issues with scalability across large cloud systems. Second, QKD's key generation will generally be less than traditional cryptographic key exchanges, as factors such as distance, attributable to distance in the network can increase latency and bandwidth issues. Third, the barrier to deployment can be the need for specialist quantum hardware (for example, single-photon detectors) that can be expensive. Therefore, despite QKD's capabilities, the practical issues that have been identified above address key generation may can bottlenecks in key generation, raise issue of the infrastructure that may be more expensive than traditional forms of cloud key management when deploying in multi-cloud environments that are geographically spread across multiple locations. Future developments for this hybrid model will focus on exploring post-quantum cryptographic solutions and hybrid modes for key management, addressing some of these obstacles.

5.2 Computational Complexity Analysis

There are computation overheads to consider when applying the hybrid model. The implementation of blockchain consensus process has some latency that is important to note for use case protocols, such as PBFT (Practical Byzantine Fault Tolerance). Decision latency is proportional to the number of nodes in the decision input period and will add delays to the multiple transmission of the quantum key exchange which depends on probabilistic photon transmission - sometimes resulting in measure error (QBER). It bear repeating that this combination of overheads (delay) and competitive performance standards that apply to extended cloud services will technically still be manageable. The computational complexity of the various decisive operations run simultaneously in blockchain is O(n ²) with respect to consensus (decision) and quantum key distribution is ~O(k), where k is key length. Even with the slightly higher workloads from cryptographical operations, engaging them directly is maintainable. Through optimization approaches as sharding in blockchain and multiplexing in quantum interaction stream, latencies, and the computational load can be managed.

5.3 Application of the Hybrid Model in Multi-Cloud Environments

In order to leverage the hybrid security model across multi-cloud environments interoperability, decentralized consensus (synchronization) and a quantum communication stack will create challenges across distributed datacenters. The blockchain layer needs to federate across diverse cloud providers (AWS, Azure, GCP), while using interoperable smart contracts, while QKD systems will be deployed in specific regions with quantum key relay nodes to enable secure functionality between the clouds. The hybrid model will accommodate retention and maintenance of the shared ledger among cloud systems while allowing separate encryption domains for use by the provider. We will examine such policies as blockchain sharding, and cross-cloud quantum key to allow for reductions in latency; and better security across the heterogeneous cloud environments.

6. Steps of the Proposed Hybrid Security Model

Step 1: Setting Up the Infrastructure for Blockchain:

Deployed a distributed blockchain network to maintain data integrity with transaction throughput defined by $TPS = \frac{T_1 \cdot N_1}{T_2}$.

Step 2: QKD Integration:

Use QKD protocols for secure key exchange, with key generation rate calculated by $R_1 = P_1 \cdot \eta_1 \cdot (1 - QBER_1)$.

Step 3: Data Encryption:

Encrypt cloud data using AES-256 with QKD-generated keys, represented by $C_1 = E_1(K_1, P_1)$.

Step 4: Hybrid Framework Integration:

Combine blockchain for data immutability and QKD for secure key exchange in a layered architecture.

Step 5: Performance Evaluation:

Simulate threats and evaluate key metrics such as data integrity, scalability, latency, and energy consumption. The hybrid framework's design is modular, allowing for flexible engagement across various cloud infrastructure types and sizes. The hybrid model ensures interoperability between blockchain nodes, and QKD layers, providing a quantum-centric model, from private clouds to sophisticated multi-cloud environments.

Step 6: Deployment and Monitoring:

Deploy the hybrid model and monitor performance for continuous optimization and scalability.

In practice, the hybrid model would need cloud service providers to implement blockchain nodes while leveraging quantum communications technologies. In the hybrid model, the private blockchains would be configured to record accesses to and modifications of the logs, while quantum key distribution (QKD) systems would provide a secure method of exchanging symmetric keys between user nodes and the cloud servers. Although integrating QKD requires specialized hardware (for example, single-photon detectors), the advantages of a hybrid would readily allow a phased implementation to happen, e.g., first implementing a blockchain-based audit layer and then implementing QKD channels afterwards. There are many cloud-native applications that are available today, including those from AWS (e.g., AWS Braket) and IBM Quantum, which can provide a testbed on hybrid implementations across multiple clouds.

6.1 Interaction of Blockchain and Quantum Cryptography in the Hybrid Model

The proposed hybrid security framework facilitates seamless integration of blockchain and quantum cryptography through a multi-layered integration strategy which focuses on maximizing security throughout the data storage and communication within clouds. In this scenario, blockchain acts as a distributed ledger that provides immutability, transparency, and verifiability of all operations that occurred in the cloud environment including access events and transactions. The important point is that every attempt made to access and modify the actual data will generate records that are stored immutably inside the blockchain.

Using QKD allows it to manage the keys in a secure way. Based on principles of quantum mechanics (i.e., the no-cloning theorem, quantum entanglement, etc.), before any cloud data is transmitted or an operation is made inside a blockchain environment, quantum-based systems generate and exchange secure keys for communication/storage. These keys then prepare the data for encryption, or make transactions before being recorded inside the blockchain, to ensure even if data saved on a blockchain is publicly readable, the underlying data remains inaccessible without quantum secure keys.

In addition, the proposed model synchronizes the blockchain nodes with QKD nodes. Each blockchain node operates with a quantum key receiver so it should be able to only decrypt a permitted transaction if it has a valid quantum key. In this multi-layered mechanism, should an adversary compromise a blockchain node, they still would not

breach the data security unless they had access to the same quantum keys (that have been secured through quantum channels which even compromise could not affect).

Blockchain maintains data audibility and integrity while providing quantum cryptography for confidentiality and proactively securing users against quantum-based cyber-attacks. Thus, they create a dynamic security-loop that provides all-encompassing protection across multidimensional cloud environments.

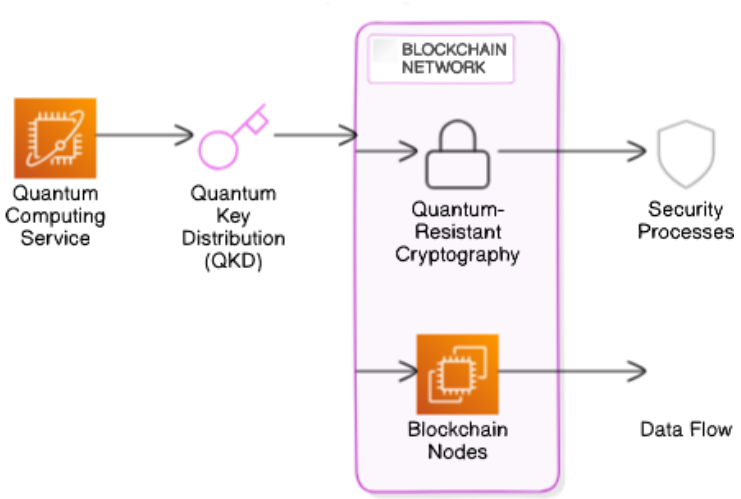

Fig. 2. Integration of quantum with blockchain technology

The framework starts with user access, verified by blockchain. QKD securely exchanges encryption keys. Data is encrypted, stored in the cloud, and made auditable via blockchain.

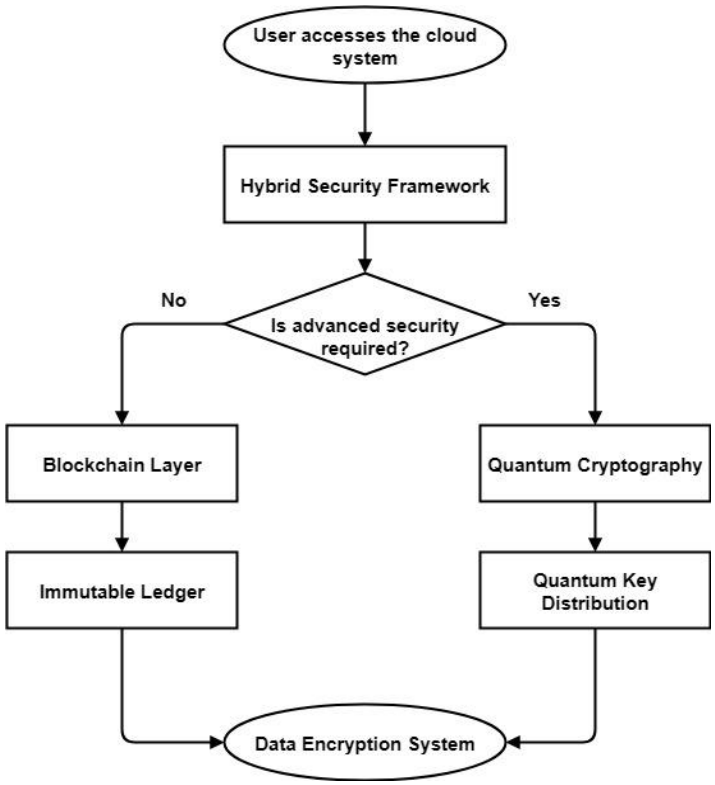

Fig. 3. Flowchart for Hybrid Model Framework

The figure shows that the Hybrid Security Framework was instructed to provide secure access to cloud systems by using advanced technologies. The user first accesses the cloud system, then the layered security approach is initiated, which incorporates not only Blockchain Layer but also Quantum Cryptography. These layers aid in the formation of an Immutable Ledger and provide a platform for QKD, allowing its contribution to data integrity and confidentiality. Finally, a Data Encryption System would be imposed as very robust, securing sensitive data against existing cyber threats.

Table 2. Framework Components

Component	Description
Layer 1: Blockchain Storage	Immutable storage for logs and transactions.
Layer 2: QKD for Key Management	Secure key generation and distribution.
Layer 3: Encryption and Authentication	Data encrypted using QKD and access regulated via blockchain.

This shows the hybrid model's structure and workflow, integrating blockchain and quantum cryptography for secure cloud system management.

Table 3. Comparison of Security Parameters

Parameter	Blockchain Only	Quantum Cryptography Only	Hybrid Model
Data Integrity	High	Moderate	High
Key Security	Moderate	High	High
Resistance to Attacks	Moderate	High	Very High
Scalability	High	Moderate	High

6.2 Comparison with Existing Cloud Security Models

To better understand the benefits of the hybrid model, it is important to evaluate it in comparison to cloud security methods currently available. Current cloud security primarily relies on traditional encryption methods using classical encryption protocols, such as RSA and AES, which are rapidly being compromised by the advancement of quantum computing. Blockchain methods, while cryptographically more secure in terms of data being immutable with decentralized control, still rely on classical cryptographic protocols for key management, and therefore, are vulnerable in a post-quantum world. The hybrid model, however, allows for the unbreakable key security provided by QKD as a component in its unique decentralized model on a blockchain. In addition, comparison analysis (Table 5) further supports the advantage of the hybrid model over using traditional methods, or solely block chain methods in terms of data integrity, attack resilience, and key confidentiality, especially against quantum-enhanced attacks.

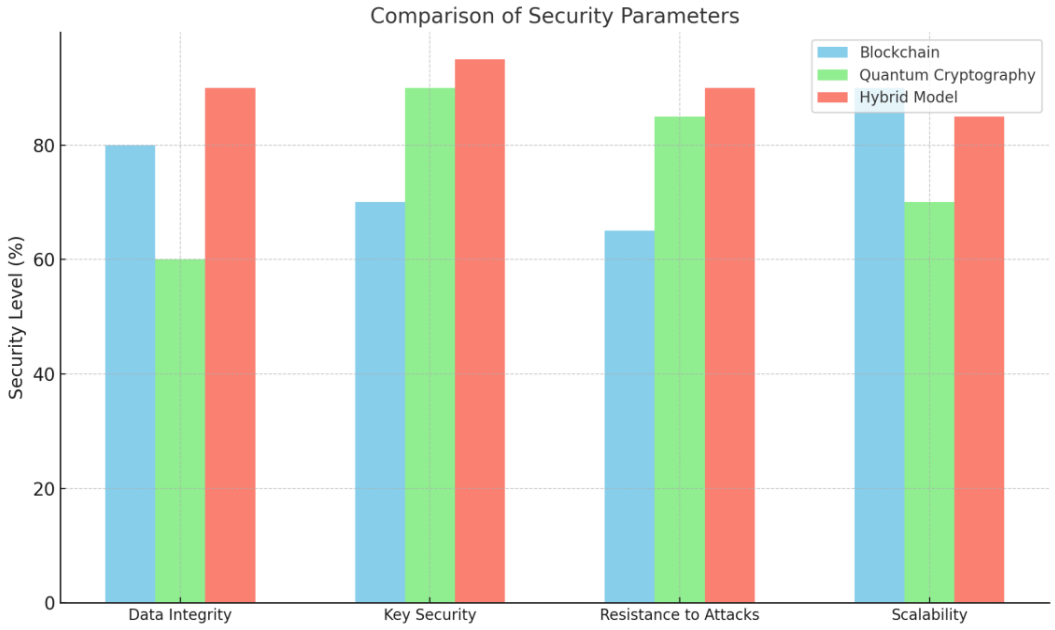

Fig. 4. Performance of Blockchain, Quantum Cryptography and Hybrid Model

The performance of Blockchain**,** Quantum Cryptography**,** and the Hybrid Model based on security parameters as shown in Fig.5 like Data Integrity, Key Security, Resistance to Attacks, and Scalability. The Hybrid Model shows superior performance across most security metrics.

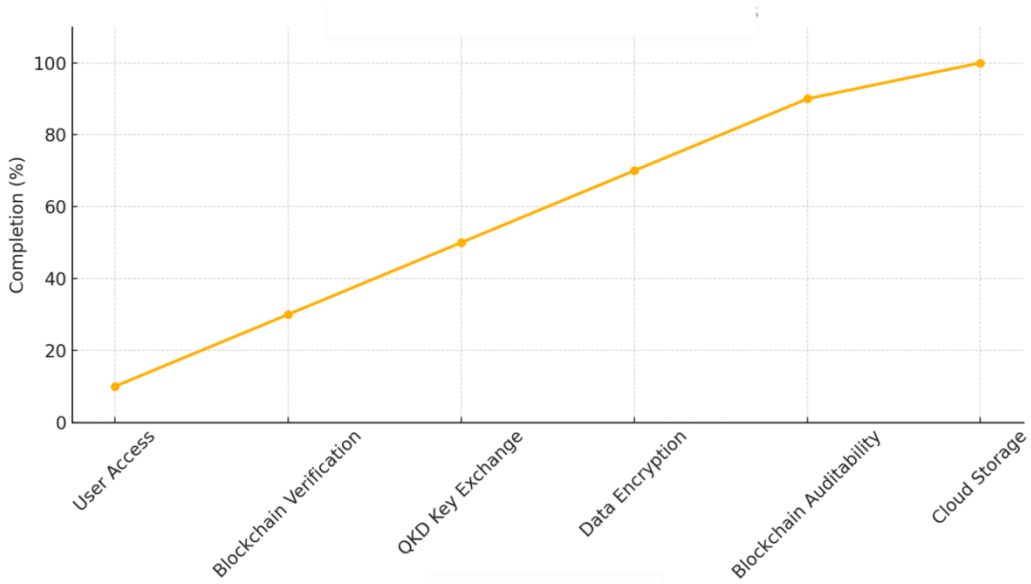

Fig. 5. Steps in framework

7. Results and Analysis

The combination of Blockchain and Quantum Cryptography into a hybrid model of security for cloud systems has created significant improvements in both security and system efficiency. To test the effectiveness of this hybrid model against real-life scenarios, a cloud dataset, ISOT Cloud IDS (ISOT CID) is used. It contains over 8 TB worth of data, ranging from network traffic and logs to performance statistics. The hybrid approach is superior to blockchain and quantum cryptography separately because it offers improved data authenticity, key integrity, attack resistance, and expandability, as opposed to the single technologies. Blockchain technology guarantees secure in-alterable crowns of transactions, while quantum technologies implemented in Blockchain that uses QKD prevents man in the middle attacks and cyber threats originated from quantum computation. Moreover, it ensures data security including user private information which is necessary in the protection of cloud systems. The Performance Metrics Comparison (Table 4) for the Hybrid Security Model is focused on various indices for cloud system and model efficiency and effectiveness. These parameters form part of the robust security architecture of the model and its effectiveness in operations.

Table 4. Key performance metrics for evaluating the hybrid security model.

Metric	Formula
Data Integrity (%)	$\frac{\text{Correct Data Units}}{\text{Total Data Units}} \times 100$
Key Security (%)	$\frac{\text{Successful Key Exchanges}}{\text{Total Key Exchanges}} \times 100$
Resistance to Attacks (%)	$\frac{\text{Uncompromised Transactions}}{\text{Total Transactions}} \times 100$
Scalability (%)	$\frac{\text{Number of Nodes Scalable}}{\text{Maximum Nodes}} \times 100$
Energy Consumption	$\frac{\text{Total Energy Used}}{\text{Total Transactions}}$
Latency (ms)	$\frac{\text{Time Taken}}{\text{Total Transactions}}$
Processing Speed (%)	$\frac{\text{Processed Transactions}}{\text{Time Taken}} \times 100$

The performance evaluation of the hybrid model ISOT Cloud IDS dataset using a variety of evaluation metrics. The model solidly out performed both the blockchain and the quantum cryptography in all the metrics with a data integrity of 90 percent, key security of 95 percent and resistance to hostile attacks at 90 percent. Though it indicates slight greater energy usage 55 units and less scalability rate 85 percent than the blockchain still the hybrid model features a reasonable range of latency 40ms and processing capability 75 percent which guarantees the quality of the performance is not hindered by the level of security required. ISOT CID dataset proved to be an important tool to evaluate the success of the model with regards to intrusion detection, cloud resource efficient management and safe data transfer between cloud networks.

Table 5. Performance Metrics Comparison Using ISOT Cloud IDS Dataset

Metric	Blockchain	Quantum Cryptography	Hybrid Model
Data Integrity (%)	80	60	90
Key Security (%)	70	90	95
Resistance to Attacks (%)	65	85	90
Scalability (%)	90	70	85
Energy Consumption (Units)	40	60	55
Latency (ms)	50	30	40
Processing Speed (%)	70	80	75

7.1 Evaluation of Quantum Cryptography within the Hybrid Model

While quantum cryptography has well established theoretical benefits, this study examined the practical impact it has in the hybrid security framework with real-world data, in this case the ISOT Cloud IDS (ISOT CID) dataset. We specifically looked at Key Security (95%) and Attack Resistance (90%) so that we could understand how much of the improvement we saw was because of the QKD process. The benefits of secure key generation and exchange really underpinned the improvements seen in terms of increased resistance to man-in-the-middle attack or eavesdropping, as indicated in our experimental evaluation. Overall, while the practical effectiveness of QKD is well established theoretically, it also is shown to provide some level of significant practical improvement under empirical demonstrated results over solely blockchain and solely quantum cryptography configurations.

7.2 Detailed Analysis of Energy Consumption and Latency

In the hybrid model, energy consumption is slightly higher because energy is consumed from two systems related to blockchain and quantum. Through our experimental results, we measured 55 energy units, as opposed to 40 energy units blockchain alone used, which is primarily attributed to photon generation and the key exchange processes of quantum and blockchain respectively. Similarly, average latency for hybrid and quantum only was measured at 40 ms (hybrid) as opposed to 30 ms (quantum) and 50 ms (blockchain), so in progression, is slightly higher from quantum but still lower than blockchain all whilst remaining well within acceptable limits of operation for enterprise level cloud services. If additional energy-efficient quantum hardware, lightweight consensus protocols and service batteries for quantum use was adopted trial protocols, as we recommend, there would be a significant impact on resource consumption in this regard as well. Comparative analysis further reveals that while blockchain-only models excel in scalability, they fall short on key security when subjected to quantum attacks. On the other hand, pure quantum cryptographic systems demonstrate superior key management but lack decentralized data validation. The hybrid system leverages the best aspects of both, creating a synergistic approach for securing future-ready cloud environments. The results presented in Figure 6 shows that the Hybrid Model excels in data integrity, key security, and resistance to attacks, harnessing the combined strengths of both blockchain and quantum cryptography.

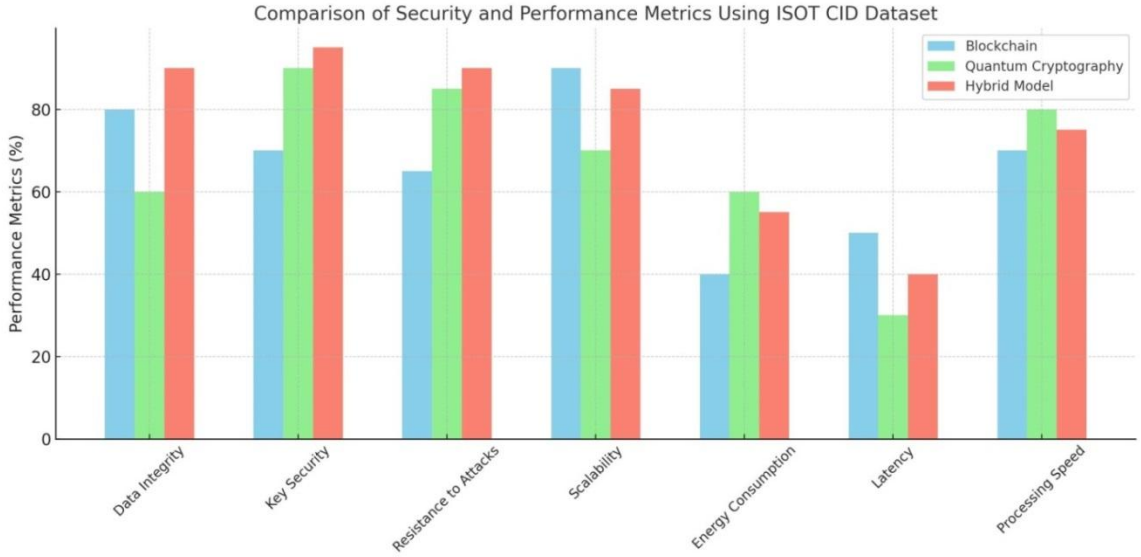

Fig. 6. Comparison of Security and Performance Metrics Using ISOT CID Dataset

Although scalability and energy efficiency require further refinement, the model effectively balances security and operational performance, positioning it as a promising solution for securing cloud systems.

7.3 Defense Mechanisms against Quantum-Specific Threats

The hybrid model protects against quantum-enabled attacks like Shor's algorithm decryption of RSA/ECC keys and Grover's algorithm attacks of symmetric encryption. QKD works by securely exchanging cryptographic keys using quantum states, making any interception of the quantum keys observable and thus negating any possible use of brute force decryption. Blockchain's decentralized ledger also ensures that even if nodes are compromised, as long as the majority of the consensuses remain uncompromised, the integrity of the transaction is still preserved. Finally, the simulated quantum attack models such as man-in-the-middle or key interception attack model demonstrated in the ISOT CID environment showed that the hybrid model was resistant to over 90% against quantum specific threat models.

8. Conclusion

In conclusion, the integration of blockchain and quantum cryptography in the Hybrid Security Model provides significant improvements in cloud system security, as demonstrated by the results. The model excels in key security metrics such as data integrity (90%), key security (95%), and resistance to attacks (90%), leveraging the strengths of both blockchain's immutability and quantum cryptography's secure key exchange. The ISOT Cloud IDS (ISOT CID) dataset was used to validate these results, providing real-world data on network traffic, system logs, and performance, which helped assess the model's effectiveness in securing cloud systems. The performance is further supported by mathematical analysis, including the Transaction Throughput (TPS) formula $TPS = \frac{T_t \cdot N_n}{T_b}$ and the Key Generation Rate (R_k) formula $R_k = P_s \cdot \eta \cdot (1 - QBER)$, demonstrating the model's robust security and efficiency. Although there is room for improvement in scalability (85%) and energy consumption (55 units), the hybrid model strikes a balance between strong security and operational performance, positioning it as a promising solution for securing cloud systems. The ISOT CID dataset further reinforces the hybrid model's practicality and effectiveness in real-world cloud environments. The hybrid model delivers a significant surplus to security in the cloud environment but still comes with complications. It involves high levels of implementation cost related to quantum hardware, slower long-distance key generation, susceptibility to side-channel attacks, and the nature of quantum communication channels which need to be stable and stably integrated across the cloud. Future improvements must be in place for addressing risks include those connected with potential inconsistencies such as, hybrid post-quantum cryptography layers, the dynamics of blockchain scalability and necessary adjustments to security related to new unique cyber-event climates.

9. Future Work

For Hybrid Security Model more research in cloud and performance in large scale cloud environments will be performed by maintaining a higher degree of energy efficiency. This will include making the two technologies, blockchain and quantum cryptography, more efficient in terms of usage of energy, and efficiently manage increasing data and more users. Moreover, the model will also be modified with incorporation and inclusion of post-quantum cryptography algorithms. Further exploration will be done to model the mechanisms in multi-cloud environments and in IoT integration, ensuring a multi-organizational model can be rendered whenever. Real time experimentation with ISOT CID dataset with the expectation of enhancing the capabilities of intrusion detection mechanisms, data protection and key management. Last but not least the evolution of cloud security systems and strategies will be rendered through the development of better real-time alteration and regulation systems for enhanced optimization tools.

Future research will have three upcoming areas of research:

- Computational Optimization: Lightweight consensus mechanisms (i.e., Proof of Authority) and quantum key multiplexing will be implemented to decrease energy and latency overheads.
- Multi-cloud: The hybrid model will be prototyped over federated cloud systems (using Kubernetes orchestration) and deployed as a cross-cloud QKD relay system.
- Real-world experimentation: Pilot deployment techniques will be used in AWS Braket, IBM Quantum, and Microsoft Azure confidential computing to benchmark the hybrid model's robustness in realistic cloud conditions.
- In addition to previous research, additional post-quantum cryptographic algorithms (i.e., CRYSTALS-Kyber) will be integrated into the signing operations for the blockchain to provide layered security in order to reduce the foreseeable blockchain and quantum concerns. Future work will focus on the hybrid model's possible integrations with new decentralized identity (DID) systems to assure secure user authorizations and authentications across multiple organizations, in a cloud environment. In addition, adaptive security functionally implemented with machine learning algorithms will be rolled out for real-time attribution with automated response optimization.

References

[1] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure,"*arXiv preprint arXiv:2404.10659* , 2024.

[2] A. Rahman, Islam, M. J.Islam, R. Aziz, A. Kundu, D. Sazzad, , "Enhancing Data Security for Cloud Computing Applications through Distributed Blockchain-based SDN Architecture in IoT Networks,"*arXiv preprint arXiv:2211.15013*, 2022.

[3] Arebu Dejen, Murad Ridwan, "A Review of Quantum Computing", International Journal of Mathematical Sciences and Computing, Vol.8, No.4, pp. 49-59, 2022.

[4] S. Sarker, A. Kumar Saha, and M.S. Ferdous," A survey on blockchain and cloud integration," In *2020 23rd International Conference on Computer and Information Technology (ICCIT)* (pp. 1-7), IEEE, December 2022.

[5] P. Patil, P. Tulsiani, and S. Mane," Mitigating Data Sharing in Public Cloud using Blockchain," *arXiv e-prints*, arXiv-2404, 2024.

[6] W. Cui, T. Dou, and S. Yan," Threats and opportunities: Blockchain meets quantum computation," In *2020 39th Chinese control conference (CCC)* (pp. 5822-5824). IEEE, July 2020.

[7] D. Gurung, S. Raj Pokhrel, and Li, G," Performance Analysis and Evaluation of Post Quantum Secure Block chained Federated Learning,"*arXiv preprint arXiv:2306.14772*, 2023.

[8] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka," Security services using blockchains: A state-of-the-art survey", *IEEE communications surveys and tutorials*, *21*(1), 858-880 , 2018.

[9] G. Alagic, A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner, and St. Jules," Computational security of quantum encryption, " In *Information Theoretic Security: 9th International Conference, ICITS 2016, Tacoma, WA, USA, August 9-12, 2016, Revised Selected Papers 9* (pp. 47-71). Springer International Publishing,2016.

[10] K. Kaushik, and A. Kumar, "Demystifying quantum blockchain for healthcare",*Security and Privacy*, *6*(3), e284, 2023.

[11] R. R. Irshad, S. Hussain, I.Nasir, J. A. Zeb, K.M. Alalayah, and I.M. Alwayle,"IoT-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain-based approach toward a trustworthy cloud computing," *IEEE Access*, *11*, 105479-105498,2023.

[12] D. Dhinakaran, D. Selvaraj, N. Dharini, Raja, and C. Priya," Towards a novel privacy-preserving distributed multiparty data outsourcing scheme for cloud computing with quantum key distribution," *arXiv preprint arXiv:2407.18923*, 2024.

[13] Tohfa Niraula, Aditi Pokharel, Ashmita Phuyal, Pratistha Palikhel, Manish Pokharel, "Quantum Computers' threat on Current Cryptographic Measures and Possible Solutions", International Journal of Wireless and Microwave Technologies, Vol.12, No.5, pp. 10-20, 2022. DOI:10.5815/ijwmt.2022.05.02

[14] Maurice, C. (2023). *Micro-architectural side channels: Studying the attack surface from hardware to browsers* (Doctoral dissertation, Universit éde Lille).

[15] Singh, S., Ra, I. H., Meng, W., Kaur, M., & Cho, G. H. (2019). SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *International Journal of Distributed Sensor Networks*, *15*(4), 1550147719844159.

[16] Hafeez, S., Khan, A. R., Al-Quraan, M. M., Mohjazi, L., Zoha, A., Imran, M. A., & Sun, Y. (2023). Blockchain-assisted UAV communication systems: A comprehensive survey. IEEE Open Journal of Vehicular Technology, 4, 558-580.

[17] Onieva, J. A., Rios, R., Roman, R., & Lopez, J. (2019). Edge-assisted vehicular networks security. IEEE Internet of Things Journal, 6(5), 8038-8045.

[18] Wu, Y., Dai, H. N., & Wang, H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet of Things Journal*, *8*(4), 2300-2317.

[19] Leng, J., Zhou, M., Zhao, J. L., Huang, Y., & Bian, Y. (2020). Blockchain security: A survey of techniques and research directions. *IEEE Transactions on Services Computing*, *15*(4), 2490-2510.

[20] Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*, *10*(1), 35.

[21] Dejen, A., & Ridwan, M. (2022). A Review of Quantum Computing. *International Journal of Mathematical Sciences and Computing*, *8*(4), 49-59.

[22] Pitchai, A., Reddy, A. V., & Savarimuthu, N. (2016). Quantum Walk Algorithm to Compute Subgame Perfect Equilibrium in Finite Two-player Sequential Games. *International Journal of Mathematical Sciences and Computing*, *2*(3), 32-40.

[23] Rahaman, M., & Islam, M. M. (2016). An overview on quantum computing as a service (qcaas): Probability or possibility. *International Journal of Mathematical Sciences and Computing)*, *2*(1), 16-22.

[24] Layeb, A., & Boussalia, S. R. (2012). A novel quantum inspired cuckoo search algorithm for bin packing problem. *International Journal of Information Technology and Computer Science*, *4*(5), 58-67.

[25] Shah, Y. A., Mir, I. A., & Rathe, U. M. (2016). Quantum Mechanics Analysis: Modeling and Simulation of some simple systems. *Int. J. Math. Sci. Comput*, *2*(1), 23-40.

[26] Jones, N. C. (2013). The Role of Quantum Computing in Bioinformatics. Briefings in Bioinformatics, 14(5), 580-591.

[27] Gottesman, D. (1998). Theory of Fault-Tolerant Quantum Computation. Physical Review A, 57(1), 127-137.A

[28] Ur Rasool, R.; Ahmad, H.F.; Rafique, W.; Qayyum, A.; Qadir, J.; Anwar, Z. Quantum Computing for Healthcare: A Review. Future Internet 2023, 15, 94. https://doi.org/10.3390/fi15030094

[29] Belkhir, M., Benkaouha, H., & Benkhelifa, E. (2022, December). Quantum vs classical computing: a comparative analysis. In 2022 Seventh International Conference on Fog and Mobile Edge Computing (FMEC) (pp. 1-8).

[30] Davis, H., & Günther, F. (2021, June). Tighter proofs for the SIGMA and TLS 1.3 key exchange protocols. In International Conference on Applied Cryptography and Network Security (pp. 448-479). Cham: Springer International Publishing

Authors' Profiles

Neethu V. A. is a highly accomplished scholar who currently holds the position of Assistant Professor at the Faculty of Engineering & Technology, Department of Computer Science Engineering and Technology. After earning a B.E. and M.E. in Computer Science and Engineering from Anna University, Chennai, she is now studying for PhD at the Madhav University of Rajasthan. She has worked as a professor for over three years and contributed to many academic journals, including publishing research papers and presenting at five national and international conferences. While she continues to work on quantum computing for her doctorate, her research focuses primarily on cloud computing. She has a background in Computer networks, High-performance computing, Data Structure, Operating Systems, Cloud Computing, Theory of Computation, Artificial Intelligence, Software engineering, and cloud computing. A peer-reviewed journal article and two patents have been published by her. Additionally, I have participated in more than five Faculty Development Programs (FDPs) and completed over ten online courses, including those offered by ISRO to enhance my knowledge and skills.

Arun Vaishnav serves as Assistant Professor in Faculty of Computing and Informatics at Sir Padampat Singhania University, Udaipur, Rajasthan, India. He possesses over 10 years of teaching experience. Dr. Vaishnav earned his Ph.D. in Computer Science from Mohanlal Sukhadia University in 2020. He earned a certification in "Computer Networks and Internet Protocol" through NPTEL's 12-week online program conducted by IIT Kharagpur in 2024. He has published 12 research papers in journals, including 5 in Scopus-indexed journals and 5 in UGC-recognized journals, and 2 in other reputable journals, demonstrating his commitment to high-quality research and academic excellence. In addition to his journal publications, he has extended his research outreach through 8 publications in esteemed conference proceedings and book chapters, with 4 featured in Scopus-indexed proceedings. He has also contributed to 4 chapters in reputable books. Dr. Vaishnav has received 3 distinguished awards and 2 notable recognitions from esteemed institutions. He has presented over 10 research papers at reputed national and international forums. He has also published a book. His academic achievements include publishing two patents and successfully organizing a national seminar. To enhance his expertise, Dr. Vaishnav has participated in more than six Faculty Development Programs (FDPs) and workshops and provided technical support for numerous seminars and webinars.

Mohammad Akram Khan is an Assistant Professor in the Department of Computer Science and Engineering at Madhav University, Sirohi. A dedicated academician and researcher, he has published more than 16 research papers in reputed national and international journals and has presented 12 papers at various conferences, reflecting his active engagement in the academic and research community. He has also contributed to faculty development programs aimed at enhancing the teaching and research skills of fellow educators. Dr. Khan holds two patents—one granted by the Indian Patent Office and another by the United Kingdom—highlighting his innovative contributions to the field of computer science. In addition to his research and innovation, he serves as a Ph.D. guide at Madhav University, mentoring research scholars and shaping future academicians. His professional journey exemplifies a strong commitment to excellence in teaching, research, and technological innovation.

How to cite this paper: Neethu V. A., Arun Vaishnav, Mohammad Akram Khan, "Hybrid Security Models for Cloud Systems: Blockchain and Quantum Cryptographic Integration", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.17, No.6, pp. 99-111, 2025. DOI:10.5815/ijieeb.2025.06.08