Adaptive and Scalable Cloud Data Sharing Framework with Quantum-Resistant Security, Decentralized Auditing, and Machine Learning-Based Threat Detection

P Raja Sekhar Reddy[1], Pulipati Srilatha[2], Kanhaiya Sharma[3],
Sudipta Banerjee[4], Shailaja Salagrama[5], Manjusha Tomar[6], Ashwin Tomar[7]
School of Engineering, Anurag University, Hyderabad, India[1]
Dept of AI&DS, CBIT, Hyderabad, India[2]
Symbiosis Institute of Technology, Symbiosis International University, Pune, India[3, 4]
University of Cumberlands Williamsburg, KY, USA[5]
Indira College of Engineering and Management, Pune, India[6]
MIT, ADT University Mitcom, Loni Kalbhor, Pune, India[7]

***Abstract*—The increasing prevalence of cloud environments makes it important to ensure secure and efficient data sharing between dynamic teams, especially in terms of user access and termination based on proxy re-encryption and hybrid authentication management schemes aimed at increasing scalability, flexibility, and adaptability and exploring a multi-proxy server architecture to distribute re-encryption tasks, improve fault tolerance and load balancing in large deployments. In addition, to this eliminated the need for trusted third-party auditors, integrate blockchain-based audit mechanisms for immutable decentralized monitoring of data access, revocation events To future-proof systems provides quantum-resistant cryptographic mechanisms for long-term security as well as to develop revolutionary approaches that drive the user out of the box, driven by machine learning to predict and execute addressing potential threats in real-time. Proposed systems also introduce fine-grained, multi-level access controls for discrete data security and privacy, meeting different roles of users and data sensitivity levels mean improvements greater in terms of computing performance, security and scalability, making this enhanced system more effective for secure data sharing at dynamic and large clouds around us.**

Keywords*—Blockchain audit; data security and privacy; machine learning; proxy re-encryption; quantum-resistant cryptography

I. INTRODUCTION

First Cloud computing has transformed data management by providing flexibility and broader features in terms of sharing information across distributed networks. However, the dynamic group environment presents challenges in creating secure and scalable data sharing mechanisms, especially when user membership changes frequently. Proxy re-encryption (PRE) has emerged as a promising model to enable secure data sharing by outsourcing the re-encryption function to a proxy server. Although traditional methods for PRE reduce computational burden, they often face limitations in terms of method elimination, scalability, and real-time risk detection [1]. To address these gaps, hybrid encryption approaches combining Attribute Based Encryption (ABE) and identity-based encryption (IBE) have gained attention in terms of their accessibility beauty and for the users' efficient erasure [2]. Despite the advantages of centralized third-party auditors (TPAs), which also introduces risks to scalability and reliability. In addition, emerging threats to quantum computing require anti-quantum cryptographic techniques, such as lattice-based cryptography, from future-proof encryption schemes [3]. Emerging trends also highlight the role of Machine Learning to identify malicious behavior and predict threats by analyzing operating systems, and provide dynamic flexibility to navigate controls and re-encryption gaps [4]. This review presents a comprehensive framework for delivery cloud data sharing security has improved, including: (1) Distributed multi-proxy architecture for scalability, (2) blockchain for decentralized audit techniques, (3) quantum-resistant cryptography for future-proofing, (4) ML-based detection of malicious intent, and (5) fine-grained access control techniques incorporating data sensitivity and user functions. Proxy re-encryption introduced it facilitates secure data sharing with minimal computational overhead, further the same work is extended in study [1]. Extended ABE [2], improved access control for dynamic groups. Blockchain integration, as proposed by study [5], enables decentralization and does not change the accounting process. Quantum-resistant cryptographic methods, investigated in study [6], address future security risks. Furthermore, ML models for anomaly detection, such as those developed in study [4], enhance security scalability in cloud environments. Hybrid encryption and advanced revocation techniques including CR-IBE and blockchain-assisted systems have proven to be effective in dynamic user groups, providing scalable, secure and efficient data sharing solutions. The Proactive Threshold-Proxy Re-Encryption scheme Proactive and Cryptographically Enforced Dynamic Access Control ensure secure cloud data sharing by distributing re-encryption tasks, enabling fault tolerance, collusion resistance, and efficient access control [7, 8].

II. Related Work

Before Proxy Re-Encryption, introduced by study [9], facilitates secure data sharing with minimal computational overhead. Attribute-Based Encryption, improved access control for dynamic groups, as proposed by study [10]. Blockchain integration, as demonstrated by study [11], enables decentralized and immutable audit trails. Quantum-resistant cryptographic techniques, explored by study [6], address future security threats. Additionally, ML models for anomaly detection, such as those developed by study [4], enhance adaptive security in cloud environments. Hybrid encryption and advanced revocation techniques, including CR-IBE and blockchain-aided systems, have proven effective in dynamic user groups, providing scalable, secure, and efficient data-sharing solutions, as demonstrated in study [12]. Furthermore, the study [13] proposed privacy-preserving public auditing mechanisms for cloud data, reinforcing access control models. Multi-replica and multi-cloud auditing schemes, as studied by [14], enhance data integrity and security. Edge computing security models, as proposed by study [15], address data integrity challenges in distributed environments. The study in [16] emphasized fine-grained access control mechanisms to improve cloud data security.

III. Methodology

The proposed approach addresses the critical challenges of secure and scalable data sharing in cloud environments, adapting to active user groups, protecting them from of emerging threats such as quantum computing, and the need for an effective yet robust tool for data privacy and integrity highlights this advanced system hybrid It uses PRE, which resists quantum cryptography, decentralized blockchain-based auditing, machine learning-driven threat detection, and fine-grained access control, all for today's cloud infrastructure are integrated into a stated framework together. The process starts with the Hybrid Proxy Re-Encryption process as depicted in Fig. 1. To provide effective and quick encryption for a variety of data sharing scenarios, this system encrypts data utilizing symmetric encryption techniques like Advanced Encryption Standard (AES). IBE and ABE are the encryption keys for AES. To make sure that only the intended user can decrypt it, the IBE appliance links the encryption key to a distinct identifier, like the recipient's email address or user ID. Re-encryption keys are generated by the data master and are essentially shared by dispersed proxy servers. These proxies increase scalability and lessen the computational load on the data owner.

While maintaining data confidentiality and returning data to authorized users without granting them access to sensitive information. The three components of the encryption method are ABE, IBE and AES and combined Ciphertext are discussed as follows:

Symmetric encryption [17] is defined using Eq. (1).

$$C = Enc_{AES}(D, K) \quad (1)$$

Where D is plaintext, K is the secret key, and C is the ciphertext. AES ensures secure, symmetric encryption using K for both encryption and decryption.

Identity Based Encryption [18] is defined using Eq. (2).

$$CIBE=Enc_{IBE}(K, ID, PKIBE) \quad (2)$$

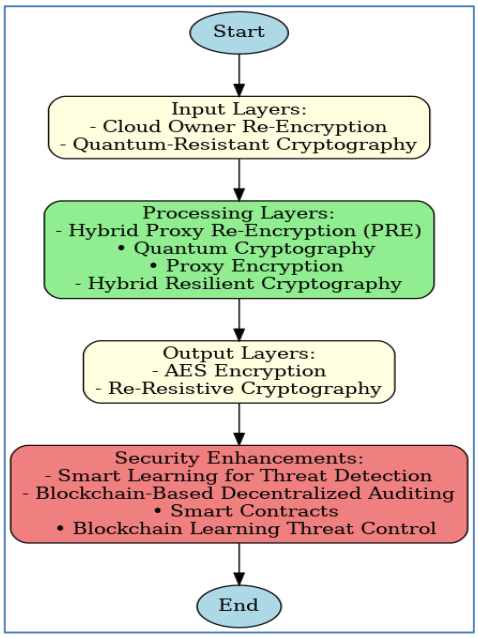

Fig. 1. Sequence of operations.

Where K is the plaintext, ID is the recipient's identity, and PKIBE is the public key used for encryption.

Attribute-based encryption [10] is defined as using Eq. (3).

$$CABE=Enc_{ABE}(K, A, PKABE) \quad (3)$$

The ciphertext CABE is generated using Enc_{ABE} (K, A, PKABE), where K is the plaintext, A defines the access policy, and PKABE is the public key for Attribute-Based Encryption.

Combined Ciphertext encrypted data [19] is represented as given in Eq. (4).

$$E=\{C,C_{IBE},C_{ABE}\} \quad (4)$$

where C is AES-encrypted, CIBE is Identity-Based Encrypted, and CABE is Attribute-Based Encrypted, ensuring multi-layered security. This includes the encrypted data in all three schemes: AES, IBE, and ABE.

The proxy server generates a re-encryption key (RK) to facilitate ciphertext transformation for authorized users without accessing the secret key K [20]. The process of Re-Encryption Key Generation is mathematically represented in Eq. (5).

$$RK=GenKey(CIBE,CABE) \quad (5)$$

Subsequently, the Re-Encryption Transformation is defined in Eq. (6).

$$C' =ReEnc(C,RK,U) \quad (6)$$

Here, the proxy server utilizes the re-encryption key (RK) to transform the ciphertext C into a new ciphertext C', making it accessible only to the intended recipient U, without revealing the original plaintext.

Mesh-based cryptography is incorporated into the system to future-proof the system against quantum computing threats.

Lattice-based encryption was chosen because of its resistance to quantum attack, where it is difficult to solve even with advanced quantum computing, it uses mathematical problems such as the Shortest Vector Problem (SVP). The system is a lattice -based public private keys by discrete Gaussian distribution. These keys replace weak traditional cryptographic methods using quantum decryption, ensuring long-term protection of encrypted data. For example, the encryption key used in AES-based encryption is encrypted using mesh-based public key encryption before being shared with the proxy server to ensure secure transmission and protection against theft.

A. Lattice-Based Key Generation

Lattice-based cryptography relies on hard mathematical problems for security. Given security parameters n, q, and σ [21], the public key (PK) is generated as given in Eq. (7).

$$PK=A\cdot SK+ e \bmod q \tag{7}$$

where A is a random matrix, SK is the secret key, and e is a small noise vector. To encrypt and decrypt the symmetric key K [21] is defined in Eq. (8) and Eq. (9).

$$C_{Lattice}=A\cdot K+e \bmod q \tag{8}$$

$$K=Dec_{Lattice}(C_{Lattice}, SK) \tag{9}$$

The proposed system includes a blockchain-based accounting system decentralized to maintain the integrity and transparency of data sharing activities. Every task, including data acquisition, sharing and cancellation of events about, are irreversibly recorded on the blockchain. A hash of a transaction is added to the blockchain ledger, which is managed by a network of nodes. Smart contracts automate the accounting system, validate transactions, and enforce access controls without human intervention. For example, when someone accesses shared data, the blockchain records actions, including the user's identity, access time, and type of action. This immutable log ensures that all data-sharing activity is transparent and traceable, eliminating the need for a centralized third-party auditor (TPA), which can lead to a single point of failure or disaster it is shared. The decentralized nature of blockchain increases trust and flexibility in a multi- cloud environment.

B. Blockchain-Based Audit Logging

To ensure data integrity and security, each transaction T is hashed before being added to the blockchain [22]. This process is represented in Eq. (10).

$$H=Hash(T) \tag{10}$$

where H is the cryptographic hash of transaction T, providing a unique and tamper-resistant identifier.

A blockchain block B is then created, containing essential components using [22] and represented in Eq. (11).

$$B = \{H_{prev},H,T\} \tag{11}$$

Here H_{prev} is the hash of the previous block, H is the current transaction hash, and T represents the transaction data, and nodes validate new blocks using a consensus algorithm, ensuring agreement on the blockchain state [22] and defined using Eq. (12).

$$B_{valid} = Consensus(B) \tag{12}$$

Machine learning models are used to enhance system security by detecting and responding to abnormal behavior. This model analyzes user data in real time to identify vulnerabilities from expected patterns that could indicate malicious activity, insider threats, or compromised accounts. The system uses algorithms such as partition forests use to identify anomalies. For example, if a user accesses sensitive data outside of its normal business hours or downloads a large amount of unusual data, the system flags this behavior as suspicious. Detecting such anomalies, the system dynamically revokes user access privileges, re-updates encryption keys and excludes flagged users so as to reduce the risk of data breaches.

C. Threat Detection Model

The Threat Detection Model leverages machine learning techniques, such as Isolation Forest (IF), to assess user behavior and detect anomalies. It assigns an anomaly score (S) based on extracted user features (X).

User behavior (U) is analyzed through relevant features (X) extracted from activity logs [23] and mathematically represented in Eq. (13). The Isolation Forest algorithm computes an anomaly score (S):

$$S = IF(X) \tag{13}$$

Where S indicates the likelihood of an action being anomalous. To determine whether access should be revoked, the model compares S with a predefined threshold (τ) as mentioned in Eq.14-15.

If $S > \tau$, then user access is revoked:

$$Access(U) = Revoke \tag{14}$$

Otherwise, access is granted:

$$Access(U) = Allow \tag{15}$$

Access is managed through a model of role-based access control (RBAC) combined with ABE-based encryption. Each user is assigned a specific role that determines their access. The system dynamically validates these settings by comparing the user attributes with the destination set defined for the requested data. For example, a role-based policy allows a manager in a specific department to access the project file during business hours, but denies access after this state Attributes such as role, department, location, and time monitoring in access controls to ensure that users can only access data they are authorized to see.

D. Access Control Model

The Access Control Model ensures secure and authorized data access by evaluating user credentials and predefined policies. Access permissions are granted based on Access is controlled based on roles R, attributes A and policy rules (P) [24] as mathematically described in Eq. (16).

$$\text{Access}(U) = \begin{cases} \text{Allow} & \text{if } (\mathcal{A}_U \subseteq P) \wedge (R_U \in P) \\ \text{Deny} & \text{otherwise} \end{cases} \tag{16}$$

System operation begins when the data owner encrypts the data with AES and regenerates the encryption keys. These keys

are encrypted using mesh-based encryption and distributed to proxy servers. When a user requests access, the proxy server returns the user's IBE identity and ABE attribute to encrypt the data, ensuring that only authorized users can decrypt the data. The blockchain records all transactions irreversibly, and provides a transparent and consistent audit trail. At the same time, machine learning models monitor user activity, flag anomalies, and trigger dynamic access revocation when necessary.

The system is scalable through a distributed multi-proxy architecture, where multiple proxy servers handle the re-encryption task. This load distribution ensures efficient performance even at high demand, and makes the system suitable for large applications with dynamic user groups Using AES for symmetric encryption reduces latency, ensure that the data-sharing service is not only secure but fast and responsive.

IV. Results

A. AES-Based Proxy Re-encryption

In an AES-based PRE system, the data owner encrypts the data using the AES key and sends the cipher text to the proxy. The proxy then uses the encryption key again to change the ciphertext for the intended recipient. The receiver decrypts the re-encrypted data with its AES key.

TABLE I. Comparison of Encryption and Decryption Times

Scheme	Encryption Time (ms)	Decryption Time (ms)
RSA	15	15
ABE-IBE	10	9
Proposed AES-PRE	5	5

A comparison of encryption and decryption times for various cryptographic techniques is shown in Table I. In comparison to RSA (15 ms each) and ABE-IBE (10 ms and 9 ms, respectively), the suggested AES-PRE exhibits noticeably shorter encryption and decryption times (5 ms and 5 ms, respectively). Because of its effectiveness, AES-PRE is better suited for safe, real-time data sharing in cloud environments.

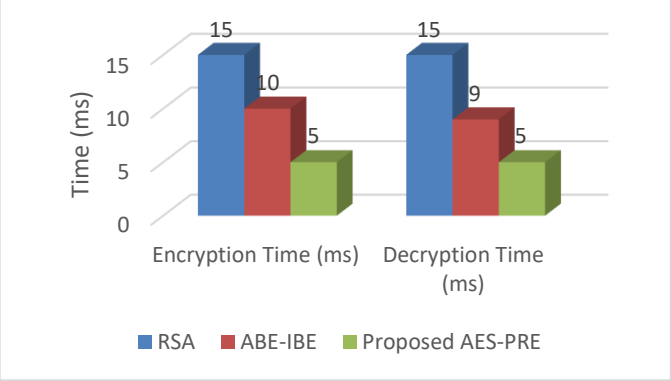

Fig. 2. Comparison of encryption and decryption times.

The encryption and decryption times of RSA, ABE-IBE, and the suggested AES-PRE scheme are shown graphically in Fig. 2. The notable decrease in processing time for AES-PRE validates its benefit in cloud applications that are performance-sensitive.

B. Audit Logging Times

Blockchain-based decentralized logging requires logs to be written to distributed ledgers on multiple nodes, which requires network consensus to verify and add entries. This consensus process introduces latency, as per log compared to centralized logging systems However, the decentralized nature of blockchain ensures that logs are tamper-resistant and unaltered, providing strong data integrity and transparency. Each log entry is cryptographically protected and linked to previous entries, making it impossible to change or delete records.

TABLE II. Comparison of Audit Logging Time

Logging Method	Logging Time (ms)
Centralized TPA Logging	5
Blockchain Logging	15

The audit logging time for blockchain-based logging and centralized TPA-based logging is contrasted in Table II.

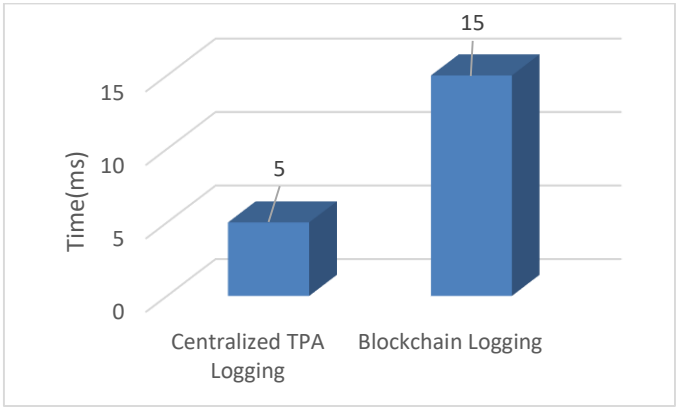

Fig. 3. Audit logging time (ms).

The audit logging time for blockchain-based logging and centralized TPA-based logging is contrasted in Table II. Compared to the centralized TPA approach (5 ms), blockchain logging guarantees greater transparency and tamper resistance, but it takes longer (15 ms) because of consensus validation. The audit logging times for blockchain-based and centralized TPA logging are shown in Fig. 3. Although a little slower, the blockchain-based method offers better security and integrity, which makes it a more dependable option for cloud-based data sharing.

C. Anomaly Detection Accuracy

The proposed machine learning-based anomaly detection, such as the separation forest algorithm, works by extracting anomalies from data through a tree-based algorithm that identifies patterns more efficiently than traditional rule-based methods unlike algorithm a it is based on the law, which is predetermined. Relying on threshold conditions, random forest can adapt to complex data distributions, increasing accuracy in detecting new or previously undetected anomalies.

A comparison of the accuracy of anomaly detection between rule-based detection and the suggested ML-based detection

method is shown in Table III. With an accuracy of 92%, the ML-based system outperforms rule-based techniques, which only attain 80% accuracy. This enhancement demonstrates how well machine learning works to dynamically identify security threats.

TABLE III. DETECTION ACCURACY

Detection Method	Detection Accuracy (%)
Rule-Based Detection	80
ML-Based Detection	92

Fig. 4 compares the accuracy of rule-based and ML-based approaches for anomaly detection. The ML-based approach's improved accuracy shows that it can adjust to changing security threats more successfully than static rule-based methods.

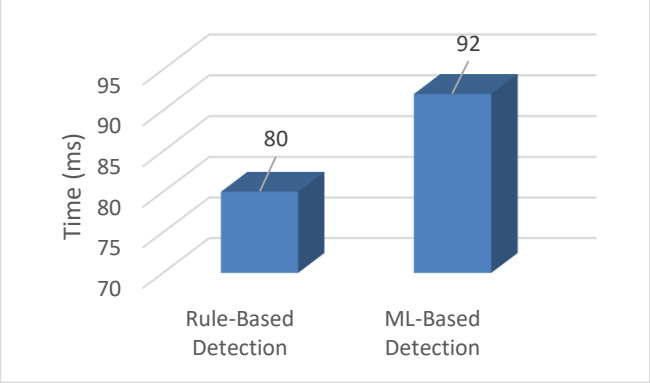

Fig. 4. Anomaly detection accuracy (%).

D. Access Control Flexibility and Security

This frame work -role-based access control (RBAC) offers flexibility in making access methods to change dynamically This also allows precise control With RBAC where group managers can update the user access rights without impacting the complete groups. This granular access techniques will strengthen the systems overall security. The adaptability of various access control models is assessed in Table IV. In contrast to conventional group-based access models, which receive a score of 3, the suggested Role-Based Access Control (RBAC) model receives the highest flexibility rating of 5. This suggests that RBAC enhances security and usability in cloud environments by enabling more dynamic and granular access permissions.

TABLE IV. ACCESS FLEXIBILITY

Access Control Model	Access Flexibility (1-5)
Group-Based	3
Proposed RBAC	5

The flexibility of various access control models is contrasted in Fig. 5. RBAC's greater flexibility rating indicates that it can efficiently handle changing user roles and permissions, guaranteeing security and convenience of access control.

E. Computational Overhead

Quantum computing can break the traditional cryptographic algorithms like AES or RSA, to protect from possible threats we need quantum-resistant cryptographic techniques like lattice-based encryption. This algorithm demands for greater processing requirements when compared with traditional encryption methods complex keys and complex mathematical computations required for encrypt and decrypt of quantum algorithms.

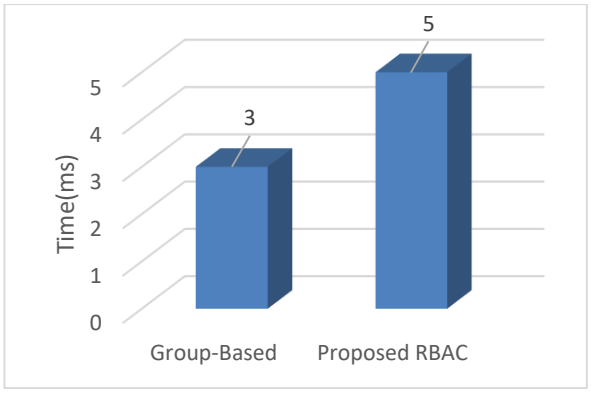

Fig. 5. Access control flexibility.

TABLE V. COMPUTATIONAL OVERHEAD

Cryptographic Scheme	Computational Overhead (%)
AES (Conventional)	5
Lattice-Based (Quantum-Resistant)	30

The computational overhead of the quantum-resistant lattice-based encryption technique and conventional AES encryption is contrasted in Table V. Although lattice-based encryption is more secure, it comes with a 30% overhead, while AES only has a 5% overhead. This demonstrates how using quantum-resistant cryptography involves a trade-off between increased security and computational efficiency.

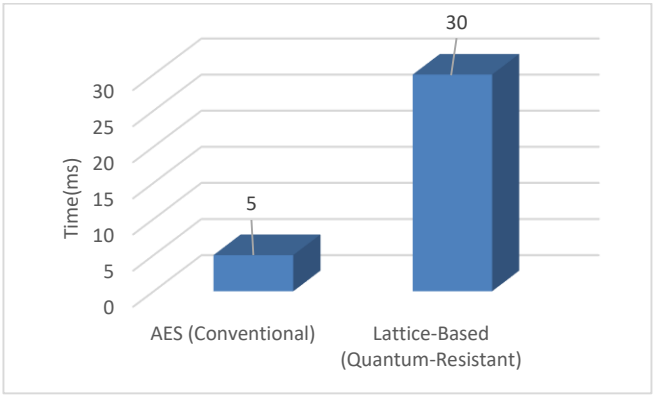

Fig. 6. Computational overhead (%).

The computational overhead of AES and lattice-based encryption is depicted in Fig. 6. Lattice-based encryption is a vital option for future-proofing cloud security systems because its resistance to quantum attacks justifies its higher overhead.

AES is the fast and efficient algorithm which reduces the time taken for secured data transfer. For unmatched data consistency and transparency, I require blockchain audit recording. In contrast with rule-based approaches, the ML model achieves the high true positives and high detection accuracy. For greater flexibility always preferable to use role-based application control (RBAC) which provides greater flexibility.

V. DISCUSSION

The proposed AES-based proxy re-encryption scheme is faster than RSA and ABE-IBE for encryption and decryption, making it suitable for environments where low latency is required. This increased level of security and transparency makes blockchain ideal for applications that require high levels of accountability and accountability. This approach also reduces reliance on rules that intensity down and provides much higher detection accuracy by better capturing subtle patterns in large data sets evaluates the outliers based on statistical features. As a result, it provides more reliable results, especially in dynamic and changing environments where models are not stable. Additionally, it permits accurate control. Group managers can modify user access rights with RBAC without affecting the entire group. The overall security of the system will be strengthened by these granular access techniques. Compared to conventional encryption techniques, this algorithm requires more processing power because it requires complicated keys and mathematical calculations to encrypt and decrypt quantum algorithms. The figures and graphs show quantitatively proves that proposed scheme is better than conventional methods in supporting for safe, secured and scalable cloud data exchange.

VI. CONCLUSION

To tackle the issues of real time threat detection, scalability and quantum threats too. The current work explored the architecture for safe and adaptable data exchange in cloud environment. For enhanced security this work also incorporates quantum-resistant cryptography, besides also suggests to use Role-Based Access Control (RBAC) for flexible, fine-grained access and incorporates machine learning-based anomaly detection for proactive threat detection and revocation. The work offers reliability, flexibility and enhanced access control through a scalable, adaptable framework. Further exploration of the current work will focus on reducing the overhead of quantum cryptography and improving blockchain logging.

VII. FUTURE WORK

While the proposed structure significantly enhances secure and scalable cloud data sharing, there are many areas for further discovery and improvements such as designing, lightweight lattice-based encryption and Post quantum cryptographic schemes such as Code-Based, Multivariate, and Hash-Based Cryptography could further enhance performance. Using Adaptive ML models that constantly learns from new attack patterns in real-time to reduce false positives and false negatives. Exploring layer -2 solutions like side chains, lightening network, shading can help optimize block chain efficiency.

REFERENCES

[1] S. Mhiri, A. Egio, M. Compastié, and P. Cosio, "Proxy Re-Encryption for Enhanced Data Security in Healthcare: A Practical Implementation," in *Proc.* 19th Int. Conf. on Availability, Reliability and Security (ARES 2024), Vienna, Austria, Jul. 30–Aug. 02, 2024, pp. 1–11, doi: 10.1145/3664476.3670874.

[2] R. Sharma and B. Joshi, "H-IBE: Hybrid-identity based encryption approach for cloud security with outsourced revocation," in Proc. 2016 Int. Conf. on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 2016, pp. 1192–1196, doi: 10.1109/SCOPES.2016.7955629.

[3] S. Ling, K. Nguyen, H. Wang, and J. Zhang, "Server-Aided Revocable Predicate Encryption: Formalization and Lattice-Based Instantiation," The Computer Journal, vol. 62, no. 12, pp. 1849–1862, Dec. 2019, doi: 10.1093/comjnl/bxz079.

[4] R. Agrawal, M. Imran, and H. Khan, "Machine Learning-Based Malicious User Detection in Cloud Computing," J. Inf. Secur. Appl., vol. 47, pp. 233–239, 2019.

[5] S. Wang, N. Luo, B. Xing, et al., "Blockchain-based proxy re-encryption access control method for biological risk privacy protection of agricultural products," Sci. Rep., vol. 14, p. 20048, 2024, doi: 10.1038/s41598-024-70533-0.

[6] N. Bindel, M. Brenner, and M. Naveed, "Lattice-based proxy re-encryption in the quantum-safe era," IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 2273–2285, 2021.

[7] S. Qi and Y. Zheng, "Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud," IEEE Trans. Dependable Secur. Comput., vol. 18, no. 2, pp. 765–779, Mar.–Apr. 2021, doi: 10.1109/TDSC.2019.2908164.

[8] R. Raghav, N. Andola, K. Verma, S. Venkatesan, and S. Verma, "Proactive threshold-proxy re-encryption scheme for secure data sharing on cloud," J. Supercomput., vol. 79, no. 13, pp. 14117–14145, Sep. 2023, doi: 10.1007/s11227-023-05221-3.

[9] H. Yu, X. Lu, and Z. Pan, "An Authorized Public Auditing Scheme for Dynamic Big Data Storage in Cloud Computing," IEEE Access, vol. 8, pp. 151465–151473, 2020.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," in Proc. 13th ACM CCS, 2006.

[11] Y. Zhang and Y. Mao, "Blockchain-Based Public Auditing for Dynamic Data Sharing in Cloud Environments," J. Cloud Comput., vol. 8, no. 1, pp. 21–32, 2019.

[12] P. R. S. Reddy and K. Ravindranath, "CR-IBE Based Data Sharing and Revocation in the Cloud," J. Discrete Mathematical Sciences and Cryptography, 2024.

[13] X. Chen, Y. Zhang, and M. Li, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Comput., vol. 64, no. 5, pp. 1223–1235, 2015.

[14] X. Yang, M. Wang, X. Wang, G. Chen, and C. Wang, "Multi-Replica and Multi-Cloud Data Public Audit Scheme Based on Blockchain," IEEE Access, vol. 8, pp. 144809–144822, 2020.

[15] B. Li, Q. He, F. Chen, H. Jin, Y. Xiang, and Y. Yang, "Auditing Cache Data Integrity in the Edge Computing Environment," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 5, pp. 1210–1223, 2021.

[16] C. Wang, K. Ren, S. Yu, and W. Lou, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19–24, 2010.

[17] J. Herranz, "Attribute-based encryption implies identity-based encryption," IET Inf. Secur., vol. 11, no. 6, 2017, doi: 10.1049/iet-ifs.2016.0490.

[18] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proc. CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, pp. 213–229, 2001.

[19] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," in Proc. IEEE INFOCOM, pp. 1–9, 2010.

[20] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1–30, Feb. 2006, doi: 10.1145/1127345.1127346.

[21] O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," in Proc. 37th Annu. ACM Symp. Theory Comput. (STOC '05), 2005, pp. 84–93.

[22] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE Access, vol. 6, pp. 12399–12421, 2017.

[23] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in Proc. 8th IEEE Int. Conf. Data Min. (ICDM), pp. 413–422, 2008.

[24] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, Feb. 2015.