Securing Data Privacy and Integrity in Cloud Computing Using Blockchain and Quantum Cryptography

Neethu V A[1], Mohammad Akram Khan[2]

[1]*Research Scholar, Department of Computer Science Engineering & Technology, Madhav University, India, arunchandranneethu@gmail.com*
[2]*Doctor, Assistant Professor, Department of Computer Science and Application, Faculty of Engineering & Technology, Madhav University, India, staryan23@gmail.com*

Abstract: Data privacy and integrity maintenance becomes more difficult as cloud computing expands. Such complex and advanced cyberattacks need for stronger and better defenses than traditional security measures can offer. A research paper that combines blockchain technology with quantum cryptography to improve data security in the cloud paradigm. In addition, aspects of blockchain itself – its distributed and cryptographically verified ledger – offer the possibility of transparency and immutability of the life of the data. Excited by that? Unlike this, Quantum Cryptography applies the concepts of quantum mechanical physics in the form of quantum key distribution (QKD) which theoretically allows secure communication that is resistant to computational attacks (and even those executed on quantum computers). This paper proposes a cloud hybrid security framework that combines these two pathbreaking technologies to provide an end-to-end data security mechanism in cloud computing. This framework deploys the construction of smart contracts of Blockchain to automate the enforcement of such security policies while using Quantum cryptography's unbreakable encryption to enable the secure transmission of valuable data and information. Moreover, This study also covers practical usage, performance evaluation, and integration challenges of integrating Blockchain/Quantum Cryptography with cloud infrastructures.It has been established through the comparative analysis of existing security models that this hybrid approach offers improved mitigation towards the cyber threats ranging from data breaches, unauthorized access, and man-in-the-middle attacks. The experimental results demonstrate that integrating Blockchain and Quantum Cryptography can significantly enhance cloud data privacy, integrity, and trustworthiness. With this advancement, quantum-secured cloud-computing environments will be built to guard their data with a security measure that offers a strong, future-proofed level of security and prevents quantum-based threats that may arise in the future.

Keywords: Data Privacy, Data Integrity, Cloud Computing, Blockchain Technology, Quantum Bit Error Rate (QBER), Quantum Key Distribution(QKD).

1. Introduction

In today `s cloud computing in a world that is revolutionizing the way we handle, store and process data, strong security measures have never been more important. Cloud platforms have become the go-to for many businesses and individuals, thanks to their scalability and flexibility, leading to a giant store of sensitive data. Consequently, cloud infrastructures are becoming more vulnerable to unauthorized access, data breaches, and cyberattacks. Data integrity and privacy represent major challenges, while modern cloud infrastructural complexities frequently make traditional security mechanisms inadequate.

While quantum cryptography and blockchain technology have been put forward as potential solutions to these security issues. Blockchain is a distributed and decentralized ledger that guarantees the transparency and unchangeability of data when it has been recorded, significantly minimizing the chance of unauthorized data modifications or alterations. As all transactions of this technology are public and the transaction is auditable, hence, it is becoming troublesome for the attackers to alter the data or replicate it. Using blockchain technology will be a life jacket that will protect and validate the facts that stored in the cloud platform as the number of data breaches in the cloud environment continues to grow. By employing cloud computing and blockchain technology in IoT, the authors in [1] introduced SH-BlockCC, a successful, enhanced and secure smart home architecture. Through the employment of blockchain, this architecture facilitates secure data storage and transaction processing, thereby improving security and efficiency in IoT-enabled smart homes. [2] 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. In the whitepaper published in 2008,[3] debuted bitcoin, the peer-to-peer electronic cash computer system that allows coin transfers between users directly through the internet without going through a financial institution.

Quantum cryptography offers a new level of communications security based on the laws of quantum mechanics, enabling the construction of encryption systems that can be proven to be impervious to attacks by classical computers and quantum computers alike. For instance, quantum states can be used in QKD to allow encryption keys to be securely transmitted between parties, making it an unbreakable encryption method. As the capabilities of quantum computers continue to advance, traditional methods of encryption may become vulnerable, making quantum cryptography an essential tool for safeguarding data into the future. This paper aims to report suitable integration of Blockchain Technology with Quantum Cryptography to enhance data privacy and integrity of cloud computing through Quantum Cryptography integration. Our aim is to produce a comprehensive security architecture, based on a combination of these technologies, that maintains the security, authenticity and integrity of the data without taking away the scalability and flexibility cloud platforms offer. Such a creative approach may lay the foundation for a cloud-computing ecosystem that is much more resilient and secure in the future.

2. Literature review:

The increase in use of cloud computing for data processing and storage has raised critical concerns over data privacy, integrity and security. Traditional information security techniques, such as traditional encryption and access control mechanisms, are increasingly becoming ineffective to the evolving nature of cyber threats originating from the vast amount of sensitive data replicated and stored over disparate cloud systems. As cloud computing continues to take hold on a variety of organizations, the need for security and integrity of data in the cloud is paramount to maintaining user trust and meeting legal obligations [4].

Blockchain technology is proving to be a viable option to enhance data security in cloud environments due to its immutable ledger and decentralized architecture. Block Chain enhances integrity and accountability by making record visible and verifiable as it tamper-proofs and distributes recording for each of the data transaction [5]. This feature allows cloud service providers to provide auditable logs of all data actions, making it extremely difficult for malicious actors to alter or modify stored data unnoticed [6]. In addition, blockchain functions as a secure method for sharing data between more than one party without the need and risks of a central authority, effectively reducing the risk of data breaches and enhancing privacy. Quantum Cryptography , especially QKD, offers a level of encryption that is expected to secure data transmission even against potential attacks made by quantum computing in the future. Quantum Cryptography uses the laws of quantum mechanics to create encryption keys that are cryptographically unbreakable in theory [7]. This technology ensures that every attempt to intercept a communication channel changes the quantum states without being able to prevent it [8] and warns sender and recipient about the security breach. Quantum cryptography may also be the key enabling technology to secure sensitive data in cloud infrastructures as quantum computers develop [9].In addition, the decentralized nature of blockchain ensures the integrity of data, and quantum cryptography enables unbreakable encryption, supplying a solid means of protection against cyberattacks in cloud computing environments [10]. A hybrid approach where collaborative computing and cloud computing are combined will deliver high security, privacy, and trustworthiness [11] . To fulfill this purpose, the

paper intends to introduce a novel architecture for safeguarding data in the cloud. [12] 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. [13] investigated the convergence between blockchain and edge computing to improve the security, scalability, and reliability of operators and services for IIoT critical infrastructures in Industry 4.0. [14] 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. [15] 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.

3. Methodology:

Blockchain and Quantum Cryptography Integration to Cloud Systems: A New Approach to the Security Data Privacy and Integrity Challenges in the Era of Quantum Computing Quantum attacks can break classical encryption techniques like RSA, AES, and Diffie-Hellman (DH), making traditional cloud security ineffective. We propose in this paper a strong post-quantum secure model for cloud systems based on the union between Blockchain and Quantum Cryptography.

Weaknesses of Classical Cryptography

Cloud security mechanisms are mainly based on classical cryptographic algorithms (e.g., RSA, AES, Diffie-Hellman (DH)). RS encryption, for example, is predicated on the difficulty of factoring the integer. While this is safe from traditional attacks, quantum computing algorithms, such as Shor's algorithm, are capable of factoring large integers in polynomial time, making them feasible in the time of quantum computing. As a result, RSA and similar encryption schemes are vulnerable to quantum computers, where the chances of an attack become very high, leaving these classical techniques powerless against quantum machines.

QKD for Secure Key Exchange

The weakness of the conventional key exchange systems as the usage of QKD, in particular the BB84 protocol, is circumvented by our proposed method. QKD: Provides secure key exchange using quantum physics Eavesdropping would be obvious because the laws of quantum mechanics ensure that any hacker who intercepts and measures the quantum states in the communication channel will induce detectable imperfections in the system. To detect the presence of Eve, Alice and Bob use the error rate in the BB84 protocol to share a secure key. Yet with a QKD you achieve a quantum attack-resistant method that comes with a proof of security and which classical key exchange methods can easily fall prey to new quantum decryption algorithms.

Data Integrity Blockchain

The system implements Blockchain technology to ensure data integrity, in addition to safeguarding the key exchange procedure. Classic cloud systems store data in a centralized database that can be tampered with. Instead, given its decentralized, immutable ledger for storing data, with blockchain, any change or tampering of stored information can be easily identified. The Blockchain is a distributed database, where its chain of blocks is designed to be tamper-proof, as each block contains the cryptographic hash of the previous block. Since changing a single block prompts the re-computation of all successive blocks, it is computationally improbable, thus preserving the integrity of data stored in the cloud.

Post-Quantum Security Through QKD and Blockchain Combination

By combining the strengths of QKD for secure key exchange and Blockchain for tamper-proof data storage, the proposed solution offers a unique and powerful approach to addressing the vulnerabilities of traditional cloud systems. QKD also addresses the problem of quantum attacks on encryption keys, while Blockchain ensures data integrity by providing decentralized and immutable records. This combination of two technologies delivers security that is only possible if used with quantum technology that classical cryptography can't provide.

Overall attack likelihood and security improvements

The explained method is less susceptible to successful attack in comparison with traditional one. The attack probability in classical cryptography is proportional to $O(1/(\exp(n)))$ being the key size.

Whereas, the attack probability against QKD and Blockchain affects exponentially. This leaves a final probability of O(2^(-n)× 2^(-256))for successfully attacking the system, rendering the compromise of the system practically infeasible even in the face of quantum computers. QKD and Blockchain Integration for cloud systems QKD and Blockchain for cloud systems data privacy integrity and security. The solution proposed in this paper does not only grant post-quantum security by eliminating vulnerabilities in classical cryptographic systems but also guarantees tamper-proof data storage using Blockchain. The implications for cloud systems include a hybrid approach that brings together the best of traditional and quantum-resistant cryptographic techniques, resulting in an extremely secure, scalable option for systems in the post-quantum age while minimizing the threats from quantum computing and preserving sensitive data for the long term.

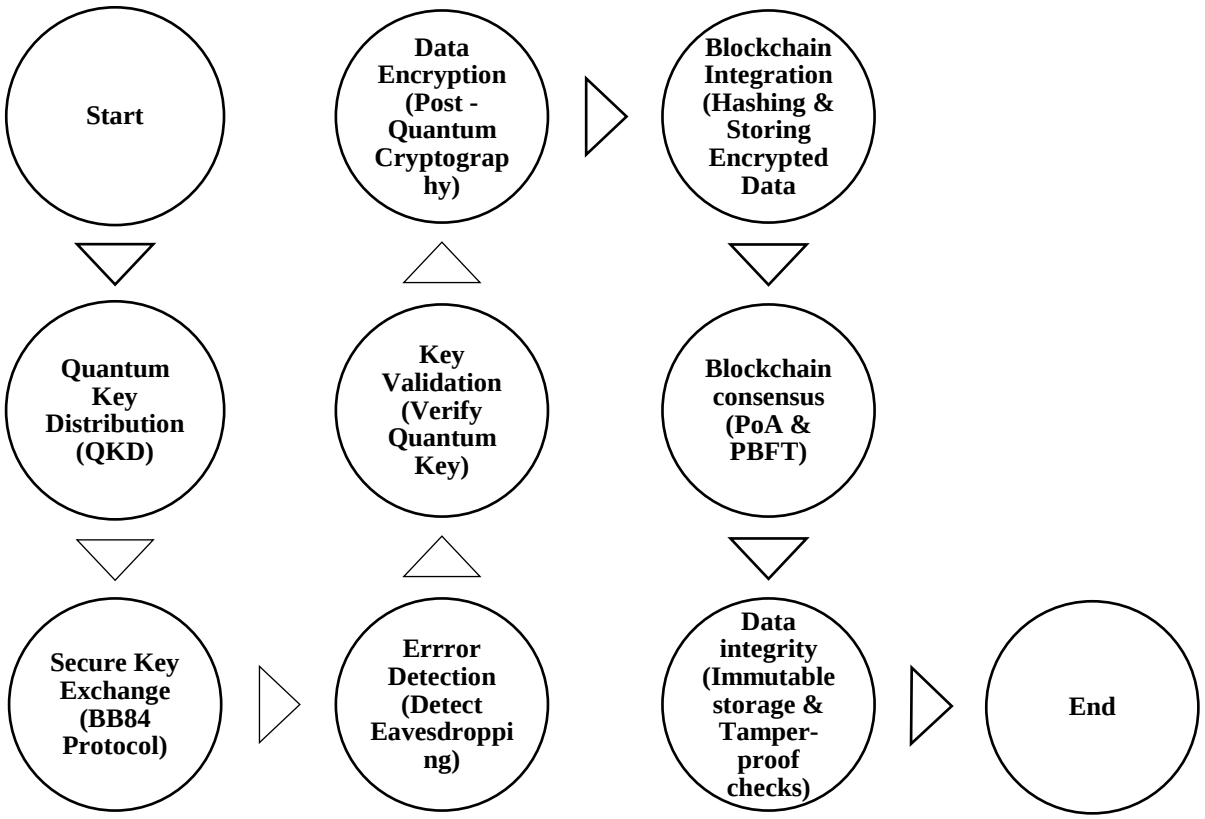

Figure 1: Flowchart of the Proposed Blockchain and Quantum Cryptography-based Secure Cloud Architecture

4. Algorithm Techniques:

QKD protocol based on BB84 utilizes specialized quantum properties as key to encryption, and its implementation comprises multiple methods for secure upload of keys from Alice (the sender) to Bob (the receiver). The exchange of keys is further refined through the use of classical communication protocols and error-correction techniques on top of the quantum mechanics of BB84. The following are the detailed explanation of the algorithm techniques in the BB84 QKD protocol:

4.1 Random Key Generation:

Alice-Key Generation: Alice generates a random string of bits (0s and 1s) to construct the raw key. For each bit, Alice

- randomly selects one of two possible measurement bases:
- Rectilinear basis ("+" or "0", "1"): Corresponds to binary values states 0 and 1.
- Diagonal Basis ("×" or "/"): States at 45° to the rectilinear basis.

Since Alice randomly chooses one of the two bases for each bit, she ends up with a random sequence of bits and their corresponding bases.

Bob's Measurement: Bob generates random bits and randomly selects a basis (rectilinear or diagonal) When qubits are sent from Alice, Bob uses his own basis to measure them. If the bases of Alice and

Bob match, Bob will correctly measure the bit. If the bases do not match, Bob's measurement will be random.

4.2 Eavesdropping (Optional):

- Interception of Eve: An adversary (or eavesdropper) could attempt to intercept and measure the qubits transmitted by Alice, provided eavesdropping is allowed. Eve selects a random basis for each intercepted qubit.
- If Eve's basis is the same as Alice's she will measure the qubit correctly.
- If Eve's basis differs from Alice's, she will measure the qubit incorrectly.
- Eve breaks the BB84 protocol by measuring your shared string and then sending her measures to Bob accurately which introduces errors in the final key.

4.3Noise Introduction:

- Real-world quantum communication is noisy (e.g., subject to photon loss or interference). In order to mimic this, we introduce a bit of noise (i.e., we flip Bob's key bits with some probability).
- Bit Flip Noises: This noise randomly flips bits with specific probability (also called noise_level in simulation). This causes errors in Bob's key.

4.4Key Sifting:

- After the qubits have been received, Bob and Alice share the bases they used for each qubit. By the same token, they retain the same corresponding bit in the key (called a sifted bit).
- If Alice and Bob have used different bases, the bit is discarded as it is not reliable.
- Sifted Key: Once the bases match, the rest of the bits are sifted out to produce the sifted key. These bits are the potential shared secret key between Alice and Bob.

4.5Calculating Quantum Bit Error Rate (QBER)

QBER Calculation:

- QBER, the Quantum Bit Error Rate, is the ratio of mismatched bits of Alice's key to Bob's sifted key. It is an important measure for indicating whether eavesdropping exists.
- QBER calculation: Alice and Bob can publicly compare one subset of their sifted key. Low QBER means the communication is secure, while high QBER means that the channel has been potentially interfered with by noise or eavesdropping.

$$\text{QBER} = \frac{\text{Total number of shifted bits}}{\text{Error rate in the shifted key}} \times 100 \text{ ---------(1)}$$

If the QBER exceeds a threshold (of about 11% in practice) it is a sign the transmission is dishonest and the key is discarded.

4.6Key Reconciliation and Error Correction

- Error Correction: When Alice and Bob detect a non-zero QBER they apply error-correction algorithms to correct the discrepancies of the sifted keys . These errors could be introduced by noise or by Eve's eavesdropping.
- Error Correction Common error-correction algorithms used in QKD include Low-Density Parity-Check (LDPC) codes and Reed-Solomon codes which provide mechanisms for Alice and Bob to correct errors and reconcile their keys.
- Classical Communication: Comparison of bases: Alice and Bob openly communicate their measurements (via a public classical channel) and use this information to determine whether they made the same measurement. This classical communication reveals no information about the key itself, and is used only to remove errors.
- Privacy Amplification: If Eve possesses partial information about the key (which can be estimated using the QBER and errors observed), Alice and Bob perform a privacy amplification step that will shrink the size of the key while ensuring that Eve has no significant information remaining (sifting key, hash function is privacy amplification) Alice and Bob then share the remaining shortened key.This makes sure that the final key is secure and not known to Eve.
- Key Efficiency: While the efficiency of the protocol is measured in key bits per raw bit, Key Efficiency is the fraction of bits that Alice and Bob share once they have sifted, corrected errors, and performed privacy amplification. We call such efficiency a measure how many bits end in the last key in the protocol steps. Which is a function of the level of noise, error rates, and the key length.So we can measure key efficiency as:

$$\text{Key Efficiency} = \frac{\text{Length of final key}}{\text{Initial Key Length}} \times 100 \text{---------(2)}$$

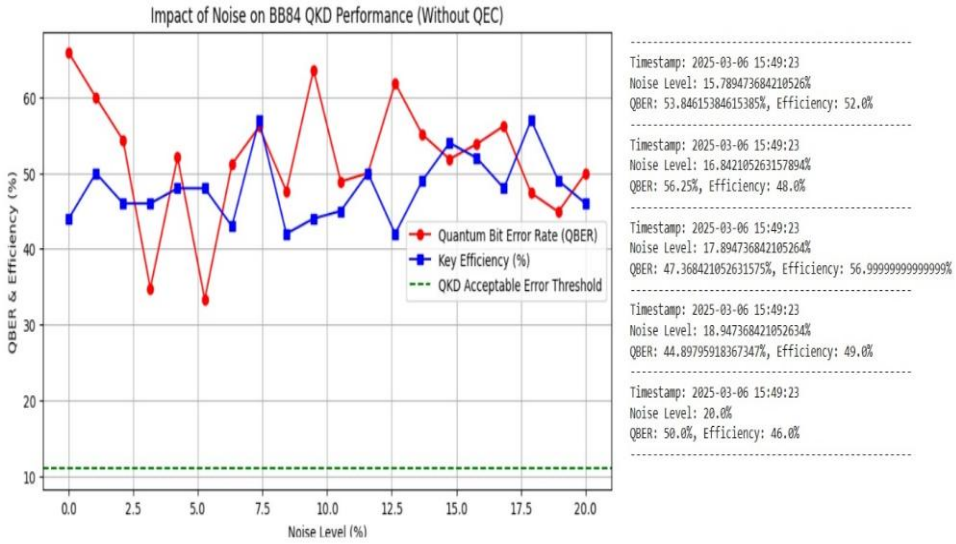

Figure 2: Impact of noise on BB84 QKD performance without QEC

Security of the Protocol:

Eavesdropping Detection: If Eve is the eavesdropper then she would create some errors in the key, and both Alice and Bob will be able to detect this so BB84 will be secure by default. By using the QBER, they can then calculate how much information would an Eavesdropper (Eve) gain. If the error rate is too large the key will be discarded.

No-Cloning Theorem: Quantum mechanics has the unique feature that information cannot be copied perfectly (as per no-cloning theorem). This makes it more difficult for Eve to intercept and copy Alice's qubits perfectly, adding another layer of security.

5. Result Analysis and Discussion:

This study evaluates the performance of the BB84 QKD protocol in the presence of noise, ranging from 0% to 20%, without using any error correction or mitigation techniques. It examines the two critical metrics: QBER, which measures the proportion of erroneous bits in the sifted key, and key efficiency, which indicates the percentage of Alice's original key that remains usable after base reconciliation. The simulation assesses how noise impacts the security and practicality of the protocol, providing insights into the effects of noise on quantum communication channels and the need for error correction methods in real-world scenarios.

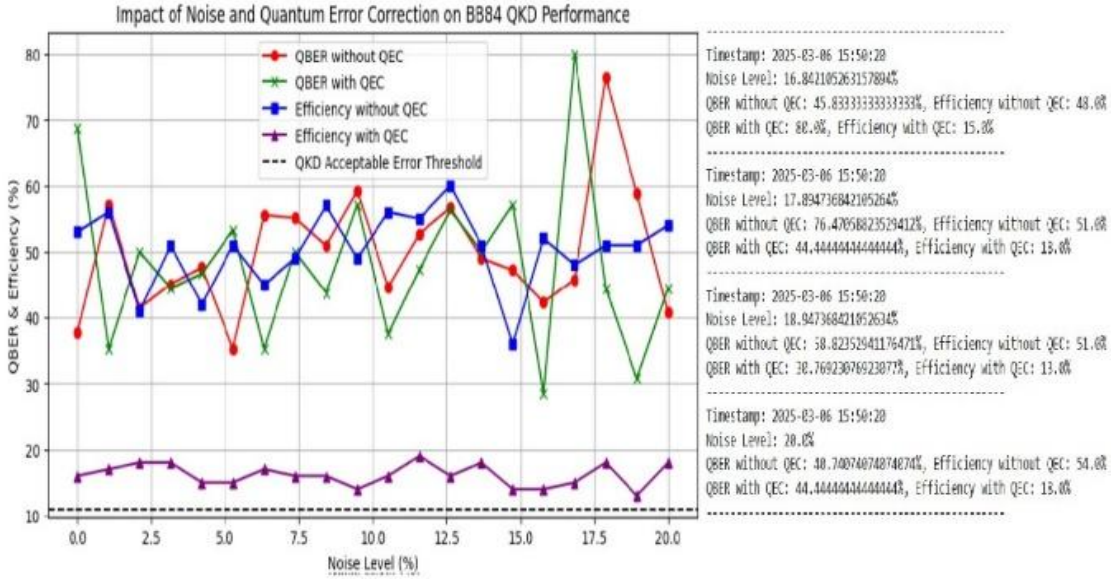

Figure 3: Impact of noise on BB84 QKD performance with QEC

Classical Cryptography Security Vulnerability

Traditional Cloud Security: Classical-based cryptographic techniques like RSA and AES The security strength of RSA encryption is based on integer factorization quotienting some adversary needs to solve:

N=p×q----------(3)

Where p and q are large prime numbers. The most-quoted classical factoring algorithm goes in sub-exponential time, whereas Shor's algorithm on a quantum computer can perform factoring in polynomial time O((〖log N〗)^3), thus breaking RSA in the presence of a quantum computer.

So, the likelihood of your RSA Protected Cloud system getting hacked is as follows:

P_(c)=O(1⁄(exp(n)))----------(4)

Where n is the key size. However, once you factor in quantum attacks, this probability gains the following exponent of sorts:

P_(q)=O(1)----------(5)

which means classical encryption is neither new nor secure against quantum threat.

Quantum Cryptography for Key Exchange

Apply QKD where keys used for encryption are generated and shared. BB84 protocol ensures eavesdropping will induce discrepancies in quantum pair.

Consider the quantum key sequence to be:

Q_k={q_1,q_2,.....q_n}, q_(i)∈ {0,1,+,-}

If an attacker observes the qubits by measuring them, that induces an error rate e:

e=(number of detected errors)/(total qubits exchanged)--------(6)

If e > e_threshold , the key exchange is terminated. Considering that in BB84 the error rate threshold is 11%, the probability of undetected interception is exponentially small:

P_(attack success)= O(2^(-n))----------(7)

which is orders of magnitude lower than classical cryptography security.

Therefore, our innovative mechanism employs QKD for key exchange to avoid classical key exchange vulnerabilities (e.g., Diffie-Hellman which is breakable by quantum algorithms).

Blockchain for Data Integrity

Adaptive classical cloud the stores the data in centralized databases, which exposes them to integrity attacks. In this, our method incorporates blockchain for verifiable status storage. single block in the blockchain holds:

B_i=(H(B_(i-1)),T_i,S_i ----------(8)

where:

H(B_(i-1)), is the hash of the previous block, creating a tamper-proof chain.

T_i is the transaction data.

S_i is the digital sign for authentication.

Finally, the new malicious block Hold that Sentinal, that malicious attempt to change a previous block must solve:

H(B_i^*)=H(B_(i-1)) Where B_i^*≠B_i----------(9)

The probability of finding a valid modification lies because of the collision resistance of cryptographic hash functions:

P_collision = O(1⁄2^b)----------(10)

For SHA-256,b=256, so:

P_collision = O(2^(-256) ----------(11)

The integration of data on the blockchain, preventing any future unauthorized modifications, is a novelty compared to traditional cloud security models, which depend on centralized integrity checks.

Combined Security Model: Blockchain + Quantum Cryptography

With the synthesis of QKD for secure key exchange and blockchain for integrity verification, our system manages post-quantum security and data immutability.

Let:

P_qbe the success probability of a quantum attack on the encryption.

P_h be the probability of deviating from blockchain integrity.

Since QKD removes classical crypto vulnerabilities:

P_q=O(2^(-n))----------(12)

And blockchain provides tamper-proof integrity:

〖P〗_(h)=O(2^(-256))----------(13)

Thus, the final probability of successfully attacking our system is:

P_final= P_q × P_h =O(2^(-n)×2^(-256)) ----------(14)

Assuming our level of encryption is n (e.g., 1024-bit quantum-resistant encryption), the probability of any existing model intuitively to break the encryption is negligible, making our model equally powerful and significantly more challenging than standard models.

Table 1: Comparison of Traditional Cloud Security vs. Proposed Quantum Cryptography and Blockchain Approach

Feature	Traditional Cloud Security	Proposed Approach
Key Exchange	Classical (RSA, DH, AES) – breakable by quantum computing	Quantum Key Distribution (QKD) – provably secure
Data Integrity	Centralized verification – vulnerable to tampering	Blockchain – immutable ledger with cryptographic hashes
Attack Probability	$P_c = O(1/\exp(n))$ (classical security)	$P_{final} = O(2^{-n} \times 2^{-256})$ (exponentially secure)

Comparison between Conventional Techniques and Proposed Techniques

Comparison of Previous Techniques and Proposed Techniques

The table below compares the traditional techniques used for data privacy and integrity in cloud computing with the proposed Blockchain and QKD integration:

Table 2: Comparison of Traditional Techniques vs. Proposed Blockchain and Quantum Cryptography Approach

Feature	Traditional Techniques	Proposed Technique (Blockchain + Quantum Cryptography)	Improvement
Key Exchange	RSA, Diffie-Hellman (DH), AES	QKD	QKD provides provably secure key exchange, eliminating quantum attacks.
Encryption Security	RSA, AES (128/256-bit)	Post-Quantum Cryptography(Lattice-based, QKD)	Classical encryption is breakable by Shor's algorithm; QKD ensures secure encryption.
Integrity Verification	Hashing + Digital Signatures	Blockchain-based tamper-proof storage	Blockchain ensures immutability, preventing unauthorized modifications.
Attack Resistance	Vulnerable to quantum computing (Shor's algorithm can break RSA, DH)	Post-quantum secure due to QKD and blockchain integration	Eliminates vulnerabilities in classical encryption and centralized integrity verification.
Tamper Detection	Centralized database integrity checks	Blockchain with cryptographic hash chaining	Blockchain ensures data integrity without reliance on centralized authorities.
Attack Probability	$O(1/\exp(n))$ (classical security)	$O(2^{-n} \times 2^{-256})$ (exponentially secure)	Attack feasibility drops exponentially, making the system highly secure.
Eavesdropping Detection	No mechanism in classical cryptography	QKD detects eavesdropping using quantum properties (e.g., BB84 protocol)	QKD provides real-time attack detection, unlike classical key exchange.
Data Privacy in Cloud	Encrypted but can be decrypted with future quantum computers	Secure with QKD and blockchain-stored encryption keys	Ensures long-term data privacy, even against future quantum threats.
Scalability	Requires increased key sizes for security	Scalable with quantum-safe cryptography and distributed blockchain networks	Prevents the need for larger key sizes, making security efficient.

5. Conclusion:

The integration of cloud computing, in conjunction with blockchain and quantum cryptography, has the potential to be a far-reaching solution to the growing challenges surrounding data integrity and privacy. The decentralized and immutable nature of blockchain guarantees that data cannot be altered or manipulated after being stored, resulting in the creation of a safe and transparent atmosphere. This decreases the threat of challenges such as unauthorized access to or alteration of information, primary issues with conventional cloud to be systems. Blockchain also decentralizes solutions, reducing reliance on a single central authority, making it less vulnerable to single points of failure. Even better, quantum cryptography offers complex encryption techniques that cannot be broken by even the most advanced quantum computers at some point, ensuring that critical data remains secure despite technological

advancements. It allows a type of encryption that can never be broken using classic methods, harnessing the power of the laws of quantum physics to offer a level of protection that is impossible to match against any cyberthreat, no matter how state-of-the-art. These pieces together enable a comprehensive cloud security solution where data is secured as quantum cryptography is used and data integrity is guaranteed via the transparency of the blockchain. This means, therefore, that such integration constructs a secure cloud computing environment that prevents current security issues and prepares for future challenges in the digital world. Such an amalgamation has high prospects to establish a secure, scalable and future-proof cloud ecosystem that ensures the integrity and confidentiality of data, whether for individuals or organizations.

References

1. 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.
2. 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.
3. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
4. Jamil, B., Ijaz, H., Shojafar, M., Munir, K., & Buyya, R. (2022). Resource allocation and task scheduling in fog computing and internet of everything environments: A taxonomy, review, and future directions. ACM Computing Surveys (CSUR), 54(11s), 1-38.
5. Zohar, M., et al. (2020). Blockchain in Cloud Computing: A Comprehensive Survey. Future Generation Computer Systems, 108, 835-849.
6. Narayana, S. (2022). Security analysis of web application for industrial internet of things.
7. Lin, J., Upadhyaya, T., & Lütkenhaus, N. (2019). Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. Physical Review X, 9(4), 041064.
8. Bennett, C. H., & Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.
9. Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). Ieee.
10. Wang, F., Liao, S., Yin, Y., Ni, R., & Zhang, Y. (2023). RETRACTED ARTICLE: Radio optical network security analysis with routing in quantum computing for 5G wireless communication using blockchain machine learning model. Optical and Quantum Electronics, 55(11), 1008.
11. Khan, H. U., Ali, N., Ali, F., & Nazir, S. (2024). Transforming future technology with quantum-based IoT. The Journal of Supercomputing, 80(15), 22362-22396.
12. Onieva, J. A., Rios, R., Roman, R., & Lopez, J. (2019). Edge-assisted vehicular networks security. IEEE Internet of Things Journal, 6(5), 8038-8045.
13. 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.
14. 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.
15. 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.