Comparative Analysis of IECC-QKD with several access control and security approaches for Secure Authentication and Data Sharing in Cloud Environments.

Akshay Agrawal[1], Dr. Rahul Thour[2]

[1] Ph.D. Scholar, Department of Computer Science & Engineering, Desh Bhagat University, Punjab
[2]Assistant Professor, Department of Computer Science & Engineering, Desh Bhagat University, Punjab

Abstract:

Blockchain has evolved a lot in the context of digital transformation as it is decentralized and accessible. However, it has become extremely difficult to keep sensitive data secure in cloud storage and distributed systems. Traditional methods didn't do a good job of controlling who could access data, and there was a risk of unauthorized access, especially in centralized cloud systems, which raised concerns about data security and privacy. This study suggested an Improved Elliptic Curve Cryptography-based Quantum Key Distribution (IECC-QKD) framework that uses a blockchain system to protect data exchange and access control mechanisms in order to reduce security risks. The Edwards curve and binary randomness are both used in the IECC to make sure that the encryption and sensitive data participated on the cloud are safe from tampering. The QKD-based secure key uses quantum mechanics to keep the data safe from unauthorized access by making it impossible to tamper with. The new Proof of Storage (PoSt) consensus mechanism in the Ethereum blockchain also combines the best parts of Proof of Space (PoS) to store and prove the integrity of the data while using as few resources as possible. [27]

Keywords:

IECC-QKD, Consortium Blockchain Entities (CBE), Cloud-Based Monitoring (CBM), Cloud Service Provider (CSP), Cloud-Based Data Users (CBDU).

1. Introduction

As digital infrastructures become increasingly complex and interdependent, ensuring robust security for sensitive data and communications is critical for both organizations and individuals. As a result, the demand for future-proof and quantum-resistant security solutions has intensified across digital infrastructures. Access control systems such as Cipher Text-Policy Attribute-Based Encryption (CP-ABE), Fabric-Attribute Based Access Control (Fabric-ABAC), Blockchain Capability Access Control (BCAC), Blockchain-based Privacy-preserving Attribute-Driven Access Control (BPADAC), and Blockchain-powered Dynamic Access Control (BPDAC) have emerged to address the scalability, privacy, and fine-grained policy enforcement requirements inherent in distributed environments. These models offer advanced frameworks that shift beyond static, identity-based approaches by utilizing attributes or blockchain technology for efficient authorization and detailed auditing.

Parallel to these advancements, Quantum Key Distribution (QKD) presents an innovative cryptographic paradigm that leverages quantum mechanical principles to ensure theoretically unbreakable key exchange. Improved Elliptic Curve Cryptography-based Quantum Key Distribution (IECC-QKD) integrates the computational efficiency and strong mathematical assurances of elliptic curve cryptography with the information-theoretic security guarantees of QKD, thereby strengthening both resistance to quantum attacks and practical deployment for next-generation communications. This hybrid approach aims to achieve robust authentication,

lightweight computation, and provable resilience against both traditional and quantum-enabled adversaries.

This paper presents a comprehensive comparative analysis of IECC-QKD with contemporary attribute-based and blockchain-enhanced access control frameworks. The analysis systematically evaluates their underlying security principles, protocol structures, implementation feasibility, and resilience to present and emerging threats. By situating IECC-QKD alongside CP-ABE, Fabric-ABAC, BCAC, BPADAC, and BPDAC, this study aims to clarify the unique strengths, operational constraints, and potential integration pathways for quantum-secure cryptography in the evolving landscape of distributed access control.

The main contributions of the research are highlighted below:

- **IECC-QKD**: The incorporation of multiple random values in the ECC encryption generates stronger defensive results than the basic ECC algorithm. The IECC uses Edwards's curves instead of Weierstrass curve which enhances security by reducing processing requirements. Combining QKD with improved ECC offers a strong secure encryption system where two parties communicate safely through the quantum mechanics principles of QKD. IECC-QKD stands out as the best cryptographic system when resources are limited due to its processing speed and high-security levels while using shorter keys. [21]
- **Index and Token generation:** The mechanism of generating index and token helps to prevent tampering of data by unauthorized users. The index generated through SHA-3 offers a strong standard against vulnerabilities and avoidance of length-extensive attacks. The tokens allow the users to access the system for particular validity to assure accessibility only during the intended time frame. This two-factor authentication procedure enhances defense mechanisms and improves digital data protection. [19]
- **Ethereum as Proof of Storage:** PoSt builds an enhanced consensus system that replaces PoS with strong defence capabilities to benefit the network's performance. User access complete system functions through the Ethereum blockchain while performing verification tasks without using significant computer power. This technique has transformed the blockchain systems and decentralized storage networks by integrating the PoSt algorithm replacing the conventional consensus method. [25]

The remaining portion of the research is categorized as follows. Section 2 explains the literature works, and section 3 delves into the problem statement to rectify and innovate. Section 4 describes the mechanisms and the processes carried out for developing access control systems. Section 5 delivers the comparative analysis and section 6 concludes with wrapping the future scopes.

2. Literature Review

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

Yang, Z. *et al.* [1] developed a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) framework aimed at enhancing security by eliminating centralization and trust issues. Their approach supports decentralized access control while reducing risks such as replay attacks and temporary access through optimized parameters, demonstrating superior privacy protection and overall security compared to previous schemes.

Sun, L. *et al.* [2] proposed a dynamic access control system for managing cloud server data that incorporates data provenance. Their Blockchain-based Provenance-enabled Dynamic Access Control (BPDAC) system utilizes a quick look-up table (QLT) to accelerate access mechanisms.

Performance evaluation using Hyperledger Fabric showcases improved metrics, though optimization of the QLT remains an area for enhancement to boost efficiency.

Kanakasabapathi, R.S. and Judith, J.E. [3] introduced an improved Salp Swarm Optimization-based Paillier Federated Multi-Layer Perceptron (ISSO-based PF-MLP) to mitigate security breaches in cloud systems. This method integrates blockchain, access control, and cryptography; however, vulnerabilities to quantum computing attacks reduce the robustness of the encryption algorithms involved.

Ma, Z. and Zhang, J. [4] used a privacy-aware Blockchain-based Access Control (BPADAC) model to secure UAV data sharing in cloud systems using Ethereum smart contracts. While the approach demonstrates efficacy for distributed security, critical challenges such as cloud data verification and UAV source identification remain unaddressed.

Sarfaraz, A. *et al.* [5] introduced AccessChain, which combines decentralized architecture with Attribute-Based Access Control (ABAC) to provide fine-grained, dynamic data privacy protection. The framework exhibits high throughput and scalability but suffers from limitations in the Proof-of-Work mechanism of its access point ledger, restricting latency, scalability, and throughput trade-offs.

Liu, Y. *et al.* [6] developed Fabric-ABAC, improving cross-domain data sharing security by integrating Hyperledger Fabric with ABAC. This multi-level, auditable access control framework employs delegated permission verification, enhancing security and simplifying permission management in multi-domain blockchain environments.

Blockchain technology and ABE are used in the novel method put forth by Yan, L. et al. [7] to enhance cloud environments' data security and access control systems. ABE offers a safe and data-sharing environment, but this method used a decentralized blockchain and tamper-proof access control management. However, the drawbacks, such as increased computational demands, had an impact on performance and scalability.

Liu, T. *et al.* [8] proposed a Blockchain-based Access Control (BCAC) scheme integrating ABE to bolster privacy and policy enforcement while minimizing dependence on centralized authorities. This approach offers decentralized secure data sharing and integrity assurance; however, it exhibits high computational costs that hinder system performance.

2.1. Challenges

Several key challenges continue to hinder the effectiveness of access control mechanisms within cloud and blockchain systems.

- Enhancing the Quality of Logical Thinking (QLT) to improve the precision of access control decisions remains a significant challenge. Moreover, provenance-based access policies require adaptation for wider applicability, policy definition frameworks need to be standardized and strengthened, conflicts among policies must be effectively resolved, and user-friendly interfaces are essential to empower end-users in managing their own data and access rights.
- The performance of encryption algorithms within the Privacy-Preserving Federated Multi-Level Permission (PF-MLP) framework deteriorates, leading to diminished protection of data privacy and secure communication across multiple cloud environments. This highlights a gap where advanced encryption techniques have yet to be fully integrated and utilized.
- Systems based on Blockchain-based Privacy-preserving Attribute-Driven Access Control (BPADAC) exhibit limitations by focusing primarily on addressing vulnerabilities related

to outsourced UAV data within cloud ecosystems, thereby restricting their broader applicability and utility.

- The access chain framework lacks comprehensive analytical components, resulting in increased Proof-of-Work (PoW) costs associated with maintaining the access point ledger. Additionally, this insufficiency impacts the overall expenses related to ledger upkeep and the metrics of access control cost-efficiency.
- Attribute-Based Encryption (ABE)-based systems suffer from inefficiencies in multi-keyword search functions within blockchain contexts, which directly hamper the effectiveness and responsiveness of user access operations.

3. Problem Statement

Evaluating access control and security mechanisms requires a comprehensive balance between cryptographic strength and system performance. Key performance indicators such as encryption time, decryption time, transaction time, privacy ratio, responsiveness, and memory usage collectively determine the practical viability and security assurance of these mechanisms in real-world deployments.

Existing attribute-based and blockchain-enhanced access control models often suffer from computational overheads in encryption and decryption processes, resulting in latency that impairs system responsiveness and transaction throughput. Moreover, these conventional systems may inadequately protect user privacy, reflected in suboptimal privacy ratios, while high memory consumption limits scalability and implementation feasibility in resource-constrained environments.

Although Quantum Key Distribution (QKD) protocols provide unparalleled security guarantees founded on quantum physics, practical issues such as error rates, key generation rate, and integration latency impact the encryption and decryption efficiency. The Improved Elliptic Curve Cryptography-based QKD (IECC-QKD) approach aims to optimize this trade-off by enhancing key generation efficiency and reducing computational overhead while preserving high privacy and responsiveness standards. [22]

This research investigates how IECC-QKD compares with state-of-the-art access control approaches on these fundamental metrics, seeking to address performance bottlenecks and privacy challenges that inhibit the widespread adoption of secure, scalable quantum-resilient access control systems.

4. Mechanism & Process:

4.1. User Registration

To ensure the overall security of the system and the safe utilization of cryptographic keys, the registration process initiates authorized access. Initially, the sensitivity level of the data owner is represented through a security parameter. Subsequently, each blockchain node employs a designated algorithm to generate corresponding public and private key pairs after the relevant attributes have been initialized. [27]

4.1.1. Initializing the Registration Setup:

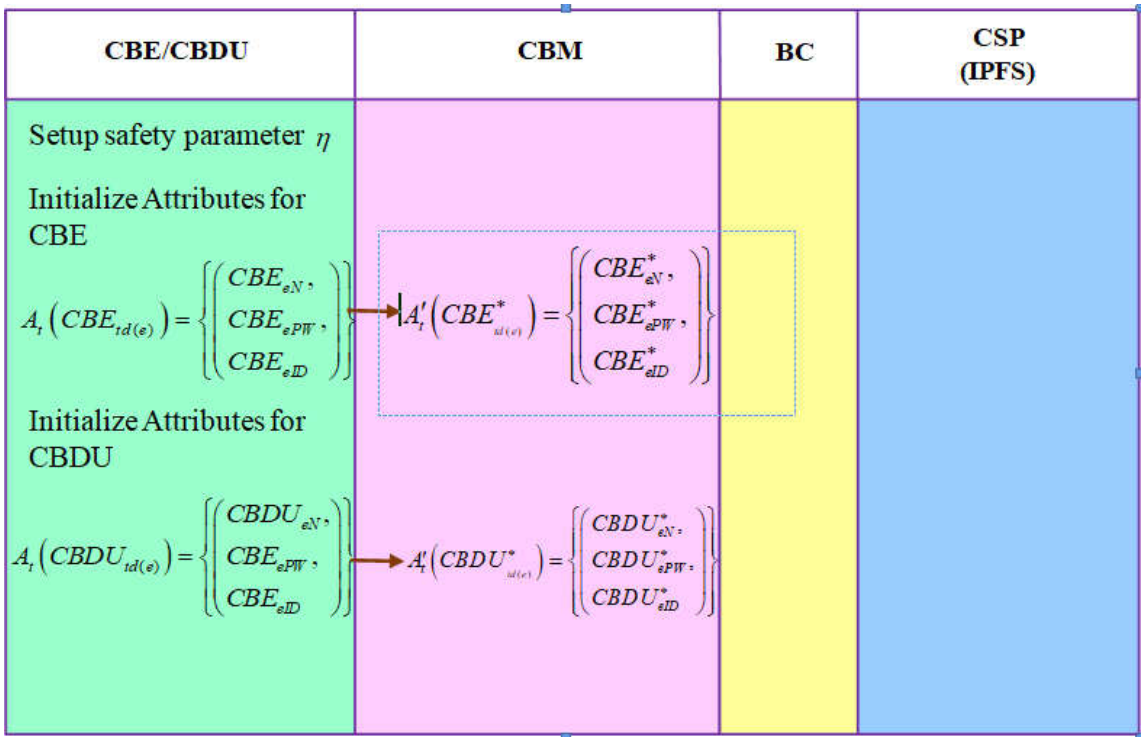


Figure 4.1.1. Initial Register phase for initializing Attributes

4.1.2. CBM Verification process:

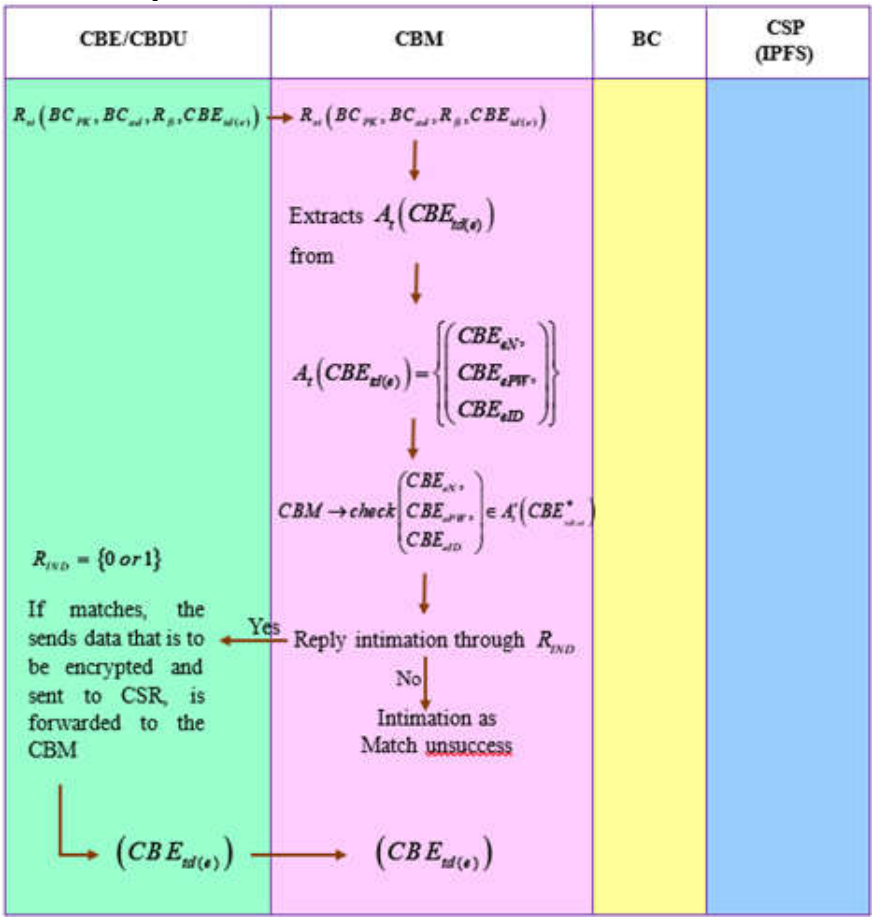


Figure 4.1.2. Schematic representation of CBM Verification process

4.1.3. Index & Token generation process through Salt

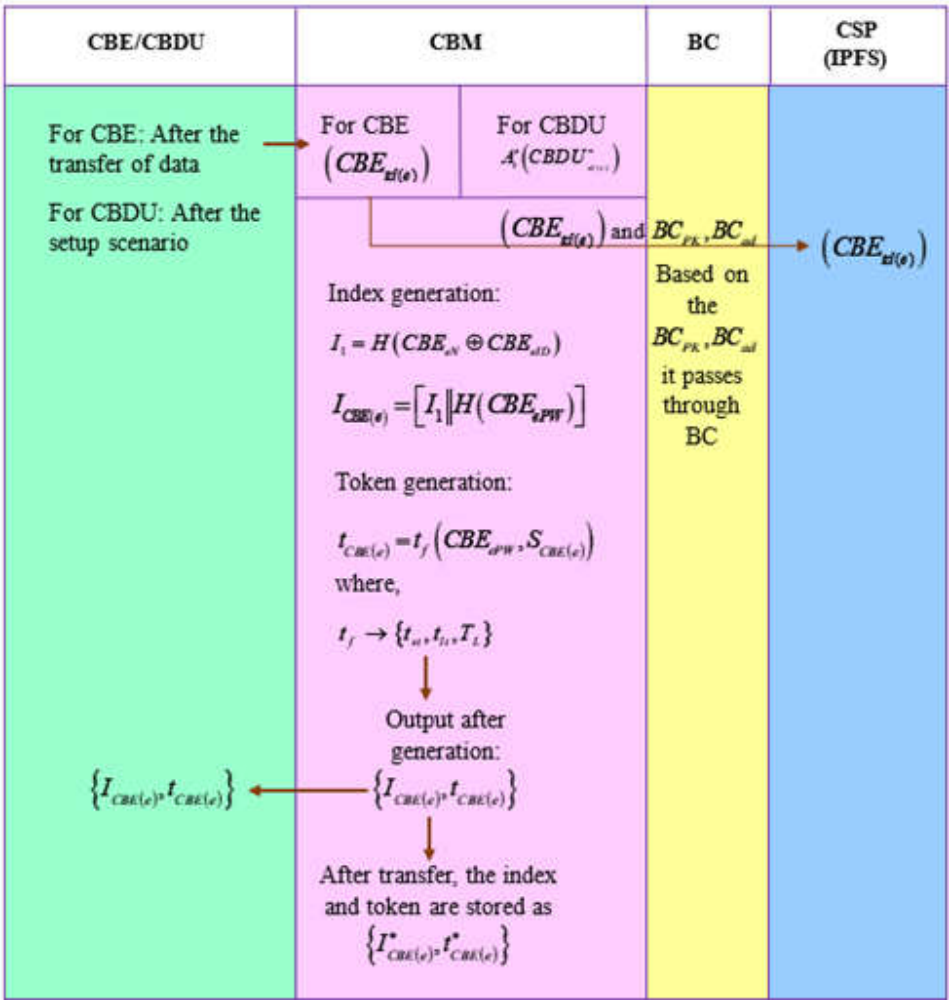


Figure 4.1.3. Diagrammatic depiction of the Index and token generation process [20]

4.1.4. Improved Elliptic Curve Cryptography based Quantum Key Distribution for encryption

After transferring the outcomes from the index and token generation process to the CBE/CBDU, the subsequent owner's data $\left(CBE_{td(e)}\right)$ is forwarded to CSP using the BC_{PK}, BC_{ad} for performing the encryption process. The IECC-QKD is utilized as the encryption standard that overcomes the issues of traditional ECC mechanism like exposure to quantum threats, vulnerability to random values leading to leakage of the private key, and spamming the system with a large volume of transactions with misleading the legitimate user's transactions. Moreover, to mitigate the computational complexity, the ECC is improved with the utilization of different curves by introducing additional randomness and QKD. The IECC algorithm uses elliptic curves over finite fields. Generally, the ECC algorithm produces curve based on the Weierstrass form. However, to improve time complexity and to minimize processing, this curve is replaced by implementing the Edward's curve [22] which performs well compared to the other conventional elliptic curves. The equation, implying the standard Edward's curve is described as,

$$E_d(k): a^2 + b^2 = z^2\left(1 + la^2b^2\right) mod\ kz \qquad (1)$$

where, $E_d(k)$ denotes the Edward's curve at the field k . The point coordinates of curve are denoted as a,b and z,l denote the parameters that contribute to Edward's form $z,l \in k$. Every elliptic curve over the particular finite field k is birationally mapped to the curve. The improved

curve in the IECC algorithm [21] performs deliberately well by improving the performance of the algorithm and minimizing key size when compared to other encryption standards. Using the IECC as encryption standard involves generating sequences using the curve points to generate the cipher text for efficient data encryption.

Step 1: The CBM chooses random value x through the IECC algorithm and computes them accordingly with the point zK.

$$K_1(a_1, b_1) = r_1 K \tag{2}$$

$$K_2(a_2, b_2) = K_y + r_1(zK) \tag{3}$$

Here, the K implies the point generator that generates finite fields K_1, K_2 along the points (a_1, b_1) and (a_2, b_2). r_1 denotes the random integer initialized to generate the secret key, and K_y denotes the embedded form of the original data.

Step 2: The single random integer with a pair of points can diminish the security concerns leading to cipher text attacks. To overcome this, another random integer r_2 is added to the IECC scheme to improve the encryption.

$$K_3(a_3, b_3) = r_2 K \tag{4}$$

$$K_4(a_4, b_4) = K_y + r_2(zK) \tag{5}$$

Here, K_3, K_4 denotes the finite fields along the points (a_3, b_3) and (a_4, b_4).

Step 3: Generate the set of sequences for the points using the shifting operation

Step 4: Calculate $W(a_1, b_1), W(a_2, b_2), W(a_3, b_3)$, and $W(a_4, b_4)$ where W represents the values of the sequence generated through Step 3.

Step 5: Following the sequence, the cipher text is measured as $T_c = \{W(a_1, b_1), W(a_2, b_2), W(a_3, b_3), W(a_4, b_4)\}$, where T_c denotes the cipher text calculated using IECC.

The CSP, also the encryptor converts the T_c into the binary form and sends it inside the storage space with a series of bits attained through QKD. The integration of QKD with IECC provides reliable and advanced security methods using quantum keys and defends abnormalities through quantum computing devices at the same time. Through QKD [23] the two participants CBM and CSP create secret keys by using fundamental quantum physics rules of superposition and entanglement. The protocols of QKD operate on random qubit transmission through quantum space, where CSP sends the qubit-generated key through a specific channel When CSP receives the key from CBM it identifies them with randomly generated testing bases. When CBM and CSP establish the basis values publicly by discarding mismatches and creating the raw key which is then processed further into a shared secret key. The transmission method finds users who try to steal and avoid eavesdropping attempts by indication of quantum signals E_{QKD} since state variations automatically reveal their presence. The E_{QKD} is the indication parameter used by the QKD to notify whether any intruder interrupts the quantum channel. The operations at the QKD can be determined as,

$$CBM : T_c \xrightarrow{QKD} CSP \tag{6}$$

$$QKD \rightarrow E_{QKD} = \begin{cases} 1; if\ attac\ker present \\ 0; else \end{cases} \tag{7}$$

The secret keys shared through QKD [24] become a stronger standard and can be used as a symmetric key for encryption. The key generation through QKD serves either to encrypt IECC public keys or to collaborate with IECC by managing safe access to keys. Uniting these security strategies makes better protection and suitable for resource-constrained environments. The combined approach offers benefits with IECC's security enhanced by QKD integration. QKD

ensures quantum-resistant protection while IECC provides an additional layer of backup security compared to other cryptographic techniques. The usage of IECC in the proposed system becomes faster due to its smaller keys that reduce processing requirements. The mixed characteristics will persist in serving our needs as quantum technology makes current encryption methods no longer secure. QKD distributes secret keys securely between parties and supports IECC to develop better encryption and digital key handling. IECC defends the system from both side-channel attacks and other vulnerabilities and protects key exchange operations from hackers using QKD. Similarly, after this process, the decryption process uses z,l with base point K and the prime value k are transferred to the CBE/CBDU whoever is the data owner and the encrypted data is stored on the IPFS network. Figure 4.1.4. represents the encryption process carried out using the IECC-QKD model.

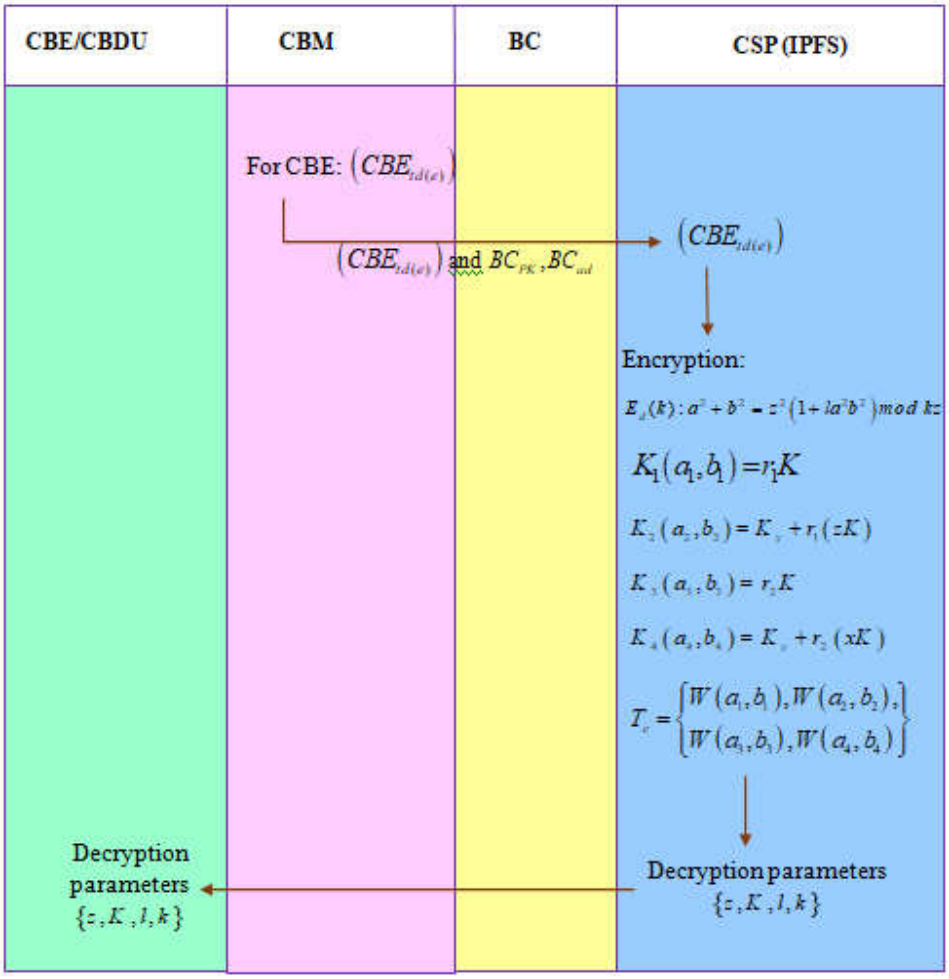


Figure 4.1.4. Schematic depiction of IECC-QKD-based encryption process

4.1.5. Decryption of data

The user authenticates the data through the CSP scheme, for retrieval using the two-factor authenticator mechanism called the index and token. The verifier CBM checks the subsequent index and token, if the authentication matches, the decryption is performed through CSP with the recovery of key from CBE utilizing QKD's channel. The steps carried out for decrypting the data are as follows.

Step 1: For decryption, the CBDU applies encrypted data T_c and the decryption parameters $\{z, K, l, k\}$ which are known to the CBDU through CSP.

Step 2: The known data is converted back to the binary form by transforming T_c of every group.

Step 3: The groups $\{W(a_1,b_1),W(a_2,b_2),W(a_3,b_3),W(a_4,b_4)\}$ are extracted according to the initialization of the groups.
Step 4: Reverse the set of sequences through the operation by circular shift.
Step 5: The sequences set are converted back to the decimal values and stored as g.
Step 6: The pre-arranged point $(g+1)K$ and the point that is stored $(g+1)K=(a_1,b_1)$ is calculated.
Step 7: The next set of points in the sequence of step 3 repeats the same process for the generated sequences $\{W(a_1,b_1),W(a_2,b_2),W(a_3,b_3),W(a_4,b_4)\}$.
Step 8: The process is repeated throughout the next sets of data that the T_c possess and not measured previously.
For the calculation of K_y, that is mentioned in the (14) and the (16), the CSP uses the secret key and measures the $r_1(zK)$ and $r_2(zK)$ to acquire the K_y.

$$K_y + r_1(zK) - z(r_1K) = K_y + r_1zK - r_1zK = K_y \quad (8)$$

$$K_y + r_2(zK) - z(r_2K) = K_y + r_2zK - r_2zK = K_y \quad (9)$$

Following, this the process is reversed using the embedding K_y to decipher and retrieve the original data. Figure 4.1.5. illustrates the decryption process for the retrieval of the original data.

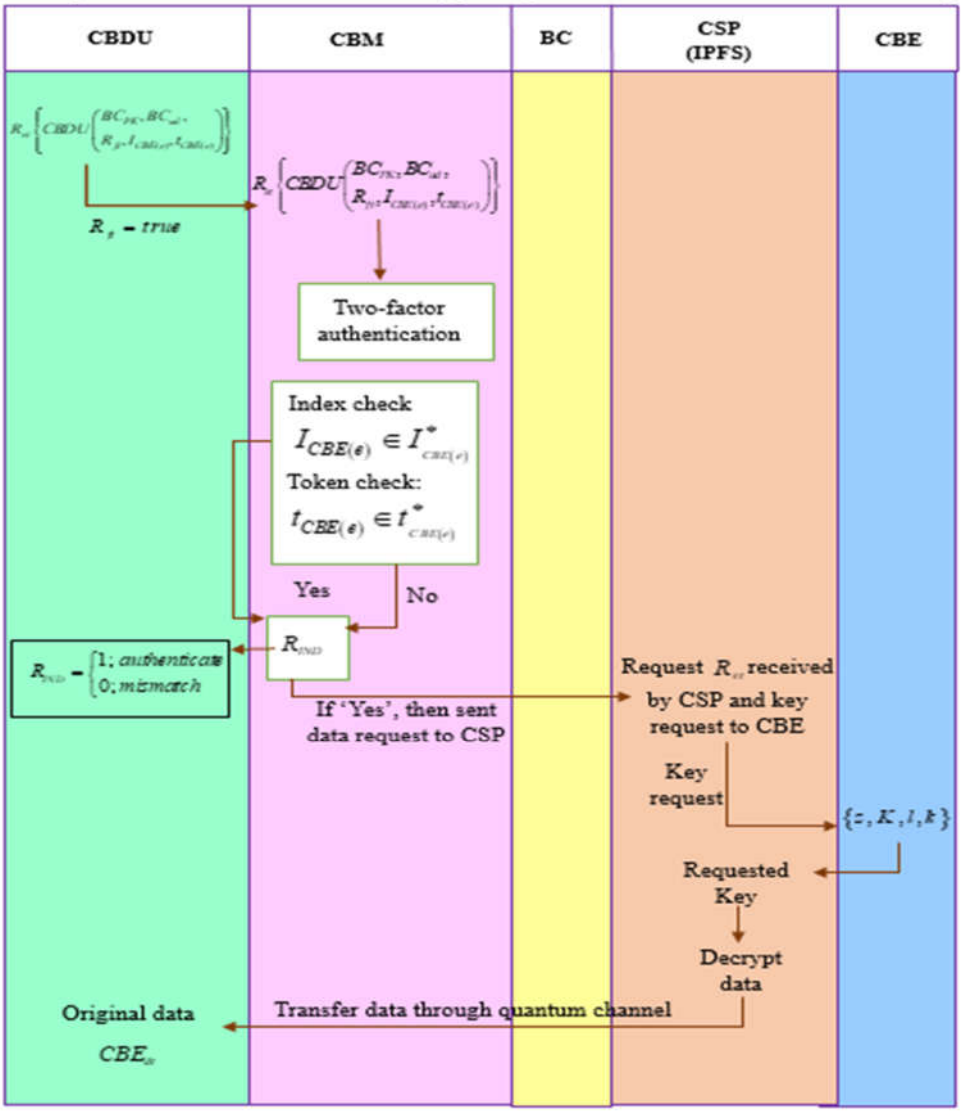


Figure 4.1.5. Schematic diagram of the decryption process and the original data transfer

5. Comparative Methods

The blockchain-based IECC-QKD framework is compared against other established data security and access control methods like CP-ABE [1], Fabric-ABAC [6], BCAC [8], BPADAC [4], BPDAC [2], AccessChain [4], and the ISSO-Based PF-MLP [3] considering the 50,100,150,200, and 250 users respectively.

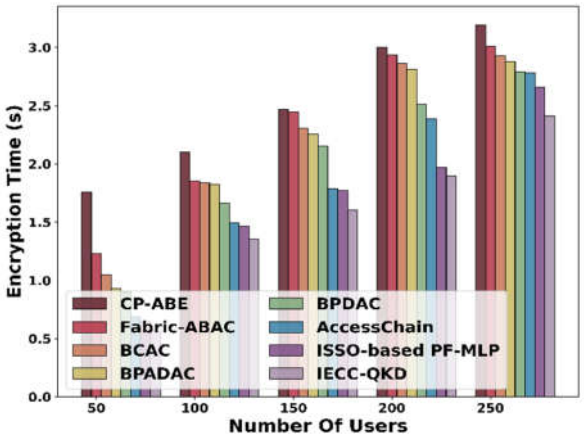
5.1. Comparative Analysis

Figure 5.1. illustrates the comparison of evaluation analyzed against other established methods across different users. The aforementioned metrics are derived as a standard to measure the effectiveness of the model. The encryption time necessitated by the IECC-QKD for encrypting the data of the 250 users is 2.41s which is far better with gaining margins of 0.78s by CP-ABE, 0.60s by Fabric-ABAC, 0.52s by BCAC, 0.47s by BPADAC, 0.38s by BPDAC, 0.37s by AccessChain, and 0.25s by the ISSO-Based PF-MLP.

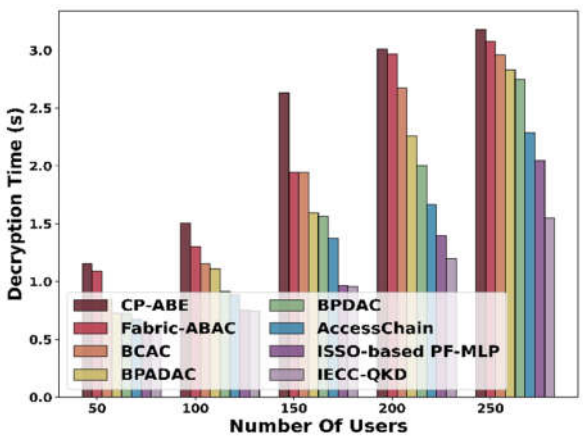
Similarly, for decrypting the data the IECC-QKD requires very less time of 1.55s, that is shorter in terms of decryption time of other methods over 1.63s of CP-ABE, 1.53s of Fabric-ABAC, 1.41s of BCAC, 1.28s of BPADAC, 1.20s of BPDAC, 0.74s of AccessChain, and 0.50s of ISSO-Based PF-MLP. The transaction time needed for the proposed framework for the exchange of data is 5.42s which outperforms other models like CP-ABE, Fabric-ABAC, BCAC, BPADAC, BPDAC, AccessChain, and the ISSO-Based PF-MLP with the ranges of 4.58s, 1.98s, 1.66s, 1.52s, 1.28s, 1.25s, and the 1.13s.

The privacy ratio achieved by the IECC-QKD for maintaining the authentication and secure transfer is 0.74 which is longer when compared to 0.50 of CP-ABE, 0.52 of Fabric-ABAC, 0.52 of BCAC, 0.54 of BPADAC, 0.58 of BPDAC, 0.62 of AccessChain, and 0.65 of ISSO-Based PF-MLP. The proposed framework attained a responsiveness of 8.50s, which is reduced when compared with other baseline methods achieving a time difference of 2.63s, 1.94s, 1.91s, 1.90s, 1.61s, 1.47s, and 1.31s over CP-ABE, Fabric-ABAC, BCAC, BPADAC, BPDAC, AccessChain, and the ISSO-Based PF-MLP.

Finally, for the memory usage metric, the energy consumed by the proposed IECC-QKD is 430.88 KB, which is minimized by attaining a difference of CP-ABE with 59.62KB, Fabric-ABAC with 55.04KB, BCAC with 53.10KB, BPADAC with 49.07KB, BPDAC with 32.66KB, AccessChain with 29.49KB, and the ISSO-Based PF-MLP with 13.98KB, respectively.



Encryption time(s)



Decryption time (s)

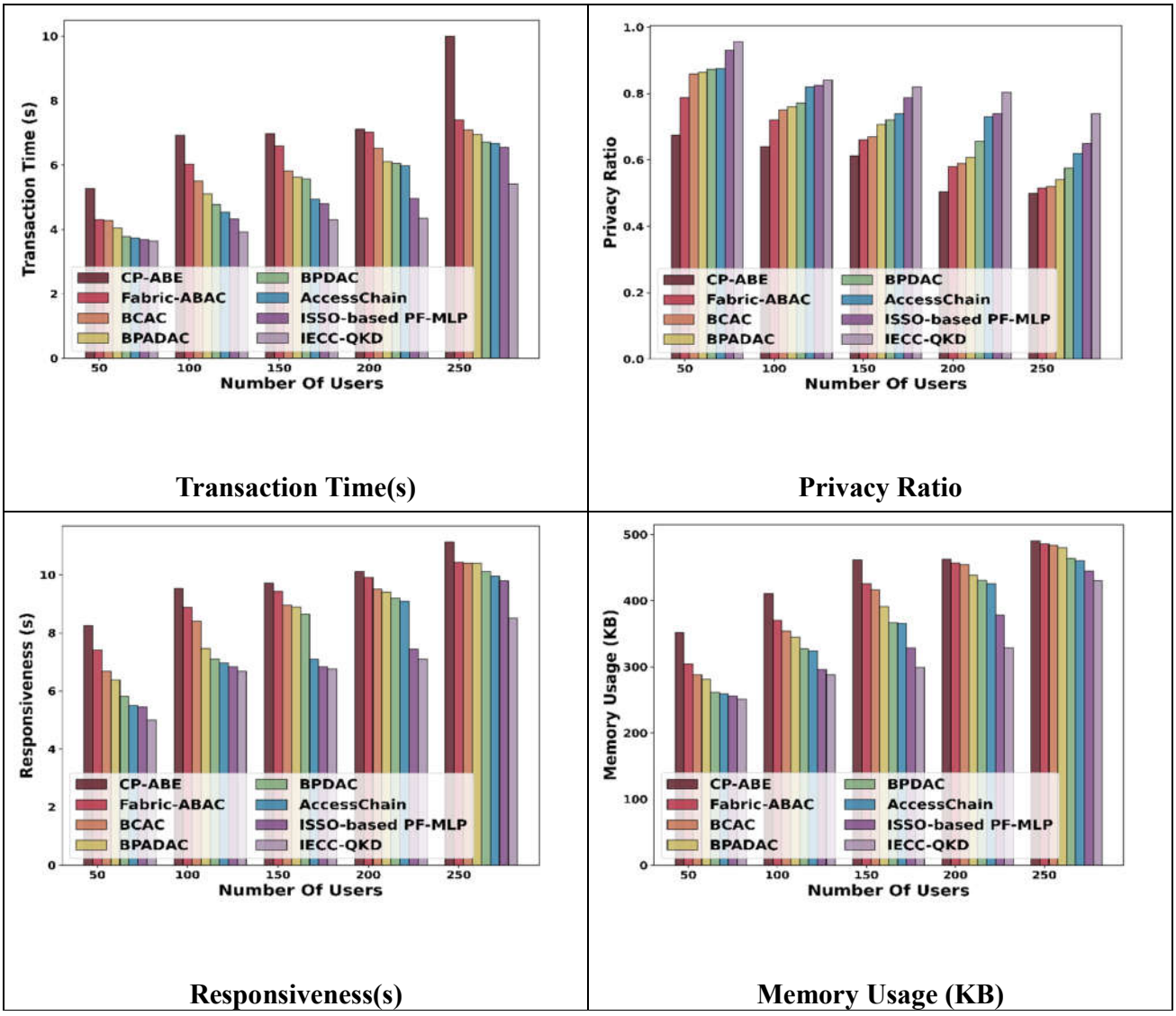


Figure 5.1. Comparison of IECC-QK performance with existing approaches

5.2. Statistical Analysis

The statistical analysis for the IECC-QKD-based framework is evaluated by analysing both the curves with existing methods. The aforementioned metrics are utilized and the best, mean and variance are measured to highlight the overall efficiency of the proposed framework.

5.2.1. Statistical results based on the Curve Analysis

The curve analysis-based statistical results demonstrate the IECC-QKD-based model's efficacy over the elliptic curve variants like secp192r1-IECC-QKD, secp224r1-IECC-QKD, brainpoolP256r1-IECC-QKD, and brainpoolP224r1-IECC-QKD. Table 5.2.1. outlines the outcomes of the proposed frameworks when analysed with different curves of IECC.

Table 5.2.1. Statistical Analysis based on the Curves

	Curves / Metrics	secp192r1-IECC-QKD	secp224r1-IECC-QKD	brainpoolP256r1-IECC-QKD	brainpoolP224r1-IECC-QKD	**Proposed IECC-QKD**
Best	*Encryption time (s)*	3.08	2.91	2.76	2.75	**2.41**
	Decryption time (s)	3.19	3.00	2.86	2.44	**1.55**
	Transaction time (s)	10.00	6.85	6.64	6.57	**5.42**
	Privacy Ratio	0.76	0.85	0.88	0.94	**0.96**
	Responsiveness (s)	10.63	9.93	9.90	9.82	**8.50**
	Memory Usage (KB)	496.50	478.94	454.41	439.74	**430.88**
Mean	*Encryption time (s)*	2.41	2.21	2.03	1.78	**1.57**
	Decryption time (s)	2.43	1.94	1.74	1.38	**1.01**
	Transaction time (s)	6.99	5.35	5.16	5.05	**4.33**
	Privacy Ratio	0.64	0.70	0.74	0.79	**0.83**
	Responsiveness (s)	9.40	8.53	8.22	7.88	**6.81**
	Memory Usage (KB)	417.25	393.67	377.51	353.47	**319.69**
Variance	*Encryption time (s)*	0.36	0.45	0.60	0.60	**0.38**
	Decryption time (s)	0.39	0.50	0.54	0.34	**0.11**
	Transaction time (s)	2.55	1.39	1.13	1.16	**0.37**
	Privacy Ratio	0.006	0.011	0.008	0.007	**0.005**
	Responsiveness (s)	1.27	1.05	1.25	1.44	**1.25**
	Memory Usage (KB)	4461.77	4652.44	4480.54	3567.66	3713.75

5.2.2. Statistical analysis based on comparing methods

Table 5.2.2. refers to the outcomes achieved by the IECC-QKD-based framework against other conventional data authentication and access control approaches. The statistical results of the proposed method show that the model achieves profound results in terms of security and efficiency.

Table 5.2.2. Statistical Analysis based on comparing existing approaches

	Methods / Metrics	CP-ABE	Fabric-ABAC	BCAC	BPADAC	BPDAC	Access Chain	ISSO-Based PF-MLP	**Proposed IECC-QKD**
Best	*Encryption time (s)*	3.19	3.01	2.93	2.88	2.79	2.78	2.66	**2.41**
	Decryption time (s)	3.18	3.08	2.96	2.83	2.75	2.29	2.05	**1.55**
	Transaction time (s)	10.00	7.40	7.09	6.95	6.70	6.68	6.55	**5.42**
	Privacy Ratio	0.68	0.79	0.86	0.86	0.87	0.88	0.93	**0.96**
	Responsiveness (s)	11.13	10.44	10.41	10.40	10.11	9.97	9.81	**8.50**
	Memory Usage (KB)	490.50	485.92	483.98	479.95	463.54	460.37	444.86	**430.88**
Mean	*Encryption time (s)*	2.51	2.29	2.20	2.14	2.00	1.83	1.70	**1.57**
	Decryption time (s)	2.30	2.08	1.92	1.70	1.59	1.38	1.16	**1.01**
	Transaction time (s)	7.26	6.27	5.84	5.56	5.38	5.17	4.86	**4.33**
	Privacy Ratio	0.59	0.65	0.68	0.70	0.72	0.76	0.79	**0.83**
	Responsiveness (s)	9.75	9.22	8.79	8.51	8.18	7.72	7.27	**6.81**
	Memory Usage (KB)	435.63	408.58	399.32	387.02	369.87	366.98	340.55	**319.69**
Variance	*Encryption time (s)*	0.29	0.46	0.49	0.52	0.45	0.53	0.43	**0.38**
	Decryption time (s)	0.67	0.68	0.68	0.58	0.54	0.33	0.27	**0.11**
	Transaction time (s)	2.34	1.17	0.91	0.95	1.03	1.09	0.91	**0.37**
	Privacy Ratio	0.005	0.009	0.014	0.013	0.010	0.008	0.009	**0.005**
	Responsiveness (s)	0.86	1.09	1.55	2.03	2.34	2.58	2.03	**1.25**
	Memory Usage (KB)	2402.07	4174.36	4979.95	4887.96	5236.39	5121.51	4323.16	**3713.75**

5.3. Comparative Discussion

For the secured transmission of data and for ensuring effective access controls, several approaches have been implemented with each possessing their merits and also complications. The CP-ABE [1] uses attributes for secure access control but lacks scalability and efficiency with the protection of IoT data. However, with the instinct of deploying different mechanisms the Fabric-ABAC [6] has been developed, however, it produced better results in terms of secure data access but failed to allow the system for data sharing in cross-domain. The BPADAC [4] and BPDAC [2] frameworks designed based on blockchain networks enhanced the usage of decentralized systems for storage and transparency, still, the blockchain frameworks did not ensure the privacy concerns by determining the techniques of cryptography. The AccessChain [4] framework based on the ABE addressed the privacy-related consequences of accessing data but

comprised their performance on the time constraints, latency, and maintenance of ledgers. The ISSO-based PF-MLP [3] introduces optimization strategies for generating random numbers for secret keys, that increase the safeguarding of data, however, the framework faces issues with the encryption, leading to threats. The proposed IECC-QKD-based framework strives to overcome these challenges by improving the existing ECC encryption, along with the utilization of QKD that restricts the intruders with quantum-resistant and tamper-proofing sensitive data. The improved curve and the multiple randomness in the framework ensure secured transmission and boost data security. The overall IEC-QKD-based blockchain framework provides a robust, secure, and future-proof solution for data exchange and storage. Table 5.3. represents the outcomes obtained by the IECC-QKD framework when compared with other established approaches.

Table 5.3. Comparative discussion table of the IECC-QKD

	Methods / Metrics	CP-ABE	Fabric-ABAC	BCAC	BPADAC	BPDAC	Access Chain	ISSO-Based PF-MLP	**Proposed IECC-QKD**
For 250 Users	*Encryption time (s)*	3.19	3.01	2.93	2.88	2.79	2.78	2.66	**2.41**
	Decryption time (s)	3.18	3.08	2.96	2.83	2.75	2.29	2.05	**1.55**
	Transaction time (s)	10.00	7.40	7.09	6.95	6.70	6.68	6.55	**5.42**
	Privacy Ratio	0.50	0.52	0.52	0.54	0.58	0.62	0.65	**0.74**
	Responsiveness (s)	11.13	10.44	10.41	10.40	10.11	9.97	9.81	**8.50**
	Memory Usage (KB)	490.50	485.92	483.98	479.95	463.54	460.37	444.86	**430.88**

6. Conclusion

The increasing dependence on cloud servers for data storage has escalated demands for enhanced control and autonomous management of personal data access. Existing static access control models are inadequate for addressing these evolving dynamic requirements. To mitigate these concerns, this study proposes a framework that integrates Improved Elliptic Curve Cryptography-based Quantum Key Distribution (IECC-QKD) with blockchain technology to fortify data storage and access control in cloud systems. The IECC mechanism employed in the framework generates cryptographic keys utilizing multiple sources of randomness and leverages Edwards's curves to prevent spam transaction attacks while strengthening security. Compared to conventional cryptographic methods, IECC achieves superior security guarantees with smaller key sizes. Coupled with QKD, this approach offers quantum-resistant protection. Furthermore, modifications to the Ethereum blockchain consensus protocol ensure immutable and tamper-resistant data storage, thereby safeguarding against unauthorized access. Performance evaluations conducted with user groups of 50, 100, 150, 200, and 250 demonstrate that the proposed framework attains an encryption time of 2.41 seconds, decryption time of 1.55 seconds, transaction time of 5.42 seconds, privacy ratio of 0.74, responsiveness of 8.50 seconds, and memory consumption of 430.88 KB for 250 users. Nevertheless, realizing the full potential of this integrated solution necessitates addressing challenges such as the requirement for specialized quantum hardware, complexity in system integration, limitations in key generation rates, and the current absence of standardized protocols in future research efforts. [27]

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.e6383.

[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.

[27] Agrawal, Akshay, et al. "Quantum Key-Based Blockchain Access Control: A Secure Authentication and Data Exchange Framework for Cloud Environments."