iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69333

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Integrating Blockchain and Quantum Cryptography in Hybrid Security Models for Cloud Systems

Neethu V A[1], Dr. Mohammad Akram Khan[2]
[1]*Research Scholar, Department of Computer Science and Engineering, Madhav University, Abu Road, Rajasthan, India*
[2]*Doctor ,Assistant Professor, Department of Computer Science and Engineering, Madhav University, Abu Road, Rajasthan, India*

Abstract: ***Cloud technology has revolutionized data management by removing time-consuming worries about accessibility and appropriate storage, which can now be managed remotely. However, it may also be claimed that as this technology has advanced, a number of issues about data integrity, secrecy, and authentication have emerged. The authors of this study put forward a hybrid security model that tackles security issues in both cloud and quantum frameworks by combining blockchain technology with quantum cryptography. This strategy targets some of the deficiencies that have been recognized in this context. Confidentiality, integrity, and availability are the three critical dimensions of data that are vital for its protection and security, and cloud technology is known to present numerous challenges regarding these three aspects. Blockchain technology, on the other hand, makes data transparent, decentralized, and unchangeable, which lowers the possibility of unwanted access. The combination of tactics suggested in this article aids in removing several issues that are prevalent in cloud infrastructure, such as data loss, key loss, and man-in-the-middle assaults. In order to improve data security, this study demonstrates the hybrid model's structural design, data transfer, and architectural procedures. The model's research indicates that it has benefits over both a simply created blockchain model and a traditional encryption approach. Additionally, performance benchmarks are provided, proving the model's resistance to cyberattacks in the quantum era. The architecture elevates cloud security and blends in seamlessly with the present cloud status higher by resolving the significant obstacles and is prepared for wider deployment. In order to achieve greater security in today's complex cloud systems, the directed efforts will involve expanding the model to different cloud infrastructures and increasing the system's computing efficiency.***

Keywords: Blockchain Technology, Quantum Cryptography, Hybrid Security Mode, Cloud Security, Quantum Key Distribution (QKD), Post-Quantum Cryptography, Data Integrity and Scalability

I. INTRODUCTION

Cloud computing is the backbone of the internet today because data can be processed, stored and fetched through cloud computing. But, with increased adoption of cloud services brings significant security risks — data loss, system abuse, even key cracking. Quantum computing is gradually rendering ordinary encryption methods obsolete, which means new security measures for sensitive data in the cloud need to be put in place. Let us take a look at a more sophisticated solution which combines blockchain infrastructure with post-quantum encryption. The blockchain does this work by creating a more or less immutable distributed ledger that authenticates the records, and authentication is guaranteed through Quantum Key Distribution (QKD), through which quantum mechanical techniques are utilized for the secure administration and transmission of keys.To demonstrate how IT technologies are used to provide consistent, quick, and dependable outcomes, this study examines the importance of computer system dependability across a variety of disciplines, including computer science, physics, chemistry, and engineering [1]. This framework offers new methods to mitigate risks due to emerging threats arising in classical and quantum architectures while remaining agnostic of a large number of environments and requirements.

II. PROBLEM STATEMENT

Even with the advancement of cloud systems, the safeguards that have been put in place are insufficient to protect the data from the threats posed by sophisticated cyber attacks, especially now that quantum computers are becoming more prevalent and threatening long-held encryption principles.

A. *Significance of the Study*

The combination of blockchain technology and quantum cryptography offers a new approach to cloud protection that not only addresses existing vulnerabilities but also provides a robust mechanism that is likely to withstand cyber attacks in the quantum era. This study increases system resilience while also laying the groundwork for a multi-cloud infrastructure.

III. OBJECTIVES

1) To determine and evaluate the limitations of existing cloud security models against quantum attacks.
2) Develop a hybrid secure architecture using blockchain and quantum cryptography.
3) Enhance secure data storage and transfer through QKD.
4) Determine the scalability and performance of the hybrid model.
5) Examine and compare the performance of classical and quantum cyber hackers against the model.
6) Examine and determine the practicability of deploying the hybrid model in various real-world cloud scenarios.
7) Examine optimization and future research avenues.

IV. LITERATURE SURVEY

In recent years, the integration of blockchain technology and quantum cryptography with hybrid security models for cloud systems has gained much research attention. The convergence of encryption, blockchain and quantum cryptography will be the cornerstone of nextgen secure cloud computing infrastructures. Solving for cost, scalability, and seamless integration will be the key to enable help for the upcoming years of cloud security.

This is achieved by incorporating AES block permutation and hybrid public encryption method that statistically conveys superior security and unpredictability[3]. In the mentioned context shows that quantum computing changes your infrastructure and the importance of proper protection in the quantum age. Rahman et al. [4] recommended a distributed blockchain SDN architecture for IoT networks and also considered application-level security issues and solutions for cloud computing. It [5] describes the challenges and benefits of integrating blockchain technology with cloud computing in-depth. In the context of problems of data sharing, use blockchain to ensure the security of the data and to guarantee its integrity in public clouds, which means allowing the data to be shared without compromising its integrity[6]. To explore the territory of concern and potential at the junction of blockchain and quantum computation [7]. Blockchain performance federated learning in with post-quantum security measures and this PQQM federation [8].

It provides examples of the sequenced spatiotemporal gapping of security services derived from blockchains and suggests both new and old developments thereafter[9]. Address computational aspects of quantum encryption security, which is crucial to developing secure quantum cryptosystems [10]. It has done the job of interpreting the applications of quantum blockchain in the medical sector with examples New changes enhance even more the importance of this connection [11]. For example, implements post-quantum cryptographic security along with blockchain technology in an IoT cloud computing system that was built to be reliable [12]. In addition, [13] designed a cloud computing application where Multi-Party Data Outsourcing was introduced and Quantum Key Distribution was used to prevent international attacks. The above works in concert show the transformation of hybrid models of security through the growing integration of blockchain and quantum-safe cryptography to newly discovered security challenges in cloud systems.

V. DATASET

In this research, Hybrid Security Evaluation Dataset (HSED) is used to evaluate hybrid models which integrate blockchain and quantum cryptography into the cloud systems. Blockchain transaction data set, quantum cryptography data sets (key exchange logs, error rates and bit rates), cloud system logs (user IDs, control events, amount of traffic), and artificially generated attack data (man-in-the-middle and quantum attacks).

Figure 1 represents the hierarchy of the set. These elements help in determining the robustness of the security feature against various attacks. Further, it makes use of ISOT Cloud IDS (ISOT CID) dataset, being a real cloud-based dataset having traffic, system logs and performance data to evaluate the hybrid model in case of cloud based intrusion detection. These components in the dataset make it possible to verify the mechanism on board-area.

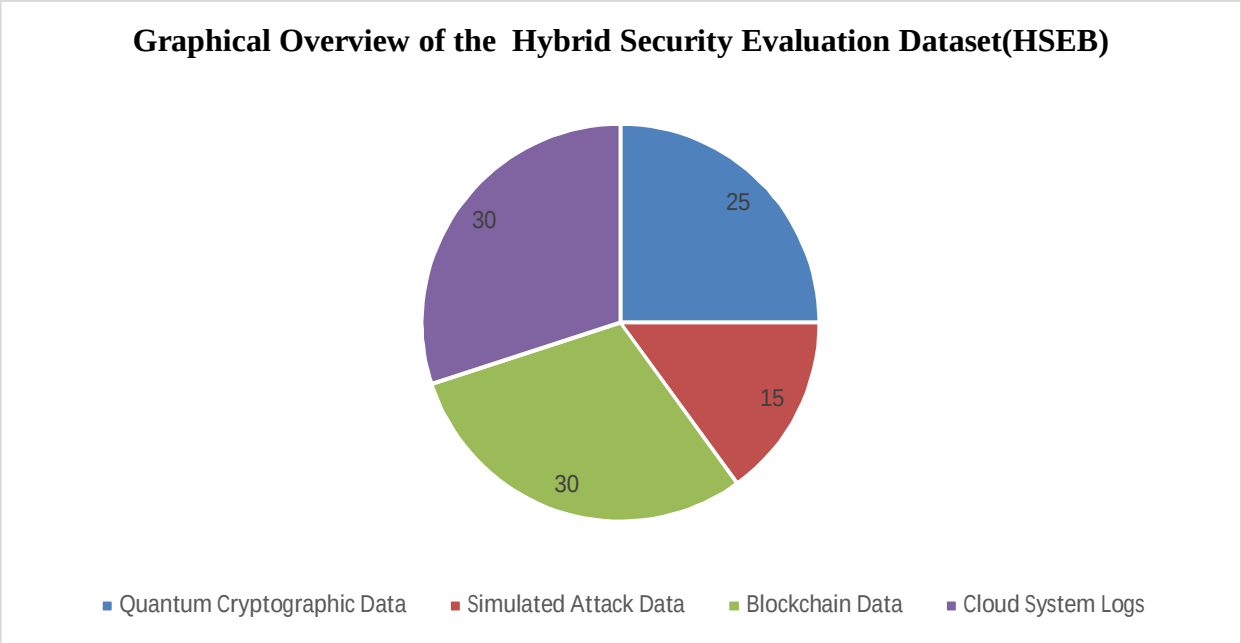


Figure 1. The distribution of data components in the Hybrid Security Evaluation Dataset (HSED).

TABLE 1
DATASET COMPONENT

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

This table summarizes the key components of the Hybrid Security Evaluation Dataset (HSED).

VI. PROPOSED METHODOLOGY

The proposed framework provides a hybrid security model taking into account quantum cryptography integrated with blockchain technology to meet the cloud systems' changing security requirements for both future and current computing that accounts for this change. Guaranteed data integrity and ability to audit transactions: Blockchain stores its record in a decentralized and unchangeable manner. Its rate of transactions per second is stated as:

$$TPS = \frac{T_t \cdot N_n}{T_b} \text{ ----------(1)}$$

Where T_t is the number of transactions per block, N_n is the number of nodes participating in the consensus process, and T_b is the block time. To enhance the security, the QKD protocol is now integrated for key exchanges. The key generation rate is defined as:

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

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:

$$C = E(K, P) \text{ ----------(3)}$$

Where K is the QKD-generated key and P is the plaintext. Such architecture is similar to the layered model and its interaction with storage and with distributed ledger systems, where each layer is synchronized with any involvement of QKD systems as demonstrated in figure 2. Performance metrics (data integrity, scalability, latency, and energy consumption) are measured by simulating the potential threats, highlighting the hybrid model's robustness and efficiency in addressing modern cloud security challenges.

A. Steps of the Proposed Hybrid Security Model

1) Infrastructure Setup For Blockchain: A Distributed Blockchain Network has been Deployed to Carry Out Data Integrity with A Defined Transaction Throughput by $TPS = \frac{T_1 \cdot N_1}{T_2}$.

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

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

4) Layering Approach: Blockchain is to ensure data immutability, while QKD is for secure key exchange.

5) Performance Metrics: Profile threats and benchmark crucial metrics (data integrity, scalability, lag and energy consumption)

6) Deployment and Monitoring: Deploy the hybrid model and monitor the performance for continuous optimization and scalability.

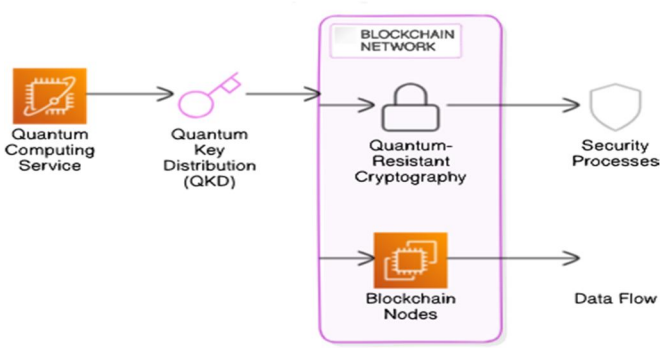


Figure 2. Integration of quantum with blockchain technology

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.

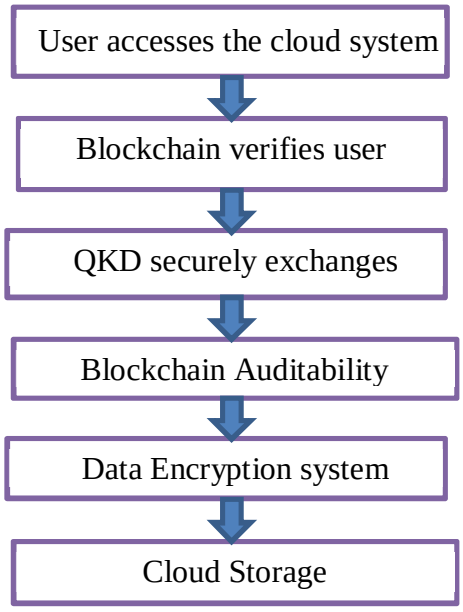


Figure 3. Flowchart for Hybrid Model Framework

TABLE 2
FRAMEWORK COMPONENTS

Component	Description
Layer 1: Blockchain Storage	Non modified storage of logs and transactions
Layer 2: QKD for Key Management	Safe Key Creation and distribution.
Layer 3: Encryption and Authentication	Data encrypted using QKD and access controlled through 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	Quantum Cryptography Only	Blockchain Only	Hybrid Model
Scalability	Moderate	High	High
Data Integrity	Moderate	High	High
Resistance to Attacks	High	Moderate	Very High
Key Security	High	Moderate	High

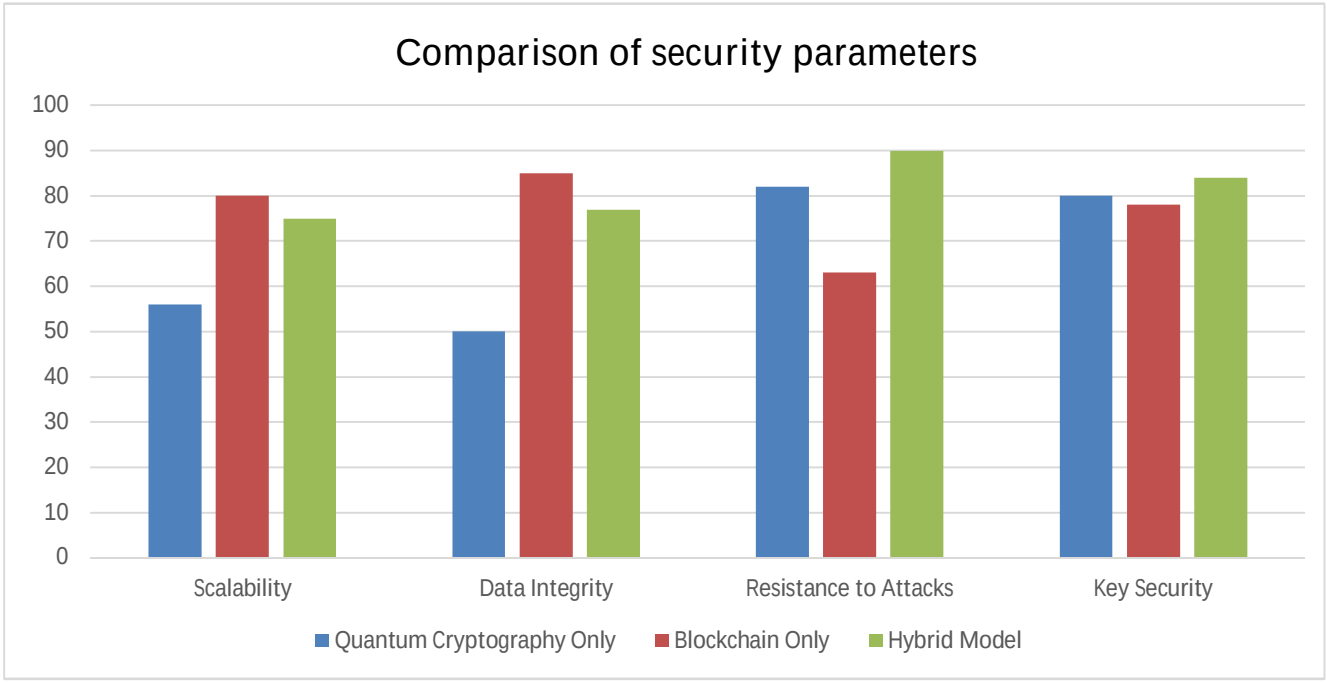


Figure 4. Performance of Blockchain, Quantum Cryptography and Hybrid Model

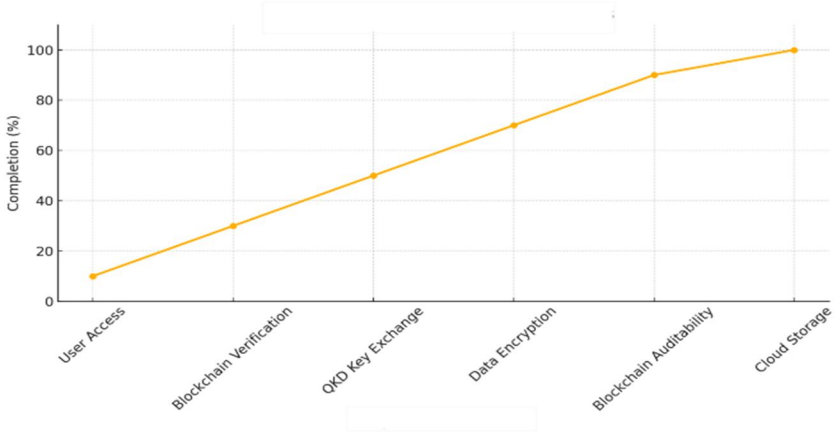


Figure 5. Steps in framework

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

VII. RESULTS AND ANALYSIS

The implementation of blockchain technology coupled with quantum crypto in a hybrid cloud security model has been responsible for marked system performance and security enhancements. The practice is tested on the cloud using a data set called ISOT Cloud IDS (ISOT CID) to observe how well it really works in the real world conditions. Here we have data of the size of around 8 TB that includes performance stats, network traffic, and logs. The hybrid solution provides more reliable data authenticity, key integrity, attack resistance, and expansion than solely blockchain and quantum cryptography do, thus it is a better choice of both technologies independently. Quantum technologies associated with blockchain, which use Quantum Key Distribution (QKD), offer the user protection against cyber risks and man-in-the-middle attacks. On the other hand, blockchain technology ensures safe and unchangeable transactions. Not only that, it makes sure data security, including privacy of users, be there because they are one of the most important things that we should take into account when it comes to securing clouding technology. The Hybrid Security Model's Performance Metrics Comparison (Table 4) covers various aspects indicating the effectiveness and efficiency of cloud systems and models. These parameters are the supporting factors for implementing the model's strong security architecture and operational efficacy.

TABLE 4
KEY PERFORMANCE METRICS FOR EVALUATING THE HYBRID SECURITY MODEL.

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

There was a performance evaluation conducted on the hybrid model ISOT Cloud IDS dataset that used a variety of evaluation metrics. The model outperformed both the blockchain and the quantum cryptography models in all the metrics with a data integrity of 90 percent, key security of 95 percent, and resistance to hostile attacks at 90 percent. Although it does show a slight energy usage of 55 units and a lesser scalability rate of 85 percent than the blockchain, still the hybrid model could achieve a reasonable range of latency 40ms and processing capability 75 percent which ensures the quality of the performance is not impaired by the required level of security. ISOT CID dataset has been proven to enable the evaluation of the model's success regarding the detection of intrusion, efficient management of the cloud resources, and safe data transfer between cloud networks

TABLE 5
PERFORMANCE METRICS COMPARISON USING ISOT CLOUD IDS DATASET

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

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.

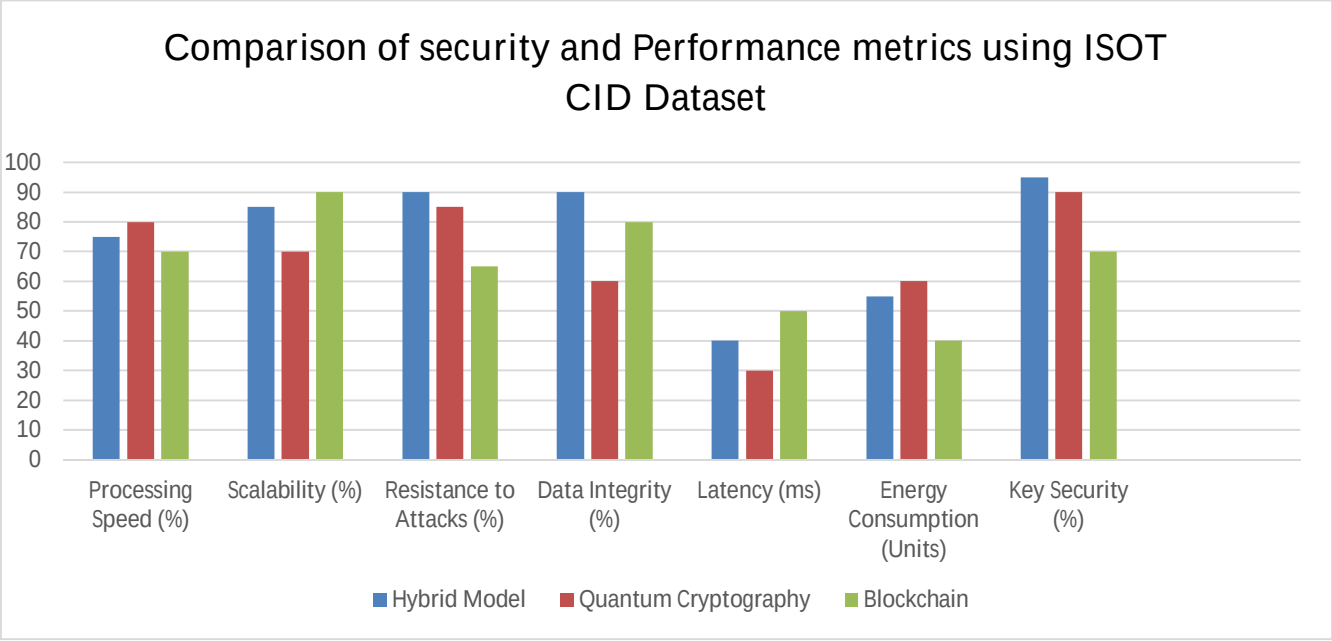


Figure 6. Comparison of Security and Performance Metrics Using ISOT CID Dataset

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.

VIII. CONCLUSION

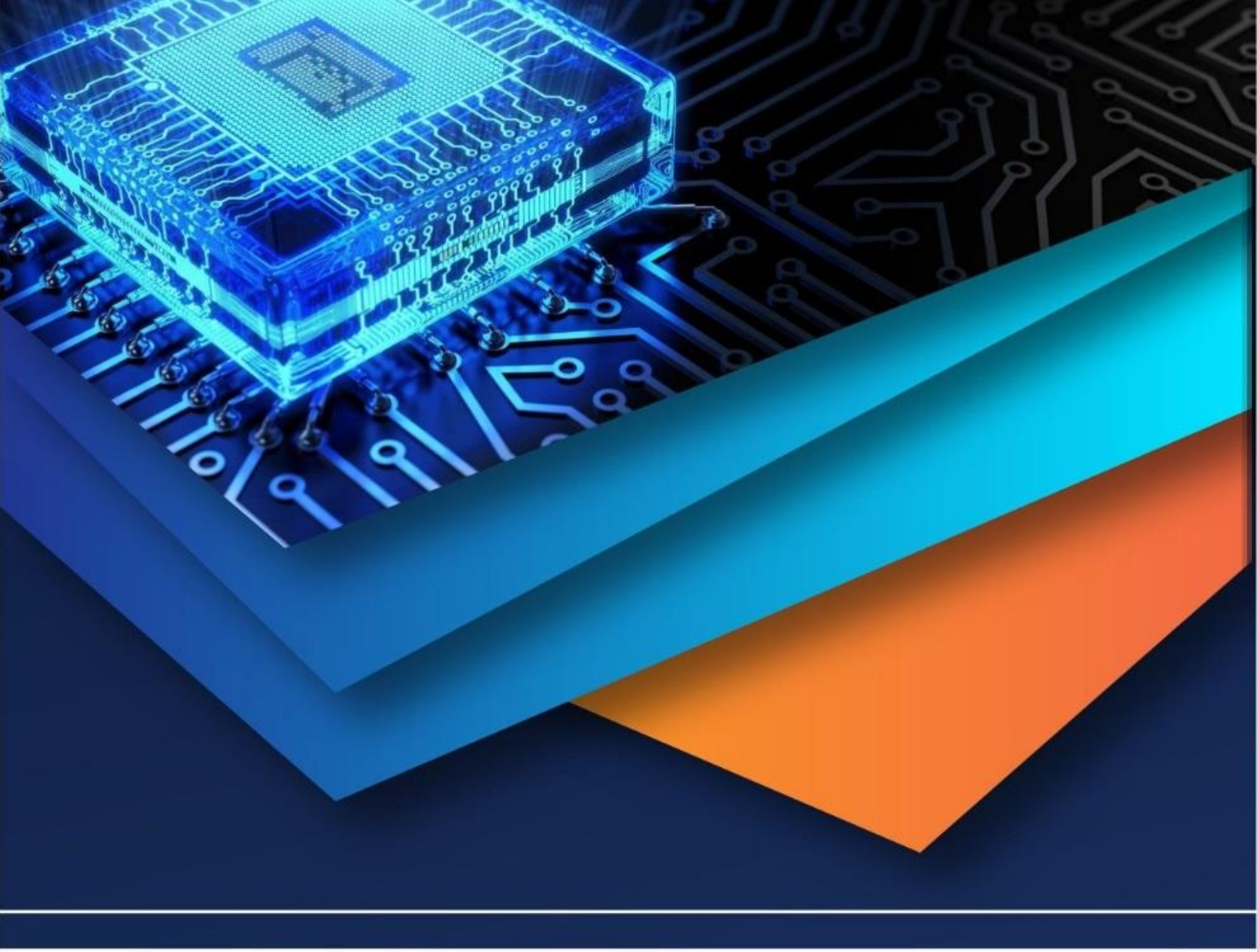
In conclusion, the results show that the Hybrid Security Model's combination of blockchain and quantum cryptography significantly enhances the security of cloud systems. The approach uses the advantages of both blockchain's immutability and quantum cryptography's safe key exchange to achieve high performance in important security metrics including data integrity (90%), key security (95%), and attack resistance (90%). So, when we dive into the ISOT Cloud IDS (or ISOT CID) dataset, we're looking at a mix of actual network traffic, system logs, and performance data. This really helps in figuring out how well the model works to protect cloud systems. the conclusions we'd reached didn't spring out of the void. Nope, they were backed by some serious analysis of data. This isn't a joke, we're effectively going through the Transaction Throughput (TPS) formula, which literally tells us more about our performance metrics. When you combine all of that, it starts to show a lot more clearly the strengths and abilities of the model. $TPS = \frac{T_t \cdot N_n}{T_b}$ and the Key Generation Rate (R_k) formula $R_k = P_s \cdot \eta \cdot (1 - QBER)$, demonstrating the strength of the a for mentioned model's security and efficiency. Hybrid model: 85% Scalability; 55 units Energy consumption Hybrid model shows that scaling undoubtedly can be improved however, trade-off between strong security and reasonably good operational performance could be an interesting solution for cloud systems. This ensure the proposed hybrid model is practical and effective in cloud environments.

IX. FUTURE WORK

The Hybrid Security Model will be the subject of more cloud research and performance testing in large-scale cloud systems while retaining a better level of energy economy. This will entail improving the energy efficiency of both blockchain and quantum cryptography as well as their ability to handle growing data and user counts. Moreover, post-quantum cryptography algorithms will be included to the model, which will also be altered. In order to ensure that a multi-organizational model can be presented at any time, more research will be conducted to model the mechanisms in multi-cloud settings and in IoT integration. Real-time testing using the ISOT CID dataset is intended to improve key management, data security, and intrusion detection system capabilities. Finally, the development of cloud security systems and tactics will be provided by improving real-time regulation and modification systems for improved optimization tools.

REFERENCES

[1] Vaishnav, A., & Bairagee, P. (2020). Computer System: A Reliable Machine. Reliability: Theory & Applications, 15(2), 17-20.
[2] Y. Baseri, V. Chouhan, and A. Ghorbani, "Cybersecurity in the Quantum Era: Assessing the Impact of Quantum Computing on Infrastructure," 2024.
[3] Shaktawat, R., Shaktawat, R. S., Lakshmi, N., Panwar, A., & Vaishnav, A. (2020). A hybrid technique of combining AES algorithm with block permutation for image encryption. Reliability: Theory & Applications, 15(1), 51-56.
[4] A. Rahman, M. Jahidul Islam, R. Islam, A. Aziz et al., "Enhancing Data Security for Cloud Computing Applications through Distributed Blockchain-based SDN Architecture in IoT Networks," 2022.
[5] S. Sarker, A. Kumar Saha, and M. Sadek Ferdous, "A Survey on Blockchain & Cloud Integration," 2020.
[6] P. Patil, P. Tulsiani, and D. Sunil Mane, "Mitigating Data Sharing in Public Cloud using Blockchain," 2024.
[7] W. Cui, T. Dou, and S. Yan, "Threats and Opportunities: Blockchain Meets Quantum Computation," 2020.
[8] D. Gurung, S. Raj Pokhrel, and G. Li, "Performance Analysis and Evaluation of Post Quantum Secure Blockchained Federated Learning," 2023.
[9] M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," 2018.
[10] G. Alagic, A. Broadbent, B. Fefferman, T. Gagliardoni et al., "Computational Security of Quantum Encryption," 2016.
[11] K. Kaushik and A. Kumar, "Demystifying Quantum Blockchain for Healthcare," 2022.
[12] Reyazur Rashid Irshad, "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," International Journal of Science and Research (IJSR), vol. 13, no. 9, pp. 3222-3225, September 2024.
[13] D. Dhinakaran, D. Selvaraj, N. Dharini, S. Edwin Raja, C. Sakthi Lakshmi Priya, "Towards a Novel Privacy-Preserving Distributed Multiparty Data Outsourcing Scheme for Cloud Computing with Quantum Key Distribution," arXiv preprint arXiv:2407.18923, July 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY