Quantum Key-Based Blockchain Access Control: A Secure Authentication and Data Exchange Framework for Cloud Environments

Akshay Agrawal[1], Sanketi Raut[2], Vishal Shinde[3], Dr. Rahul Thour[4]

[1,2,3] Ph.D. Scholars, Department of Computer Science & Engineering, Desh Bhagat University, Punjab

[4]Assistant Professor, Department of Computer Science & Engineering, Desh Bhagat University, Punjab

Abstract:
In the era of digital transformation, Blockchain has seen enormous growth due to its decentralized, transparent structure. However, securing sensitive data in cloud storage and distributed systems has become a critical challenge. Traditional methods lacked effective control over data access and suffered from potentially unauthorized access, especially in centralized cloud systems raising concerns about data security and privacy. To mitigate the inherent security concerns, this research proposed an Improved Elliptic Curve Cryptography based Quantum Key Distribution (IECC-QKD) enabled framework that utilizes Blockchain system to secure data exchange and access control mechanisms. The IECC incorporates the Edwards curve along with dual randomness to ensure tamper-proof resistance to the encryption and sensitive data shared on the cloud. The QKD based secured key inherits quantum mechanics principles and avoids unauthorized access by tamper-proofing the data. Additionally, the new Proof of Storage (PoSt) consensus mechanism in the Ethereum Blockchain integrates the benefits of Proof of Space (PoS) to store and prove the integrity of the data with minimizing resource consumption. The results are validated considering 50,100,150,200, and 250 number of users. For the 250 users, the IECC-QKD achieved 2.41s of encryption time, 1.55s of decryption time, 5.42s of transaction time, 0.74 of privacy ratio, 8.50s of responsiveness, and 43.088KB of memory usage.

Keywords: Proof of Storage, Data Exchange, Access Control, Blockchain, Cryptography, cloud computing.

1. INTRODUCTION

Blockchain technology has evolved as a distributed ledger that is decentralized and tracks all transactions through a set of interdependent blocks. With the occurrence of new transactions, these blocks start creating a growing chain structure. To assure the security and manage the integrity of the subsequent ledger, the Blockchain incorporates several cryptographic and decentralized consensus algorithms. The key component that the technology possesses towards contribution of saving the costs and enhancing operational efficacy [18]. This technology was introduced by Satoshi Nakamoto in 2008 and laid the position for a cryptocurrency called Bitcoin, with the reduced need for middleware, Blockchain minimizes the vulnerabilities, speeding up the process of transactions, and expenses [10]. Every block of the Blockchain covers transactional data along with the linkage to earlier blocks using a distinguished hash code, forming a secured and tamper-proof subset of records. The Blockchain functions as a collaborative network that allows the users to communicate directly instead of intermediates, fostering transparency and credibility [11]. In concern with the data management services, it displays it as a distributed database that coordinates data of transactions following a structured order of blocks. Blockchain depends on the collaborative network, empowered by the strong methods of cryptography and crowd computing systems, to bolster data security and protection. The prospect of Blockchain has grabbed attention across different sectors, spanning profound finance institutions and diverse industries discovering their applications. The nature of Blockchain to provide streamlined services and improved security

along with minimized expense frames the technology as a valuable asset for providing a wider range of innovations to different sectors [9].

The diverse schemes for access control mechanisms are implemented, with most of them using single-servers. Although centralization is prevalent, it imposes specific issues, including the single point of failure risk. The access policies and unauthorized request approval can cause severe breaches when the server grants malicious acts. To resolve these breaches of security, access control approaches that are decentralized and strong need to be implemented for IoT environments [14]. Access control is essential for the protection of data, but previous approaches, Discretionary Access Control (DAC) and Identity-Based Access Control (IBAC) are reasonable but cannot be used for cloud systems. These approaches may face difficulty in handling the high quantities of unknown identities inside the networks, making it infeasible to ensure an Access Control List (ACL) for each user. Mandatory Access Control (MAC) another aspect also deliberates and leads to the same failure issue [3]. Additionally, the calculation of access control policy is another critical problem. Yet, the resource owner's trusted party plays an important aspect in granting access or rejection. Although the requester does not trust the party, that needs accessibility against non-guaranteed access denials. For instance, even if the mechanisms of access control are controlled by the server of the resource owner, the party that evaluates could inherently block the access of a legitimate user, also when the policy permits. This highlights the necessity of a more reliable and transparent access control system that ensures scrutiny and security for all users in the cloud networks [17].

The research enhances cloud storage protection through Blockchain integration to secure the exchange of data by the users. Users get protected data access through the Blockchain system which prevents changes made to data by unauthorized users. The IECC encryption system uses minimal key values to reduce time complexity issues. The verification system in the Blockchain securely distributes data across the entire network through cryptographic hashing, consensus mechanism and validation processes. The QKD provides a secure exchange of data from a main source through the Blockchain networks that ensures efficient encryption and decryption of the data.

1.1 OBJECTIVES

The objectives of proposed research work are as follows.

- To create a secure authentication and access control mechanism for cloud-based data sharing using the Ethereum blockchain.
- To empower CBEs (data owners) to define access control policies, granting them the authority to determine who can access and send encrypted data to the CSP.
- To develop a structured framework comprising distinct phases, from global setup to decryption, to ensure secure data sharing.
- To assess the performance of the developed approach using key metrics such as bandwidth and responsiveness and compare the results against existing solutions to gauge its effectiveness and efficiency.

I.2. LITERATURE REVIEW

The security concerns in the Blockchain are delivered through this survey below.

Yang, Z. et al. [1] designed ciphertext-policy attribute-based encryption (CP-ABE), an access control framework to upgrade security while dismantling issues related to trust and centralization. The method facilitates decentralized access, optimizes parameters to reduce complexity, and mitigates risks such as temporary access and replay attacks. The comparison results measured using previous schemes showcased enhancements in protecting privacy and overall security.

Sun, L. et al. [2] presented a dynamic access control to address the issues related to the management of data storage through cloud servers. Block-chain-based and provenance-enabled dynamic access control (BPDAC) systems use a quick look-up table (QLT) that speeds up the

mechanisms by considering the data provenance. HyperledgerFabric technique is also incorporated as a prototype for performance evaluation, resulting in enhanced values with the metrics. Moreover, the model lacks in optimizing the QLT employed, which fairly impacted the overall efficiency of the approach.

Kanakasabapathi, R.S. and Judith, J.E. [3] introduced an approach termed the improved Salp Swarm Optimization based Paillier federated multi-layer perceptron (ISSO-based PF-MLP) to improve the breaches of security in the cloud systems. The approach integrates access control, Blockchain along cryptography methods to resolve the complexities of cloud storage systems. The notable drawback is that the imposition of quantum computing for encryption was found susceptible to attacks that compromised the cryptographic algorithms.

Ma, Z. and Zhang, J. [4] employed a Blockchain-based privacy-aware data access control (BPADAC) model to protect and distribute UAV information sharing through cloud systems. It incorporates the Ethereum Blockchain and smart contracts for the evaluation of performance. The results showcase the suitability and efficiency of the approach to be applied to distributed security systems. However, it does not resolve the crucial problems of UAV data source recognition and the verification of information in the cloud, which remain unaccessed.

Sarfaraz, A. et al. [5] presented an approach termed the AccessChain, that utilizes attribute-based access control (ABAC) to protect the privacy of data using the decentralized architecture. This framework enables fine-grained and dynamic management of access control, enabling it useful for securing data sharing of distributed settings. Results attained on evaluations replicate high throughput in large-scale request scenarios while ensuring data privacy and scalability of the network. Moreover, the approach compromised the proof-of-work mechanism for its access point ledger, which limited its capability to optimize the time-cost trade-off, scalability, throughput, and latency.

Liu, Y. et al. [6] introduced a model for enhancing cross-domain data security sharing mechanism called the Fabric-ABAC. This framework integrates Hyperledger Fabric alongside the ABAC to provide multi-level, fine-grained, and auditable access control. It ensures data security through delegated permission verification. By combining the decentralized ability of Blockchain with the adoption of ABAC, the Fabric-ABAC enhances data protection and streamlines permission management across various domains.

The innovative approach presented by Yan, L. et al. [7] involves Blockchain technology and ABE to improve data security and access control mechanisms of cloud environments. This approach used decentralized Blockchain and tamper-proof management of access control, yet ABE provides a secure and data sharing facility. Nonetheless, the negativeness like the enlarged computational demands, led to affect the scalability and performance.

Liu, T. et al. [8] introduced a Blockchain-based access control scheme (BCAC) along with the ABE utilization to enhance access policy and privacy. This approach deliberates to uncover the need of centralized authority, reduce single points of failure, and initiate elaborated access control. The key benefits include its scalability and capability to control attacks, while a significant dispute is computationally expensive because of ABE, which affected the performance. Moreover, the approach showcased that the framework provides secured, decentralized data sharing, maintaining data integrity, and offering effective access control in cloud computing environments.

1.3 EXISTING SYSTEMS

Various research in the context of authorized access discussed considering only the classic architectures, but those felt diminishing the required specifications like transparency in authorizing, scaling process, and the ability to control unreliability of wireless systems for the IoT access control [16]. With the evolution of blockchain, these issues are resolved with the construction of distributed networks. It also brings various merits like minimization of loads in heavy traffic nodes and reduction of single-point failure risks. It also serves flexibility in the matching of users and terminals along with the ability to make decisions using smart contracts

[13]. The distributed structure, unchangeability, failure resistance, and resilience towards rejection of blockchain are largely discussed [15] [12]. The integration of IoT alongside blockchain imposes it as a trusted policy to boost confidentiality and reduce overhead. This combination enables decentralization, an authentic and publicly verifiable database, collaborating billions of devices to connect over an established environment [9]. Moreover, issues occur on employing credential delegated approaches, generally used with smart contracts or transactions, requiring authentication from both the recipient and user ends, along with blockchain as the strong asset for carrying records and assured third-party attester. When the permissions are assigned, the receiver can prevent verification for access control, which may cause unauthorized access. However, the owner does not participate in this process. This way the need for a strong and robust authorization system is inherited by blockchain-contained IoT systems [10].

1.4 LIMITATION ON EXISTING SYSTEM

Some of the main challenges that block the effectiveness of access control mechanisms in cloud and Blockchain systems are described below.

- A significant challenge in [2] is optimizing QLT to enhance the efficiency of access control decisions. It also requires modifying the provenance-based policies for wider use, reinforcing standards for policy definitions, addressing conflicts between policies, and creating a user a user-friendly interface that allows users to manage data and access independently.
- The PF-MLP [3] results in diminishing protection of data, privacy, and digital communication across various cloud environments that compromise the performance of encryption algorithms. This situation demonstrates that the more advanced encryption techniques are not considered.
- The BPADAC [4] systems limit its capability by tackling only the identification issues of vulnerable access related to outsourced UAV data in cloud-based environments.
- The essential analyses are omitted by the access chain framework [5], which leads to increased cost of Proof-of-Work (PoW) for the access point ledger. Moreover, the cost metrics for access control and the expenses related to maintaining the ledger are also compromised.
- The ABE-based systems [7] lacked in improving user access efficiency and resulted in ineffective multi-keyword search capabilities within Blockchain systems.

1.5 PROBLEM STATEMENT

The development of Blockchain systems enables the framework to apply in industries like medical, central organizations, and supply chain systems. The comfort of accessing the data easily can create complications, particularly where market data is crucial for their organizations. Therefore, the increased volume of Blockchain necessitates the improvement of data security and access control mechanisms. Nonetheless, Blockchain serves as a decentralized asset that facilitates immutable storage of data; however, the incorporation of robust access control imposes frequent challenges like managing the architecture that deals with the transactions and ensuring secure data transmission for better accessibility. Conventional solutions inherit issues in data integrity, maintaining the privacy of data, addressing interpretability, and safeguarding sensitive information against unauthorized access. These issues in the later time can lead to consequences like vulnerable attacks, uncertified access, data breaches, and inconsistency in meeting regulatory policies. Moreover, the inconvenience of essential encryption standards and verification for the data in decentralized environments can reduce the scalability and security of Blockchain systems. This research aims to design a more secure authentication and access control mechanism in the cloud systems to ensure efficient information exchange between authenticators and users.

2. PROPOSED SYSTEM

The growth of decentralized technology and cloud systems has intransitively enhanced the necessity of improved authentication and access to data through employing different mechanisms. This research aims to manage the challenges that are prevalent in the domain of securing data by designing a framework that collaborates Blockchain as a digital ledger to initiate better accessibility, maintaining privacy and integrity in the cloud systems. The main objective of the model is to prevent the vulnerability of third parties in the network. The system comprises several paradigms that perform subsequent actions to share and access the data securely. The data owner and the data user are the main contributors to initiate the transfer and recovery of data. At the initial stage, the owner can store the data in the server disruptively, and the user can access the data by initiating the request. Upon request, the validation authority that serves as the central policy for verification validates whether the user accessibility is valid or not. After verifying the credentials, the authority grants access by stating the message as granted access or denied. The Blockchain that serves a decentralized mode of storage delivers the request to the cloud storage, where the decryption fundamentals like requesting the key is initiated, to the data owner. The data owner verifies the request, decrypts the data, and forwards it to the Blockchain, that ensures the effective accessibility of data. The detailed structure of the system model is illustrated in Figure 1.

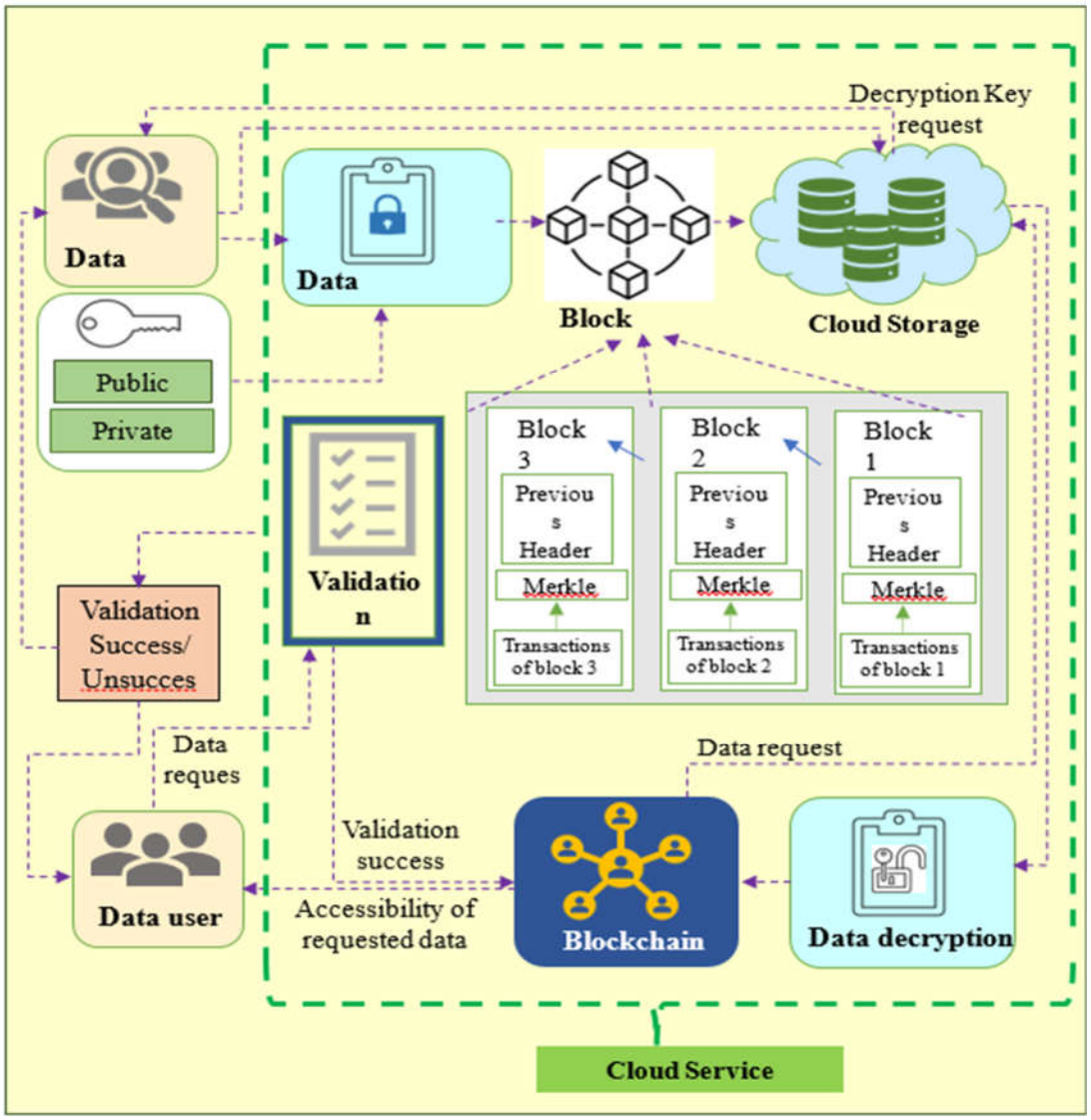

Fig. 1: Detailed structure of the system model

3. METHODOLOGY

3.1. Improved Elliptic Curve Cryptography based Quantum Key Distribution framework (IECC-QKD) for secure exchange and access of cloud data

The key intention of the research is to design a blockchain-based framework enabling the authentication and access control encryption schemes for the secured exchange and access of data. It will act as a mutual authentication system that operates according to the data users and the data owner. The proposed framework comprises various phases each determining the specific actions. In the initial global setup phase, the Consortium Blockchain Entities (CBE) which acts as data owners enrol the registration with the Cloud-Based Monitoring (CBM) through setup initialization with the Cloud Service Provider (CSP) and checks whether the user exists or not using the hash values. If the corresponding CBE is the existing user, then the CBM includes control policies along with the signature of the CSP and transfers the data to IPFS blockchain, which serves as the CSP. These actions are carried out in the CBM verification phase as join and matching. Then, the generation of tokens and indices is accomplished by the CSP for secure transactions and the copy is transferred to CBE which helps verify the authenticity further during the stage of decryption. The secret key is generated by introducing the IECC-QKD encryption scheme, which ensures that the key serves as an improved resistant standard for encrypting the data and downside also for the decryption. After storing the data, the Cloud-based Data User (CBDU), who can also act as CBE, requests data. During this phase, the generated token and index are matched to ensure the successful enrolment of the users.

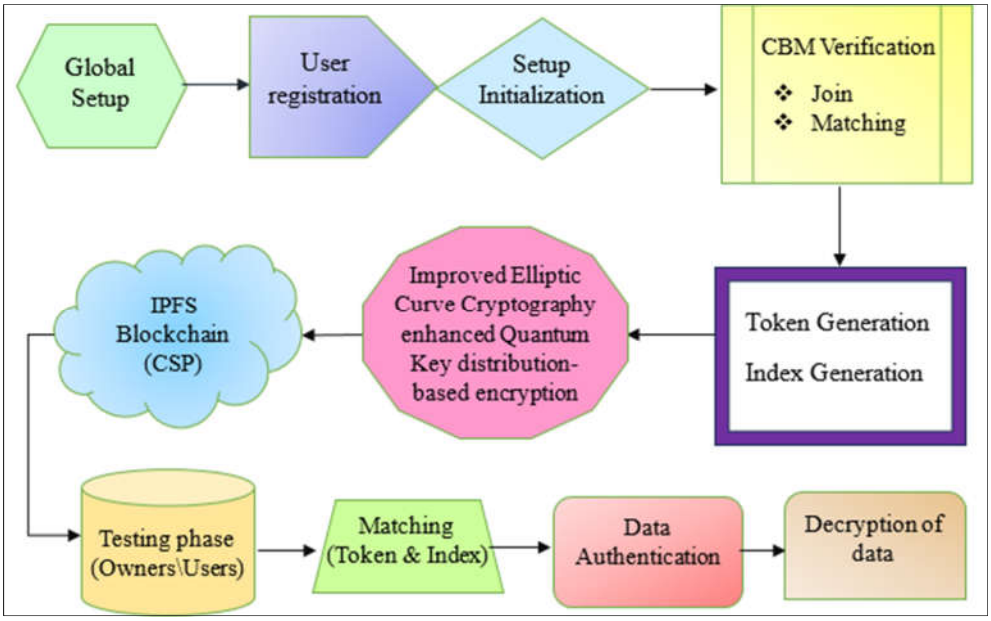

Figure 2. General workflow of the Quantum key-based Improved ECC Blockchain framework

When the subsequent entities are valid, then the authentication mechanisms and the decryption of data is performed using the generated key. Finally, the particular original data is transferred securely to the regulatory. The detailed visual representation of the phases of the proposed IECC-QKD-based BC framework is illustrated in Figure 2.

3.2 Global Setup

The system comprises several entities in the proposed IECC-QKD-based Blockchain framework that indulges subsequent actions. The global setup consists of Consortium Blockchain Entities (CBE), Cloud Based Monitoring (CBM), Cloud Service Provider (CSP), and Cloud Based Data Users (CBDU).

Consortium Blockchain Entities (CBE): CBEs are the data providers that serve as owners, that are responsible for defining the access control policies and decisions to transfer data to the CSP.
Cloud-Based Monitoring (CBM): CBM is the authority that provides authentication and initiates the transactions based on the verification of the access information.
Cloud Service Provider (CSP): CSP ensures the securing of storage systems, infrastructure layers, and many more. The IPFS is implemented as CSP, it is a type of storage that enables the users to access and store data through a decentralized network.
Cloud-Based Data Users (CBDU): CBDUs are the data users that request and retrieve data through the CSP. However, CBDU can also act as CBE in the context of storing data in the CSP.

3.3 User Registration

The authorized access is initiated by the registration for the safe usage of keys and to ensure the overall security of the system. Initially, the safety parameter η implies the sensitivity of the owner data. Every node in the Blockchain runs on an algorithm to produce public and private keys with the initialization of attributes.

3.3.1 Initializing the Setup

The setup can be initialized based on the requests of both CBE and CBDU. Let us initialize the data *td* for the CBE as

$$CBE_{td} = \left\{ CBE_{td(1)}, ..., CBE_{td(e)}, ..., CBE_{td(f)} \right\} \tag{1}$$

where, $CBE_{td(e)}$ implies the data of e^{th} CBE and $CBE_{td(f)}$ denotes the entire CBE's enrolling for the transaction. The data contains certain attributes that define the sensitive characteristics of particular CBE. The attributes A_t of the $CBE_{td(e)}$ can be initialized as,

$$A_t\left(CBE_{td(e)}\right) = \left\{ \left(CBE_{eN}, CBE_{ePW}, CBE_{eID} \right) \right\} \tag{2}$$

where, CBE_{eN} , CBE_{ePW} , CBE_{eID} denotes the unique attributes like name, password, and ID numbers, respectively. This copy of the information is also available at CSP which is described in equation (3) as

$$A'_t\left(CBE^*_{td(e)}\right) = \left\{ \left(CBE^*_{eN}, CBE^*_{ePW}, CBE^*_{eID} \right) \right\} \tag{3}$$

The CBDU is also initialized with unique attributes that can be described as

$$A_t\left(CBDU_{td(e)}\right) = \left\{ \left(CBDU_{eN}, CBDU_{ePW}, CBDU_{eID} \right) \right\} \tag{4}$$

The attributes stored at the CSP for maintaining the access is denoted as,

$$A'_t\left(CBDU^*_{td(e)}\right) = \left\{ \left(CBDU^*_{eN}, CBDU^*_{ePW}, CBDU^*_{eID} \right) \right\} \tag{5}$$

3.4 CBM Verification

The CBM verification serves as the central authority of verification that issues accessibility through several checks. It involves two phases called the join and match phase which is explained further and describes the relevant use in the framework.

3.4.1 Join phase

The CBE selects the subsequent data along with the essential credentials. This phase is known as "Request setup" which includes further information like address of Blockchain, private key, and the request indicator along with the attribute set. The request setup is mathematically derived as

$$CBE \rightarrow CBM : R_{st}\left(BC_{PK}, BC_{ad}, R_{ft}, CBE_{td(e)}\right) \tag{6}$$

Here, R_{st} denotes the request setup, BC_{PK} and BC_{ad} denotes the private key and the Blockchain address $CBE_{td(e)}$ denotes the attribute set of the owner and R_{ft} is the indicating factor that indicates whether the transaction is initiated by the CBM.

3.4.2 Matching phase

The CBM processes the request initiated through a secured channel to validate whether the owner of the existing one is a valid user or not. The CBM checks the credentials, if it matches, the CBM indulges CBE to join for data transfer process.

$$CBM \rightarrow check\left(CBE_{eN}, CBE_{ePW}, CBE_{eID}\right) \in A_t'\left(CBE^*_{td(e)}\right) \tag{7}$$

After the CBM verification, the authenticator further initiates the process of generating tokens and indices respectively.

3.5 Generation of Tokens and Indices

The process of both index and token generation avoids the possibility of using the original data by the data owner and user. This ensures the immutability of the sensitive data and serves as the enrollment factor that changes the perspective with more difficult accessibility of the data. It is generated once the CBE /CBDU is initialized by CBM through IPFS. It also serves as a two-factor authentication mechanism making it more efficient for storing and decrypting the data.

3.5.1 Index generation using SHA-3

Generating an index through SHA-3 is more efficient than the other versions of SHA due to its internal structure. SHA-3 [19] operates on a different structure called the “sponge”. The index generated through this approach provides security and resilience against malware and avoidance of length extension attacks. The sponge function works on two important phases namely the absorbing phase and the squeezing phase. The absorbing phase is performed by XOR operation between the input states and the squeeze phase involves producing message digest through concatenating the internal states. The index generation for each CBE/CBDU can be denoted as,

$$I_1 = H\left(CBE_{eN} \oplus CBE_{eID}\right) \tag{8}$$

$$I_{CBE(e)} = \left[I_1 \| H\left(CBE_{ePW}\right)\right] \tag{9}$$

where, I_1 denotes the initial index parameter, $I_{CBE(e)}$ denotes the final index parameter for the e^{th} CBE. H denotes the message digest generated by the hash function. Also, the I_1^* and $I^*_{CBE(e)}$ determines the same information stored at the CBM. The output message digest enables the system with enhanced security making it more impracticable for the intruders to identify the hash value.

3.5.2 Token generation through Salt

Token generation in the authentication system mitigates unauthorization and improves accessibility by indulging them within a specific time period. For generating tokens, the critical information of the CBE/CBDU is processed. While generated message digests through hashing algorithms produce hashed outputs that are unique. However, the system that generates output based on the provided message, can produce the same results for the identical inputs. This paves the way for the attackers to interrupt the system, and to avoid this situation the concept of salt is introduced. Salt [20] utilizes the pseudo-random number generation (PSRNG) technique to generate a unique message digest based on the target length that varies accordingly with the time spans. The generated salt for the CBE can be defined as $S_{CBE(e)}$. The token generation can be represented as,

$$t_{CBE(e)} = t_f\left(CBE_{ePW}, S_{CBE(e)}\right) \tag{10}$$

$$t_f \rightarrow \{t_{st}, t_{lt}, T_L\} \tag{11}$$

Here, the $t_{CBE(e)}$ implies the token of the e^{th} CBE, CBE_{ePW} implies the critical information of the password, $S_{CBE(e)}$ implies the salt value, and t_f implies the token function that includes the characteristics of the token. t_{st}, t_{lt}, T_L indicates the token's start time, lifetime, and the target length obtained based on the safety parameter η . Subsequently, these details are also stored at CBM end as $t^*_{CBE(e)}$ or $t^*_{CBDU(e)}$ in the case of the user acting as the owner. Thus, the generated token includes mixed characteristics that make it a more difficult and secure way to initiate the transaction.
The token generated through this technique ensures a limited period of access based on the safety parameter η to enhance the integrity of the authentication system.

3.6 Ethereum Blockchain as Proof of Storage

The secure data access and the immutable storage functions are provided by the Ethereum Blockchain. Ethereum Blockchain provides decentralized storage with the utilization of smart contracts. Smart contracts are the executable codes that serve as a locker to the system. To enroll in the system, the specific agreements should meet with the shared parties. These agreements are internally initiated through the consensus mechanism. The Ethereum [25] operates based on the Proof of Stake (PoS) consensus mechanism that relies on the node's stake aggregation. This approach is far better than the traditional Proof of Work (PoW). Even though each of these mechanisms inherits significant challenges. To mitigate this, the new Proof of Storage (PoSt) system is incorporated that focuses on solving problems with PoW and PoS by designing advanced consensus methods. PoSt does not require extensive energy usage like PoW or risk centralization like PoS. PoSt functions based on the Proof of Space concept, which evaluates users who actively use their storage space to store genuine data. Instead of showing only the available space, Proof of Space proves that network users utilize their storage space properly at the verification time. These security features of PoSt provide attractive benefits to decentralized networks besides PoW.
PoSt proves to be an energy-efficient solution in its design. The system uses existing storage systems rather than computation power like PoW [26] which makes PoSt both energy-friendly and practical to use. The stored data brings practical benefits like providing decentralized file storage and retrieving while adding value to the consensus network. PoSt provides additional security compared to Proof of Space because it confirms that storage space gets actually used whereas Proof of Space only checks storage space availability. PoSt strengthens security because people who validate must use their storage space to collect data which makes it hard for hackers to attack. Network participants depend on cryptographic evidence to verify data accuracy while trusting the system. PoSt improves decentralization through its storage-based approach because many nodes can take part as storage resources are widely available across networks.

The consensus mechanism of PoSt operates by smart contracts where all the provers need to show valid proof records at established times to confirm their ongoing data storage success. The system selects random data stored on the system to check its accuracy through a cryptographic hash or Merkle proof generation process. Other network participants verify the proofs that verifiers examine to make sure that the person holding storage space meets their agreements. The system accepts the prover into consensus activities when they present valid proof of their data storage duties. Based on this type of consensus mechanism, the smart contract works and verifies the transactions. The data transferred through the Blockchain layer BC_{PK}, BC_{ad} are finally transferred to the CSP for the encryption process.

4. Results and discussion

The results of the IECC-based QKD framework are elaborated by discussing the evaluation of performance and the comparison in the context of data authentication and security.

4.1 Experimental Setup

The whole framework is experimented with using the Windows 11 OS with 16GB RAM and 128 GB ROM and implemented through executable codes on the Python platform.

4.2 Performance Metrics

The metrics employed to reflect the effectiveness of the proposed IECC-QKD are described below.

a) Encryption time: The total time required for the authentication system to transform plain text into cipher text.

b) Decryption time: The total time required for the authentication system to recover cipher text back from plain text.

c) Transaction time: The total time initiated by the system to complete a transaction. This includes authenticating the authorized access to data.

d) Privacy Ratio: Implies the proportion of the sensitive data authenticated by the system and protected while transmitting or storing the data.

e) Responsiveness: The rate at which the access control requests are processed by the system.

f) Memory Usage: The total energy consumed by the system to perform operations like encryption, decryption, and other access control operations.

4.3 Analysis of Performance Based on the Curves

The performance of the proposed IECC-QKD-based framework is analysed using different curves like secp192r1-IECC-QKD, secp224r1-IECC-QKD, brainpoolP256r1-IECC-QKD, and brainpoolP224r1-IECC-QKD by validating with 50,100,150,200 and 250 users respectively. The visual representation of the curve-based performance is depicted in Figure 8. For 250 users, the proposed IECC-QKD required an encryption time of 2.41s, whereas the secp192r1-IECC-QKD curve required 3.08s, secp224r1-IECC-QKD required 2.91s, brainpoolP256r1-IECC-QKD required 2.76s, and brainpoolP224r1-IECC-QKD required 2.75s. Subsequently while decrypting the data, the IECC-QKD decrypts at the rate of 1.55s, with secp192r1-IECC-QKD, secp224r1-IECC-QKD, brainpoolP256r1-IECC-QKD, and brainpoolP224r1-IECC-QKD curves decrypts data at 3.19s, 3.00s, 2.86s, and 2.44s respectively. While analysing these curves for transaction time, the IECC-QKD needs 5.42s for exchanging the data. On the downside, the other curves like secp192r1-IECC-QKD need 10s, secp224r1-IECC-QKD need 6.85s, brainpoolP256r1-IECC-QKD need 6.64s, and brainpoolP224r1-IECC-QKD, needs 10s, 6.85s, 6.64s, and 5.42s for complete the transaction. Similarly, to maintain the privacy of the system the proposed model maintains a solid ratio rate of 0.74, where the secp192r1-IECC-QKD, secp224r1-IECC-QKD, brainpoolP256r1-IECC-QKD, and brainpoolP224r1-IECC-QKD curves attains privacy ratio of 0.52, 0.53, 0.59, and 0.67. With 250 users, the IECC-QKD attains responsiveness of 8.50s that is shorter than the 10.63s, 9.93s, 9.90s, 9.82s achieved by secp192r1-IECC-QKD, secp224r1-IECC-QKD, brainpoolP256r1-IECC-QKD, and brainpoolP224r1-IECC-QKD curves. For the consumption of energy, the IECC-QKD with 250 users necessitates 430.88KB, while the other curves secp192r1-IECC-QKD, secp224r1-IECC-QKD, brainpoolP256r1-IECC-QKD, and brainpoolP224r1-IECC-QKD necessitates 496.50KB, 478.94KB, 454.41KB, and 439.74KB, respectively.

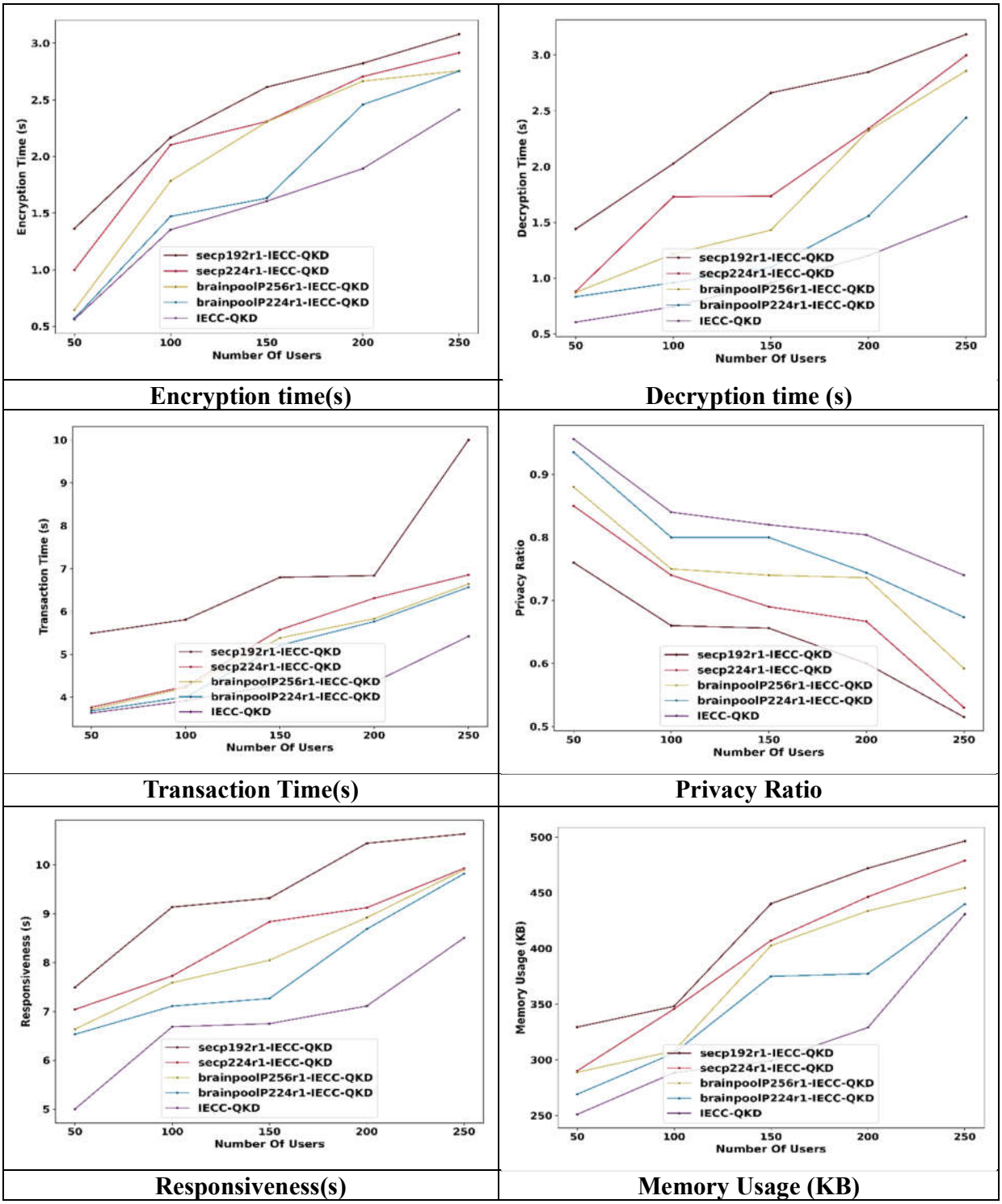

Figure 3. Performance Analysis of the IECC-QKD by analysing different curves

5. Conclusion

The growing dependence on cloud servers for data storage has driven individuals to demand more control and access over their data. Nevertheless, existing static access control models are inadequate in meeting the requirements for dynamic and self-managed access control. To address this concern, this research proposes an IECC-QKD-based framework that incorporates Blockchain to improve data access and storage in cloud systems. The standard IECC mechanism indulges the protection increase through Edwards curves while preventing spam transaction attacks, and generating keys based on multiple randomness. Also, the small key sizes of IECC demonstrate better security protection than other cryptographic methods. The QKD integrated with IECC

ensures quantum-resistant protection. The modifications in the consensus mechanism of the Ethereum Blockchain lead to secure data immutable, avoiding alterations and unauthorization. The outcomes of the IECC-QKD-based framework are analyzed for 50,100,150, 200, and 250 users. For the validation of 250 users, the proposed framework attains encryption time of 2.41s, decryption time of 1.55s, transaction time of 5.42s, privacy ratio of 0.74, responsiveness of 8.50s, and memory usage of 43.088KB. However, challenges such as the requirement for specialized quantum hardware, integration complexity, key rate limitations, and the lack of standardized protocols should be addressed in future work to fully realize the potential of this combination.

References

[1] Yang, Z., Chen, X., He, Y., Liu, L., Che, Y., Wang, X., Xiao, K. and Xu, G., 2024. An attribute-based access control scheme using Blockchain technology for IoT data protection. High-Confidence Computing, 4(3), p.100199.
[2] Sun, L., Zhou, D., Liu, D., Tang, J. and Li, Y., 2023. BPDAC: A Blockchain Based and Provenance Enabled Dynamic Access Control Scheme. IEEE Access, 11, pp.142552-142568.
[3] Kanakasabapathi, R.S. and Judith, J.E., 2024. Enhancing cloud storage security through Blockchain-integrated access control and optimized cryptographic techniques. International Journal of Advanced Technology and Engineering Exploration, 11(117), p.1183.
[4] Ma, Z. and Zhang, J., 2023. Efficient, traceable and privacy-aware data access control in distributed cloud-based IoD systems. IEEE Access, 11, pp.45206-45221.
[5] Sarfaraz, A., Chakrabortty, R.K. and Essam, D.L., 2023. AccessChain: An access control framework to protect data access in Blockchain enabled supply chain. Future Generation Computer Systems, 148, pp.380-394.
[6] Liu, Y., Yang, W., Wang, Y. and Liu, Y., 2023. An access control model for data security sharing cross-domain in consortium Blockchain. IET Blockchain, 3(1), pp.18-34.
[7] Yan, L., Ge, L., Wang, Z., Zhang, G., Xu, J. and Hu, Z., 2023. Access control scheme based on Blockchain and attribute-based searchable encryption in cloud environment. Journal of Cloud Computing, 12(1), p.61.
[8] Liu, T., Wu, J., Li, J., Li, J. and Li, Y., 2023. Efficient decentralized access control for secure data sharing in cloud computing. Concurrency and Computation: Practice and Experience, 35(17), p.e.6383.
[9] Ding, S., Cao, J., Li, C., Fan, K. and Li, H., 2019. A novel attribute-based access control scheme using Blockchain for IoT. IEEE Access, 7, pp.38431-38441.
[10] Shi, J., Li, R. and Hou, W., 2020. A mechanism to resolve the unauthorized access vulnerability caused by permission delegation in Blockchain-based access control. IEEE Access, 8, pp.156027-156042.
[11] Wang, S., Wang, X. and Zhang, Y., 2019. A secure cloud storage framework with access control based on Blockchain. IEEE access, 7, pp.112713-112725.
[12] Liu, H., Han, D. and Li, D., 2020. Fabric-IoT: A Blockchain-based access control system in IoT. IEEE Access, 8, pp.18207-18218.
[13] Li, Y., Cao, B., Liang, L., Mao, D. and Zhang, L., 2021. Block access control in wireless Blockchain network: Design, modeling and analysis. IEEE Transactions on Vehicular Technology, 70(9), pp.9258-9272.
[14] Sun, S., Du, R., Chen, S. and Li, W., 2021. Blockchain-based IoT access control system: towards security, lightweight, and cross-domain. Ieee Access, 9, pp.36868-36878.
[15] Xiong, Z., Zhang, Y., Niyato, D., Wang, P. and Han, Z., 2018. When mobile Blockchain meets edge computing. IEEE Communications Magazine, 56(8), pp.33-39.
[16] Di Francesco Maesa, D., Mori, P. and Ricci, L., 2017, May. Blockchain based access control. In IFIP international conference on distributed applications and interoperable systems (pp. 206-220). Cham: Springer International Publishing.

[17] Pinno, O.J.A., Gregio, A.R.A. and De Bona, L.C., 2017, December. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-6). IEEE.
[18] Sharma, P., Jindal, R. and Borah, M.D., 2022. Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. the Journal of Supercomputing, 78(6), pp.7700-7728.
[19] Nugroho, K.A., Hangga, A. and Sudana, I.M., 2016, October. SHA-2 and SHA-3 based sequence randomization algorithm. In 2016 2nd International Conference on Science and Technology-Computer (ICST) (pp. 150-154). IEEE.
[20] Ali, A.A.M.A., Hazar, M.J., Mabrouk, M. and Zrigui, M., 2023. Proposal of a modified hash algorithm to increase Blockchain security. Procedia Computer Science, 225, pp.3265-3275.
[21] Khan, M.A., Quasim, M.T., Alghamdi, N.S. and Khan, M.Y., 2020. A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEe Access, 8, pp.52018-52027.
[22] Veerabadrappa, K., Naikodi, C.B., Venkataswamy, S.B. and Narayanaswamy, H.K., 2024. Elliptic Curve Cryptography and Password Based Key Derivation Function with Advanced Encryption Standard Method for Cloud Data Security. International Journal of Intelligent Engineering & Systems, 17(6).
[23] Renner, R. and Wolf, R., 2023. Quantum advantage in cryptography. AIAA Journal, 61(5), pp.1895-1910.
[24] Charjan, S. and Kulkarni, D.H., 2015. Quantum key distribution by exploitation public key cryptography (ECC) in resource constrained devices. International Journal, 5.
[25] Kushwaha, S.S., Joshi, S., Singh, D., Kaur, M. and Lee, H.N., 2022. Systematic review of security vulnerabilities in ethereum Blockchain smart contract. Ieee Access, 10, pp.6605-6621.
[26] Lashkari, B. and Musilek, P., 2021. A comprehensive review of Blockchain consensus mechanisms. IEEE access, 9, pp.43620-43652.