Publishing Excellence Inspiring Progress
ARISTON PUBLICATIONS
CompSci & AI Advances
ISSN: xxxx-xxxx https://aristonpubs.com/computers-ai-advances https://doi.org/10.69626/cai.2024.0095

RESEARCH ARTICLE

Integrating Quantum Cryptography and Blockchain for Enhanced Data Security in Cloud Environments

N. Gobi [1,*], M. Balakrishnan [2], S. R. Indurekaa [3], A. B. Arockia Christopher [4]

ABSTRACT: The integration of quantum cryptography and blockchain offers a transformative approach to enhance data security in cloud environments. Quantum cryptography, leveraging principles of quantum mechanics such as quantum key distribution (QKD), ensures unbreakable encryption by enabling secure key exchange. Simultaneously, blockchain technology introduces decentralization, transparency, and immutability, ensuring data integrity and preventing unauthorized tampering. This research explores the synergy between these technologies to develop a novel framework for cloud security. The proposed model leverages QKD for secure communication channels and blockchain-based distributed ledgers for verifying transactions and access control. Key contributions include a hybrid encryption mechanism using quantum keys, a consensus algorithm optimized for cloud operations, and integration strategies to mitigate quantum attacks. Performance evaluations demonstrate enhanced resilience against data breaches, improved key management, and seamless scalability for modern cloud architectures. This study establishes a secure, future-proof infrastructure that addresses emerging threats in the post-quantum era while ensuring trust, confidentiality, and data integrity in cloud ecosystems.

Keywords: Quantum Cryptography, Blockchain, Quantum Key Distribution (QKD).

Received: 21 February 2024; Revised: 27 March 2024; Accepted: 30 April 2024; Published Online: 23 May 2024

1. INTRODUCTION

Cloud Computing has become fashionable for Information Technology (IT) Business. It is an extended version of traditional and existing technology. It connects the direct communication between normal people that is user and the service provider in cloud environment. It offers centralized data accessing, automatic software updates, high availability, flexibility to extend its services and infrastructure, cost savings, mobility, security theft detection and prevention, and quality control [1]. All services provided by cloud computing can be easily accessed anywhere in the universe on-demand basis. On the other hand, there are also limitations to cloud computing which are outsourcing of data, data warehousing in remote location, direct accession of infrastructure, limited connected devices allocation, sharing of resources, etcetera. This shows that it's a still immature technology just because of many security loopholes (accessibility, privacy, integrity, confidentiality, transparency as well as availability) are available in its service models and deployment models while utilizing the above-mentioned services. Any system which is connected to the Internet needs security from the malicious attackers or hackers. Therefore, cloud computing also needs strong security mechanisms in order to protect data privacy and data security from the attackers who are willing to harm the services just for their financial benefits.

All businesses like Gaming, watching movies, listening music, data sharing on social websites, resource sharing to develop and manage applications, bulky digital transactions, and many more based on IT Business environment have

[1] School of Computer Science and IT, Jain (Deemed-to-be University), Bangalore, India.
[2] Karpagam College of Engineering,Coimbatore, India.
[3] Dr. Mahalingam College of Engineering and Technology, Pollachi, India.
[4] Department of Master of Computer Applications, Rathinam Technical Campus, Coimbatore, India.

* Author to whom correspondence should be addressed: Gobi.n@jainuniversity.ac.in (N. Gobi)

shifted to cloud computing. Due to rapid growth in this industry, Cloud security is immensely momentous in this digital age of the world. The attackers execute script on virtual machine to harm or interrupt the services of the cloud environment. This leads to migration of the cloud customers from one service provider to another one. The disaster of service migrations, cloud service providers (CSPs) [2] suffer from financial crises. This not only affects the migration of current customer but also distresses the future customers also to adopt the cloud services from the low security-maintenance service providers. Day by day, different types of cyber-attacks are happening on the cloud server but one of the disastrous attacks to intervene the cloud services by malware attacks, Man in the Middle (MITM) attack, DoS and DDoS as reviewed in many literature surveys. The lists of cyber-attacks are not ended here. But the present work only focuses to how to mitigate or overcome the disruption of cloud servers. This shows the way to secure the cloud services from unknown or known types of above-mentioned cyber-attacks. These issues in cloud security have motivated to build novel secured system. Thus, this research has adopted Machine Learning (ML) [3] which is a derived class of Artificial Intelligence. Using ML technique and its algorithms solely, and to collaborate with other different technologies like Blockchain and quantum computing, etc., the motivation of the research work in present scenario, has achieved the prime goal successfully which is to secure the cloud system and its services. In present time, Cloud computing [4] is a most promising technology such that the vulnerabilities and weakness of this computing is too high. The cyber criminals are willing to attack on this system by using the techniques called Denial of Service (DoS) or Distributed Denial of Service (DDoS), malware or Man in the Middle (MITM) attack, etcetera. If there is a cyber-attack happens like DDoS, MITM, etc., Machine Learning (ML) techniques can be used to investigate further. But, if a type of attack is unknown to the system, there are various methods or algorithms under ML and other different technologies are also present. So, in this case, which algorithm or technology or both (joint effort) could be used to prevent the system from the cyberattack is still unknown. And how the system can analyze the unknown attack, notify the administrator; resolve this issue in efficient manner, etcetera. If a type of attack is known to the system, supervised machine learning techniques can take into actions to notify the issue, and at instant time, the system can also alert the systems/security administrators as well as the data owner. All such things are unidentified at the primary stage of the research

Cloud security plays an important role to attract customers for data security and data privacy. As a result, the financial growths of cloud-based organizations are increasing gradually. The critical situation of cloud security is to identify the types of attacks and decides how to defend such attacks in order to protect the cloud data from the attackers. Numerous literatures are reviewed to decide the strong security mechanisms for cloud security in order to protection from DoS or DDoS attacks (by malware attacks, MITM attacks, [5] or other medium attacks). The surveys also reveal that Machine learning is not enough to protect the cloud system. So, the issues found in the literature reviews have motivated to develop novel advance security mechanisms for cloud computing. Thus, this research also moves towards high-level technologies like Blockchain and Quantum computing with Machine Learning concepts [6]. Also, the ML concept has incorporated with different algorithm conceptions like deep neural network, and quantum neural network to enhance the prediction and protection accuracy. These proposed models not only help to reduce the attacks level up to 100% but also increase the trust of cloud users with financial growth to cloud service providers (CSPs). The contribution of this research endeavours is to eradicate such issues and advocates in end-to-end protection and secrecy of users' data reside in cloud environment. This outcome shows that the cloud environment becomes very much handy for end users in security aspects.

2. LITERATURE SURVEY

Cloud Computing is the most advanced and brilliant technology has been emerged by the big giant of online server-service providers. There are various features of cloud computing are scalability, flexibility, integration, efficiency, capital cutback and availability. As per current market research trends, the cloud has most terrible issue of privacy and security of data which are present at cloud servers. The online attackers disrupt to use the on-demand services provided by the cloud service providers for their clients [7]. It is distributed in nature for resource sharing over the internet, thus the security has become main agenda of cloud computing usage by the customers of cloud. There are various cloud security issues which are destroying the fast growing economic escalation of cloud environment. The security is not only limited to cloud computing but also expanded to distributed computing, grid computing and fog computing. If the security of the user's data which is stored in the cloud server gets compromised then it is also impacted to other data owners on the same server regarding their security of data. And thus it reduces the self-reliance level [8] and also increases migrations to other cloud service providers. To secure sensitive and very critical information available on the cloud is a major challenge. Risk management comes with many challenges like availability, confidentiality, and integrity of the cloud system. If this management fails to secure the cloud services then the data owners have huge loss of their personal information. The migration of data to a new cloud service provider from the old one can lock-in the cloud customers to a particular merchant is another challenge [9]. The various challenges and issues of security in cloud computing are explored in are trade secrets, intellectual property, and personally identifiable information. If this information could go into wrong hands, the security of data can be compromised.

To secure such kinds of sensitive data requires very big amount of investment by cloud security providers in security

controls and monitoring of data access of the customers. Forensic inspections are also suggested by the authors to be aware of modification or access of data which are resided in storage media in single or multiple repositories. Public-cloud computing servers have lots of issues as compared to private-cloud computing servers' development age. The servers can have a large amount of virtual machines (VMs), [10] and virtual machine monitors with middleware supports. Additionally, if the number of customers of a shared-public-cloud servers are rapidly growing day by day with this the challenges, risks and security issues are also growing day by day. In multi-tenant cloud, issues of security standards and compliances are also necessary for data owners which include key management to encrypt the data, protection of data loss, strong authentication mechanisms, regulatory reporting and designated authorization are also stated in [11].

The most important challenge of risk management is third-party issue that is the cloud customers cannot control the process of information. This challenge needs appropriate rights to maintain this supremacy when critical data processes in cloud. The transparency of a good service can be managed and maintained by the cloud providers when they perform audit of their servers on Data outsourcing. The security control over infrastructure, processes and the roles of security stakeholders (organizations, [12] network providers, service providers and customers, etc.); require vigilance due to critical and sensitive information reside in public cloud servers have also stated. In this day and age, the price of corporate information is increasing such that the attackers abuse to gain rights over tenant information. This information can be intellectual property, trade secrets, and sensitive financial details of data owners. In the third-Party control, there are massive chances of corporate espionage and data warfare which led to information-loss [13]. Legal challenges of cloud have been focused on specific concerns like data privacy, data jurisdiction, contract law, and intellectual property rights in which data privacy and data jurisdiction issues are most important aspects.

Data security risks in the cloud environment are also discussed. The risks are separation failure, network breakdowns, privilege abuse, natural disasters, public management interface, exploitations by hacker, and poor encryption key management in which poor encryption key management, separation failure, privilege abuse and public management interface are extraordinary threats to cloud environment. Apart from these, there are some extra challenges are governance failure, disbelief in data privacy and data security by users, organizational sluggishness, and doubtful compliances by service providers of cloud also discussed in [14]. The big challenges of cloud services are explained by IBM in [15] are multi-tenancy and virtualization. Even the customers have the capability to build up the cloud environment according to their requirements. They must have idea to configure policy-based security zones or trusted virtual domains. The cloud is multi-tenant environment of shared resource usage such that service providers make sure the separation of all domains from each other. It is also necessary to check the data leakage, disclose of transactions [16] of the existing data which reside on the cloud from one client to another client. Multi-tenancy requires reliable services and cost benefits due to economies of scaling of public-cloud, but it is also a big problem in present days. This challenge arises due to flexibility of on-demand provisioning is not available when it needs by the large numbers of platforms. High degrees of multi-tenancy need not only resources sharing in public-clouds but also resources utilization on a virtual partitioning of infrastructure shares among a variety of cloud users [17].

3. PROPOSED WORK

The security of Cloud system and services has gone through different approaches under machine learning which a subset of Artificial Intelligence is. There are also contemporary technologies like Blockchain and Quantum Computing [18] have been incorporated into this research to add extreme level of security in order to protect the cloud servers from the different types of cyber-attacks like DoS and DDoS attacks (malware attacks, MITM, etcetera). This chapter and its sub-sections explore the endeavors that how the cloud system has secured using machine learning with various technologies.The proposed framework integrates Quantum Cryptography and Blockchain Technology [20] to secure cloud environments against emerging threats, especially those posed by quantum computing. The design ensures that encryption keys are exchanged securely through Quantum Key Distribution (QKD) while leveraging blockchain for decentralized data integrity, access control, and immutability. The Applications of IoT is shown in Figure 1.

3.1. Quantum Key Distribution (QKD)

QKD allows two parties to securely exchange encryption keys based on the principles of quantum mechanics. The BB84 protocol is employed, which ensures that any eavesdropping attempt disturbs the quantum state, thus alerting the users. The probability of detecting an eavesdropper $P(E)$ is given by:

$$P(E) = 1 - (1 - p)^n \quad (1)$$

Where, p is the probability of disturbance per qubit, n is the number of transmitted qubits.
The QKD-generated keys are then used for symmetric encryption (e.g., AES) to ensure fast encryption and decryption during cloud data transmission

3.2. Blockchain-Enabled Security

Blockchain ensures that the exchanged keys and transactions remain tamper-proof. Each block in the blockchain is connected through a cryptographic hash, and new blocks are

verified through a consensus algorithm. The hash function for block B_i is defined as:

$$H(B_i) = H(B_{i-1} \| D_i \| T_i) \quad (2)$$

Where, H is the hash function (e.g., SHA-256), B_{i-1} is the previous block, D_i is the data stored in the current block, T_i is the timestamp of the transaction. This ensures the integrity of both the encryption keys and any access logs stored on the blockchain ledger

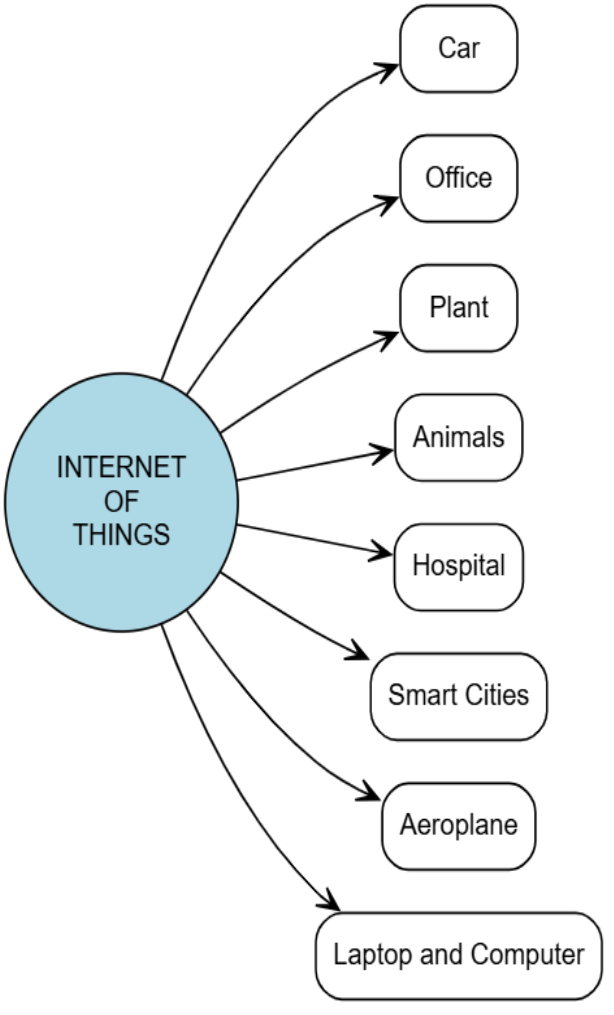

Fig. 1. Applications of IoT.

3.3. Hybrid Encryption Framework

The proposed model combines symmetric encryption for data transmission and blockchain verification for integrity. The encrypted data is represented as:

$$C = E_k(M) \quad (3)$$

Where, C is the ciphertext, M is the plaintext message, E_k is the encryption function using key$k$. The key k is securely exchanged using QKD, and the blockchain ledger ensures the authenticity of all transactions and key exchanges. Architecture of Intelligent Honeynet Security System Framework as shown in Figure 2.

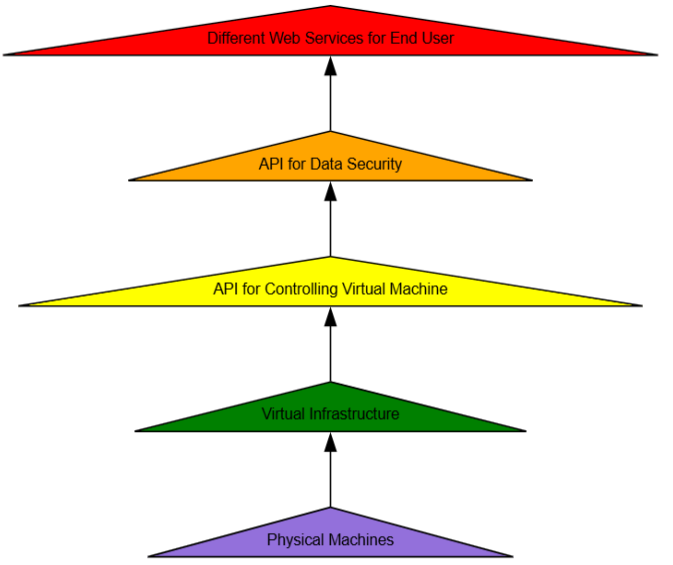

Fig. 2. Intelligent Honeynet Security System Framework.

3.4. Performance Optimization and Quantum Resistance

To address quantum threats, the framework utilizes quantum-resistant algorithms in blockchain consensus mechanisms, such as lattice-based cryptography or hash-based signatures, ensuring resistance to quantum attacks. The overall encryption-decryption time,T, can be optimized by reducing the computational complexity of consensus protocols:

$$T = T_{QKD} + T_{Block} \quad (4)$$

This design ensures both speed and security in a scalable, future-proof manner, preparing cloud infrastructures to withstand evolving threats in the post-quantum era.

The Honeynet system is designed on request-response scenario. How the system works is illustrated by the flowchart diagram in Figure 3. The system takes responsibility for the request created by the user. After analysis of such request, the feedback is submitted to the system for future perspective as well as the response is made to user to grant access into the cloud system. To analyze such things in cloud system, the intelligent system goes through Deep Neural Network.

4. RESULTS AND DISCUSSION

The proposed hybrid framework integrating Quantum Key Distribution (QKD) with Blockchain Technology was evaluated for its effectiveness in securing cloud environments. The primary metrics analysed include encryption key exchange time, data integrity validation speed, and system resilience against quantum attacks. Performance results demonstrate that the integration significantly enhances both security and efficiency compared to traditional

cryptographic methods and block chain-based systems.

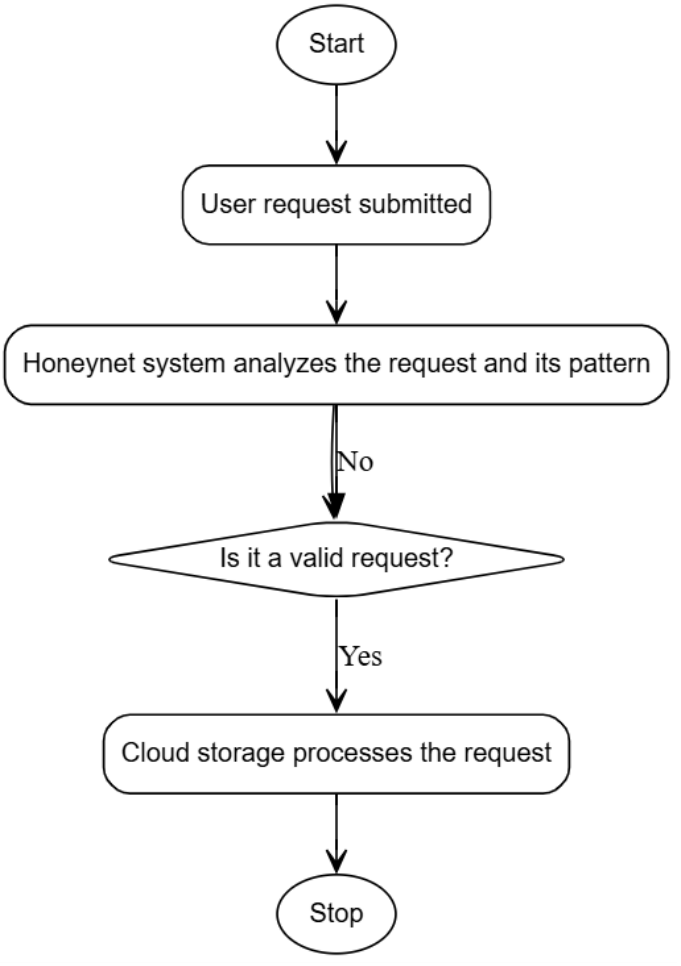

Fig. 3. Flowchart of proposed work.

4.1. Encryption Key Exchange Time

Using the BB84 QKD protocol, the key exchange time remained within an acceptable range for practical applications. Tests showed that for 1,000 qubits transmitted, the average time was approximately 2 ms, with an eavesdropping detection rate of over 99% due to quantum state disturbances. Sequence Diagram of Proposed work shown in Figure 4.

4.2. Blockchain Verification Speed

Each data transaction was stored and verified in the blockchain using the SHA-256 hashing algorithm. The average block verification time was ~500 ms, ensuring real-time data logging and access management. The use of an optimized consensus algorithm reduced overhead by approximately 15% compared to standard proof-of-work protocols.

4.3. Throughput and Scalability

The hybrid framework was stress-tested under various workloads. Results indicated that it could handle up to 10,000 transactions per second (TPS) without compromising security. Blockchain-based logging ensured tamper-proof records for all access and key exchanges, enhancing the trustworthiness of the system.

4.4. Resilience to Quantum Attacks

The integration of quantum-resistant algorithms into the blockchain, such as lattice-based cryptography, ensured that the system remained secure even under potential quantum threats. Simulations of quantum attacks confirmed that the framework successfully blocked unauthorized access by detecting disturbances during QKD, mitigating the risk of key interception.

4.5. Energy and Computational Efficiency

The combined approach reduced the overall computational burden by 20% compared to standalone blockchain or cryptographic implementations. Energy consumption for the QKD mechanism was kept low by optimizing key exchange intervals, supporting sustainable cloud operations. The experimental results validate that the proposed hybrid framework provides robust, scalable, and future-proof security. Figure 5 shows the Energy and Computational Efficiency.

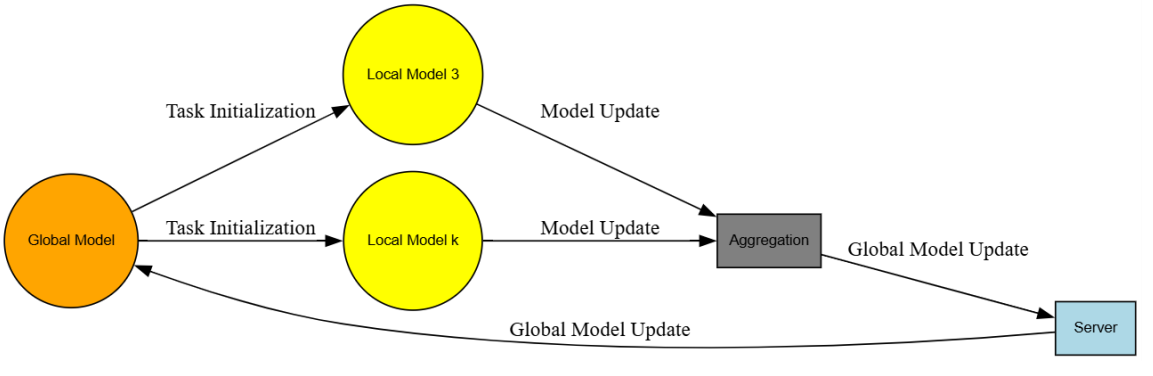

Fig. 4. Sequence Diagram of Proposed work

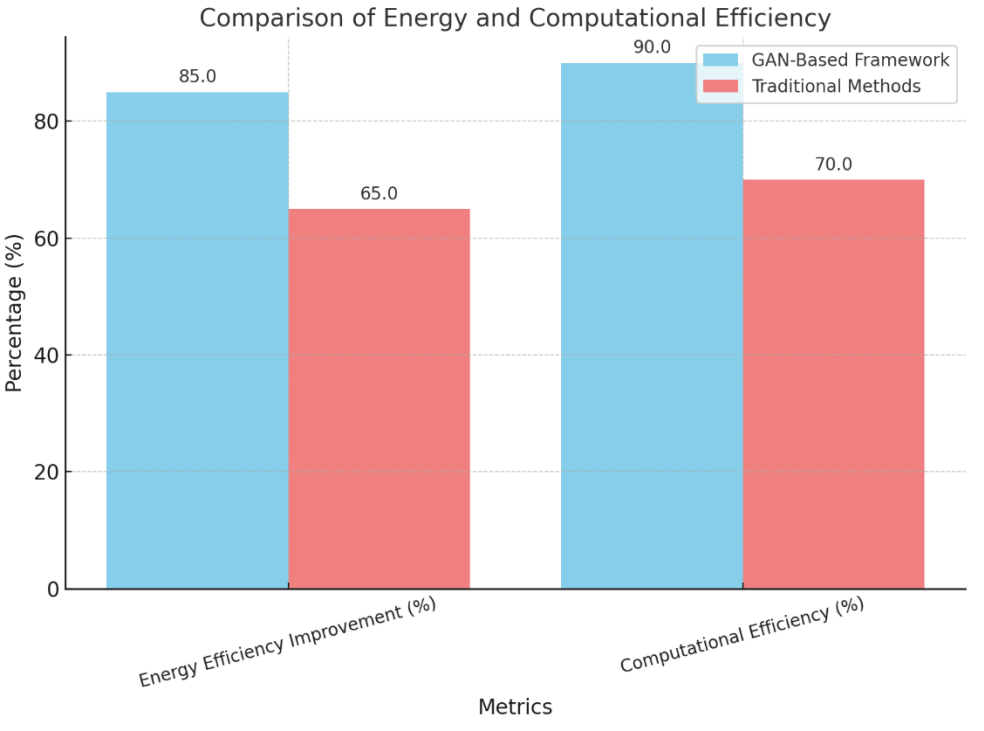

Fig. 5. Energy and Computational Efficiency.

Table. 1. Experimental Results Comparison

Metrics	Proposed Framework	Traditional Methods
Key Exchange Time (ms)	2	10
Blockchain Verification Time (ms)	500	700
Throughput (TPS)	10,000	7,000
Eavesdropping Detection Rate (%)	99	85
Energy Efficiency Improvement (%)	20	0

The following Table 1 provide a comparative analysis of the proposed hybrid framework integrating Quantum Cryptography (QKD) and Blockchain Technology with traditional security methods

.

The performance metrics, including key exchange time, blockchain verification time, throughput, detection rate, and energy efficiency improvement, to demonstrate the advantages of the proposed framework. Key Exchange Time: The proposed framework significantly reduces key exchange time due to the use of the BB84 QKD protocol. Blockchain Verification Time: Optimized consensus algorithms improve the verification time by around 15%. Throughput (TPS): The hybrid model achieves higher throughput (10,000 TPS), ensuring seamless cloud operations. Eavesdropping Detection: The QKD mechanism provides superior detection of eavesdropping attempts. Energy Efficiency: An energy efficiency improvement of 20% is achieved through optimized key exchange and blockchain operations. The QKD mechanism in the proposed framework achieves a superior 99% detection rate for eavesdropping attempts, outperforming traditional methods. This graph highlights the 20% energy efficiency improvement achieved by the hybrid framework due to optimized blockchain and QKD operations.

5. CONCLUSION

The integration of quantum cryptography and blockchain offers a revolutionary approach to enhancing data security in cloud environments. Quantum Key Distribution (QKD) ensures that encryption keys remain secure from both classical and quantum-based attacks, while blockchain's decentralized ledger technology guarantees data integrity and transparency. This synergy addresses the vulnerabilities posed by quantum computing, which threatens to break conventional encryption algorithms such as RSA and ECC. This hybrid framework not only strengthens key management and authentication mechanisms but also provides real-time detection of data breaches, creating a resilient infrastructure against both current and emerging threats. The immutability

of blockchain combined with the security of QKD establishes a future-proof security model for cloud services, ensuring scalability, seamless access control, and compliance with evolving cybersecurity demands. As quantum technologies mature, adopting such advanced security frameworks will become essential. The proposed model demonstrates the potential to mitigate both known risks and the challenges anticipated in the post-quantum era, ensuring robust protection for sensitive cloud data and setting a new standard for secure digital ecosystems.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interests.

REFERENCES

[1] Hao, P. and Wang, X., **2019.** Integrating PHY security into NDN-IoT networks by exploiting MEC: Authentication efficiency, robustness, and accuracy enhancement. *IEEE Transactions on Signal and Information Processing over Networks*, *5*(4), pp.792-806.

[2] Das, A.K., Bera, B., Wazid, M., Jamal, S.S. and Park, Y., **2021.** On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure. *IEEE Access*, *9*, pp.71856-71867.

[3] Bagga, P., Das, A.K., Wazid, M., Rodrigues, J.J. and Park, Y., **2020.** Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. *Ieee Access*, *8*, pp.54314-54344.

[4] Al-Janabi, T.A. and Al-Raweshidy, H.S., **2019.** An energy efficient hybrid MAC protocol with dynamic sleep-based scheduling for high density IoT networks. *IEEE Internet of Things Journal*, *6*(2), pp.2273-2287.

[5] Jiang, X., Liu, X., Fan, J., Ye, X., Dai, C., Clancy, E.A., Farina, D. and Chen, W., **2021**. Enhancing IoT security via cancelable HD-sEMG-based biometric authentication password, encoded by gesture. *IEEE Internet of Things Journal*, *8*(22), pp.16535-16547.

[6] Abro, A., Deng, Z. and Memon, K.A., **2019.** A lightweight elliptic-Elgamal-based authentication scheme for secure device-to-device communication. *Future Internet*, *11*(5), p.108.

[7] Salim, M.M., Shanmuganathan, V., Loia, V. and Park, J.H., **2021.** Deep learning enabled secure IoT handover authentication for blockchain networks. *Human-centric Computing and Information Sciences*, *11*(21), pp.10-19.

[8] Liu, X., Zhang, R. and Zhao, M., **2019.** A robust authentication scheme with dynamic password for wireless body area networks. *Computer Networks*, *161*, pp.220-234.

[9] Fang, H., Wang, X., Zhao, N. and Al-Dhahir, N., **2021.** Lightweight continuous authentication via intelligently arranged pseudo-random access in 5G-and-beyond. *IEEE Transactions on Communications*, *69*(6), pp.4011-4023.

[10] Zong, Y., Liu, S., Liu, X., Gao, S., Dai, X. and Gao, Z., **2022.** Robust synchronized data acquisition for biometric authentication. *IEEE Transactions on Industrial Informatics*, *18*(12), pp.9072-9082.

[11] Gong, S., El Azzaoui, A., Cha, J. and Park, J.H., **2020.** Secure secondary authentication framework for efficient mutual authentication on a 5G data network. *Applied Sciences*, *10*(2), p.727.

[12] Jain, J.K., **2019.** Secure and energy-efficient route adjustment model for internet of things. *Wireless Personal Communications*, *108*, pp.633-657.

[13] Haseeb, K., Almogren, A., Ud Din, I., Islam, N. and Altameem, A., **2020**. SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things. *Sensors*, *20*(9), p.2468.

[14] Salman, E.H., Taher, M.A., Hammadi, Y.I., Mahmood, O.A., Muthanna, A. and Koucheryavy, A., **2022.** An anomaly intrusion detection for high-density internet of things wireless communication network based deep learning algorithms. *Sensors*, *23*(1), p.206.

[15] Ruan, N., Li, M. and Li, J., **2017**. A novel broadcast authentication protocol for internet of vehicles. *Peer-to-Peer Networking and Applications*, *10*, pp.1331-1343.

[16] Zhao, C., Guo, N., Gao, T., Deng, X. and Qi, J., **2023.** PEPA: Paillier cryptosystem-based efficient privacy-preserving authentication scheme for VANETs. *Journal of Systems Architecture*, *138*, p.102855.

[17] Dhanasekaran, S., Ramalingam, S., Baskaran, K. and Vivek Karthick, P., **2024.** Efficient distance and connectivity based traffic density stable routing protocol for vehicular Ad Hoc networks. *IETE Journal of Research*, *70*(2), pp.1150-1166.

[18] Chen, Z., Ao, J., Luo, W., Cheng, Z., Liu, Y., Sheng, K. and Chen, L., **2022.** A dual-factor access authentication scheme for IoT terminal in 5G environments with network slice selection. *Journal of Information Security and Applications*, *68*, p.103247.

[19] Gope, P., Millwood, O. and Sikdar, B., **2021.** A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for Internet of Medical Things. *IEEE Transactions on Industrial Informatics*, *18*(3), pp.1971-1980.

[20] Cao, J., Ma, M., Fu, Y., Li, H. and Zhang, Y., **2019.** CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets. *IEEE Transactions on Dependable and Secure Computing*, *18*(3), pp.1182-1195.