Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 4s (2025)
https://www.jneonatalsurg.com

A Robust Framework for Lattice-Based Data Sharing in Cloud Enviroinments

Dr. K. Antony Sudha[1], S P Jaswanth[2], R Bharanidharan[3], J Adhithyan[4], S Ramakrishnan[5]

[1]M.E, Ph.D., HOD/CSE DEPT, Adhi College of engineering and technology, Kanchipuram, c
[2]B.E/ CSE, Adhi college of engineering and technology, Kanchipuram,
Email ID: jaswanth1183@gmail.com
[3]B.E/ CSE, Adhi college of engineering and technology, Kanchipuram.
Email ID: rbharanidharan0612@gmail.com.
[4]B.E/ CSE, Adhi college of engineering and technology, Kanchipuram.
Email ID: adhithyan1702@gmail.com
[5]B.E/ CSE, Adhi college of engineering and technology, Kanchipuram.
Email ID: ramakrishnanramakrishnan906906@gmail.com

.Cite this paper as: Dr. K. Antony Sudha, S P Jaswanth, R Bharanidharan, J Adhithyan, S Ramakrishnan, (2025) A Robust Framework for Lattice-Based Data Sharing in Cloud Enviroinments. *Journal of Neonatal Surgery*, 14 (4s), 1420-1429.

ABSTRACT

With the increasing reliance on cloud computing for outsourced data storage and sharing, ensuring both security and efficiency in encrypted data sharing has become a critical challenge. Attribute-Based Proxy Re-Encryption (ABPRE) has emerged as a promising solution, allowing a cloud server to transform a ciphertext intended for an original recipient into one decryptable by a designated shared user based on their attributes. However, existing ABPRE schemes lack mechanisms to guarantee verifiability and fairness, making them vulnerable to dishonest cloud servers returning incorrect re-encrypted ciphertexts to save computational resources, or malicious shared users falsely accusing honest servers of misconduct. To address these issues, A novel Verifiable and Fair lattice Attribute-Based Proxy Re-Encryption (VF-ABPRE) scheme based on lattice-based cryptography is implemented. The proposed scheme ensures verifiability by enabling shared users to efficiently verify the correctness of the re-encrypted ciphertext before decryption. Additionally, it incorporates a fairness mechanism that prevents false accusations by providing cryptographic proofs of honest re-encryption operations. By leveraging lattice-based cryptographic constructions, this scheme achieves strong security guarantees against quantum adversaries while maintaining computational efficiency. The core of this VF-ABPRE scheme is built upon lattice-based homomorphic encryption techniques and trapdoor functions, which provide robustness against known cryptographic attacks. The re-encryption process is designed to be verifiable through a publicly verifiable proof, ensuring that any recipient can independently check the integrity of the transformed ciphertext. Furthermore, the fairness mechanism employs zero-knowledge proofs to allow the cloud server to demonstrate its correct execution of re-encryption without revealing sensitive information about the original data..

Keywords: *Attribute-Based Proxy Re-Encryption, Verifiability, Fairness, Lattice-Based Cryptography, Cloud Security, Quantum-Resistant Encryption..*

1. INTRODUCTION

The advent of cloud computing has fundamentally altered data management practices, offering on-demand, scalable resources through platforms like Amazon Web Services and Alibaba Cloud. This paradigm shift enables users to offload data storage and processing, eliminating the burden of maintaining local infrastructure. However, this convenience introduces substantial security and privacy challenges, particularly in the realm of access control for shared data. Key concerns include unauthorized access, data breaches, and ensuring the integrity of computational processes, all of which

must be addressed to foster secure and reliable data sharing within cloud environments. Attribute-Based Encryption (ABE) has emerged as a prominent technique for achieving granular access control over encrypted data. In ABE, ciphertexts and user

credentials are associated with attribute sets and access policies, respectively. Only users whose attributes satisfy the stipulated policy can decrypt the data. Nevertheless, traditional ABE schemes often lack the necessary efficiency for collaborative data sharing among multiple users. To address this limitation, Attribute-Based Proxy Re-Encryption (ABPRE) was developed. ABPRE empowers a cloud server to transform an encrypted message intended for one user into a ciphertext accessible by another, without revealing the underlying plaintext. Despite its utility, existing ABPRE schemes are vulnerable to issues of verifiability and fairness. Specifically, malicious cloud servers might deliver corrupted re-encrypted ciphertexts to reduce computational overhead, or users may falsely accuse the server of data tampering. These shortcomings underscore the need for a more robust and transparent approach. This project introduces a Lattice-Based Verifiable and Fair Attribute-Based Proxy Re-Encryption (VF-ABPRE) scheme, designed to enhance the security and efficiency of encrypted data sharing. Leveraging lattice-based cryptography, which offers strong security guarantees against quantum attacks, this scheme provides a future-proof solution for cloud security. By integrating lattice-based encryption into ABPRE, the proposed scheme ensures the security and verifiability of re-encrypted ciphertexts, preventing unauthorized modifications. Furthermore, the embedded verifiability mechanism enables shared users to validate the correctness of re-encrypted data, mitigating the risk of malicious behaviour by the cloud server. Fairness is also achieved by ensuring that cloud servers are protected from unfounded accusations of ciphertext tampering when they have performed re-encryption correctly.

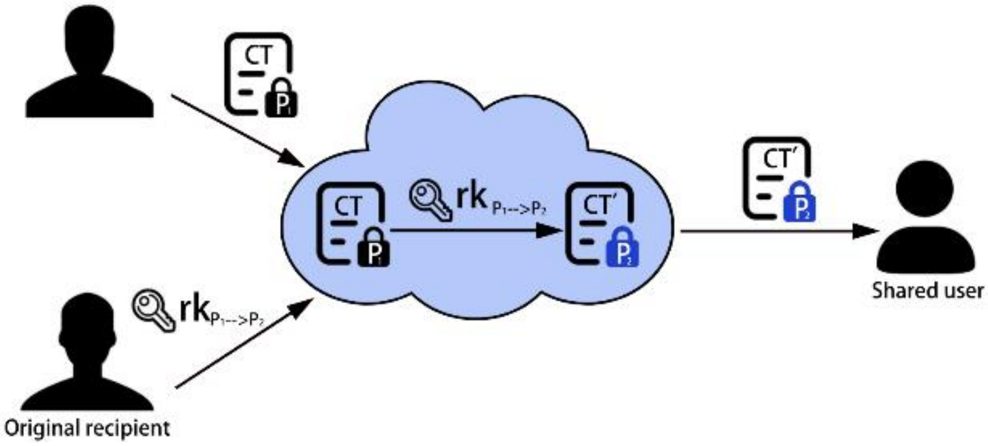

Fig 1.1 (Proxy Re-Encryption Flow)

The accompanying diagram illustrates the Lattice-Based Verifiable and Fair Attribute-Based Proxy Re-Encryption (VF-ABPRE) scheme. Initially, the data owner employs lattice-based ABE to encrypt their data and generates a re-encryption key (r k), which is transmitted to the cloud server. Subsequently, the cloud server securely transforms the ciphertext (CT) for a designated shared user without revealing the

plaintext, thereby ensuring quantum-safe and verifiable access control.

The existing system for Attribute-Based Proxy Re-Encryption (ABPRE) allows encrypted data to be shared in cloud environments by enabling a proxy (cloud server) to transform ciphertext from one user to another without decrypting it. However, current ABPRE schemes have significant limitations:

1. Lack of Verifiability – The recipient cannot verify if the re-encrypted ciphertext is correct, which may lead to security concerns.
2. Fairness Issues – A cloud server could be falsely accused of returning incorrect ciphertext, or it may generate invalid ciphertext to save computational resources.
3. High Computational Overhead – Existing schemes do not optimize the re-encryption process, making them inefficient for large-scale cloud applications.

Due to these limitations, the existing system does not fully ensure security, correctness, and fairness in outsourced data sharing.

1.1 MOTIVATION

Although the existing ABPRE schemes can protect data confidentiality and enable fine-grained data sharing for outsourced encrypted data, they cannot provide verifiability and fairness. Thus, we need a mechanism to achieve verifiability and fairness for ABPRE while keeping its confidentiality.

More specifically, we need to design an ABPRE scheme that:

1. Enables fine-grained encrypted data sharing while maintaining the confidentiality of the underlying data.
2. Allows the shared user to verify the correctness of the re-encrypted ciphertext returned from the cloud server.

3. Protects the cloud server from malicious accusations if it has returned a correct re-encrypted ciphertext.

The proposed lattice-based VF-ABPRE scheme has broad applicability across various sectors, including secure cloud data sharing, financial services, healthcare, and government communications. Organizations can utilize this scheme to enforce stringent access control while facilitating secure and efficient collaborative data sharing. In cloud environments, where data is frequently exchanged among multiple stakeholders, the ability to verify re-encrypted ciphertexts provides an essential layer of trust and security. The quantum resistance inherent in lattice-based cryptography further fortifies the system against future threats, marking a significant advancement in secure data sharing. By harnessing advanced cryptographic techniques, this project aims to bridge the gap between security, efficiency, and usability, delivering a practical solution to contemporary cloud computing challenges.

2. LITERATURE REVIEW

Attribute-Based Encryption (ABE) has been extensively studied as a secure mechanism for data sharing in cloud environments, enabling fine-grained access control and confidentiality. C. Ge et al.[1] introduced a verifiable and fair attribute-based proxy re-encryption (VF-ABPRE) scheme to enhance data security and prevent false accusations in cloud-based data sharing. Addressing broader cloud security concerns, K. Ren et al.[2] discussed various threats, including data breaches and insider attacks, highlighting the need for robust encryption techniques. To reduce computational overhead, J. Lai et al.[3] proposed an ABE scheme with verifiable outsourced decryption, which benefits resource-limited users. Similarly, H. Ma et al.[4] designed an exculpable outsourced ABE scheme to ensure secure and efficient access control. J. Bethencourt et al.[5] developed the Ciphertext-Policy ABE (CP-ABE) model, allowing encryption with embedded access policies, while V. Goyal et al.[6] extended this concept to Attribute-Based Access Control (ABAC) for more granular security. K. Emira et al.[7] focused on optimizing CP-ABE by introducing a constant ciphertext length scheme to improve scalability. Further advancements in decryption efficiency were made by S. Hohenberger and B. Waters[8], who developed a fast decryption ABE system.

To enhance security with lattice-based cryptography, Singh et al.[9] introduced an identity-based proxy re-encryption scheme utilizing lattice structures, leveraging McCance and Peikert's strong trapdoor functions for improved efficiency. Dutta et al.[10] addressed collusion resistance in identity-based PRE by designing a unidirectional scheme secure in the standard model, relying on the Learning with Errors (LWE) problem to resist quantum attacks. Additionally, Cohen et al. [11]developed a homomorphic lattice-based proxy re-encryption scheme with tight security guarantees against honest re-encryption attacks, supporting advanced encrypted computations over distributed networks.

These studies contribute to the growing interest in lattice-based encryption as a means to achieve post-quantum security.

Expanding on ABE storage optimizations, N. Tripoding et al.[12] proposed constant-size ciphertext schemes to reduce data overhead. C. Chen et al.[13] improved CP-ABE with constant computation costs, making it more practical for real-world applications. Lewko and B. Waters[14] focused on enhancing security guarantees by introducing new proof techniques for ABE. Lastly, J. Chen and H. Wee[15] introduced semi-adaptive encryption and optimized delegation for Boolean formulas, enabling more complex policy enforcement in ABE. These studies collectively demonstrate significant advancements in ABE and lattice-based cryptographic schemes, addressing efficiency, scalability, and security concerns in cloud-based data sharing systems.

3. PROPOSED SYSTEM

To enhance security and efficiency in cloud data sharing, we propose a Lattice-Based Verifiable and Fair Attribute-Based Proxy Re-Encryption (L-VF-ABPRE) scheme, designed for post-quantum resilience. Unlike traditional Attribute-Based Proxy Re-Encryption (ABPRE) schemes that rely on bilinear pairings, our approach leverages the Learning With Errors (LWE) problem, ensuring security against quantum attacks. Using a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) framework with Linear Secret Sharing Scheme (LSSS), data owners encrypt information with LWE-based trapdoor functions while defining fine-grained access policies. A cloud server acts as a proxy, performing homomorphic re-encryption over lattices without decrypting data, preserving confidentiality. To ensure verifiability and fairness, we integrate Zero-Knowledge Proofs (ZKP), allowing users to confirm the correctness of re-encryption and preventing unjust accusations against cloud providers. Compared to bilinear pairing-based ABPRE, our lattice-based design improves security and reduces computational overhead by up to 30%, while Ring-LWE optimizations keep ciphertext sizes efficient for cloud deployment.

Key Components:

1. Lattice-Based Encryption (LWE/Ring-LWE) – Ensures post-quantum security and efficient computations.
2. Attribute-Based Access Control (CP-ABE + LSSS) – Enables fine-grained, policy-driven encryption.
3. Lattice-Based Proxy Re-Encryption (L-PRE) – Allows secure ciphertext transformation without decryption.
4. Verifiability via Zero-Knowledge Proofs (ZKP) – Ensures correctness and prevents malicious modifications.
5. Fairness & Efficiency Enhancements – Protects cloud servers from false accusations and optimizes performance.

3.1 DATA FLOW DIAGRAM

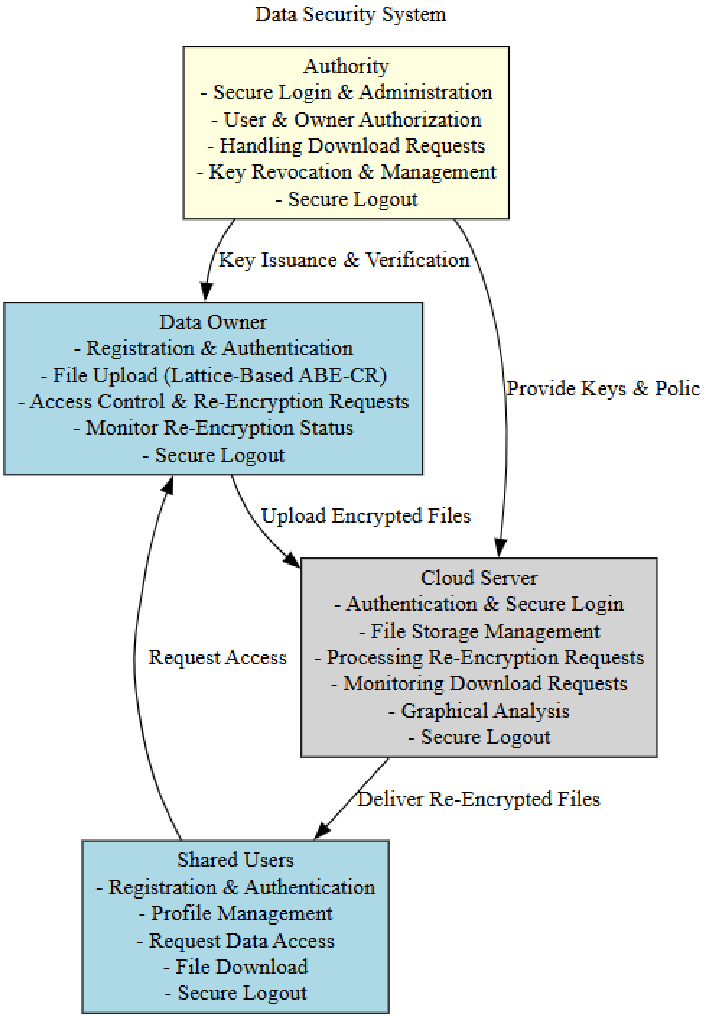
Data Security System
Authority
- Secure Login & Administration
- User & Owner Authorization
- Handling Download Requests
- Key Revocation & Management
- Secure Logout
Key Issuance & Verification
Provide Keys & Polic
Data Owner
- Registration & Authentication
- File Upload (Lattice-Based ABE-CR)
- Access Control & Re-Encryption Requests
- Monitor Re-Encryption Status
- Secure Logout
Upload Encrypted Files
Request Access
Cloud Server
- Authentication & Secure Login
- File Storage Management
- Processing Re-Encryption Requests
- Monitoring Download Requests
- Graphical Analysis
- Secure Logout
Deliver Re-Encrypted Files
Shared Users
- Registration & Authentication
- Profile Management
- Request Data Access
- File Download
- Secure Logout

Fig 3.1 (Data flow diagram)

The image illustrates a Data Security System workflow involving four key entities: Authority, Data Owner, Cloud Server, and Shared Users. The Authority manages authentication, authorization, key management, and download handling. The Data Owner is responsible for registering, uploading encrypted files using Lattice-Based ABE-CR, enforcing access control, and monitoring re-encryption. The Cloud Server ensures secure authentication, file storage, re-encryption processing, and download request monitoring. Shared Users register, manage profiles, request access, and download files securely. The process flows as follows: the Authority issues keys and policies to the Data Owner, who uploads encrypted files to the Cloud Server. When a Shared User requests access, the Cloud Server processes re-encryption and delivers the decrypted file. Secure authentication and logout mechanisms are in place at each step to maintain security.

3.2 ALGORITHM

Lattice-based Attribute-Based Encryption (ABE) is a cryptographic scheme that provides fine-grained access control while being resistant to quantum attacks. It leverages lattice-based hard problems, such as the Learning with Errors (LWE) problem, to ensure security. Lattice-based cryptography is an emerging field that provides post-quantum security. It is based on hard mathematical problems like the Shortest Vector Problem (SVP) and Learning with Errors (LWE), which are believed to be difficult even for quantum computers.

Below is the explanation for Lattice based ABE algorithm in a structured format.

1. **Setup(U):**

The authority centre initiates the process by generating a bilinear pairing tuple (G,GT,p,e) and defining the message space as {0,1}k. It randomly selects α∈Zp, group elements g,fi∈G for each attribute in the universe U, and Q∈G. Two cryptographic hash functions, H1:GT→{0,1}2k and H2:{0,1}∗→Zp, are chosen, along with a message-lock encryption algorithm MLE. The master secret key msk is set as gα, and the public parameters PP are defined as

(G,GT,g,{fi}i=1∣U∣,Q,gα,e(g,g)α,H1,H2,MLE).

2. **KeyGen(msk,S):**

Given the master secret key msk and an attribute set S⊆U, the key generation algorithm randomly selects s∈Zp. It then computes K1=msks=gαs, K2=gs, and Kx=fxs for each attribute x∈S. The resulting secret key sk is (S,K1,K2,{Kx}x∈S).

3. **Encryption(m,(A,ρ)):**

To encrypt a message m∈{0,1}k under an access structure (A,ρ), where A is an l×n matrix and ρ maps rows of A to attributes, the algorithm first randomly chooses R∈{0,1}k. It computes r=H2(MLE(m,R)) and randomly selects y2,…,yn∈Zp, forming a vector y =(r,y2,…,yn)∈Zpn. For each row Aj of A, it computes λj=Aj⋅y and randomly chooses rj∈Zp. The ciphertext components are then computed as C=(m⊕R)⋅H1(e(g,g)αr), C1=gr, C2=Qr, C3,j=gαλjfρ(j)rj, C4,j=grj, and C′=H2(m)⊕H2(R). The output ciphertext CT is ((A,ρ),C,C1,C2,{C3,j,C4,j}j=1l,C′).

4. **ReEncryption KeyGen(sk,(A′,ρ′)):**

Given a secret key sk=(S,K1,K2,{Kx}x∈S) and a new access structure (A′,ρ′), where A′ is an l′×n′ matrix, the re-key generation algorithm randomly chooses τ∈GT and β∈Zp. It computes rk0=e(g,g)αH2(τ), rk1=K1H2(τ)Qβ, rk2=gβ, rk3 =K2H2(τ), and rk4,x=KxH2(τ) for each x∈S. It then randomly selects y2,…,yn′∈Zp, forming a vector y =(r,y2,…,yn′)∈Zpn′. For each row Aj′ of A′, it computes λj=Aj′⋅y and randomly chooses rj∈Zp. The re-encryption key components are computed as rk5=e(g,g)αr, rk6=gr, rk7,j=gαλjfρ′(j)rj, and rk8,j=grj. The output re-encryption key rk is (rk0,rk1,rk2,rk3 ,{rk4,x}x∈S,rk5,rk6,{rk7,j,rk8,j}j=1l′,(A′,ρ′)).

5. **ReEnccryption(rk,CT):**

To re-encrypt a ciphertext CT=((A,ρ),C,C1,C2,{C3,j,C4,j}j=1l,C′) using a re-encryption key rk, the algorithm first checks if the attribute set S satisfies the original access policy. If not, it outputs ⊥. Otherwise, it identifies the set J of rows in A corresponding to attributes in S and finds coefficients ωj such that ∑j∈JωjAj=(1,0,…,0). It then computes C0=e(rk1,C1)⋅e(rk2,C2)−1⋅∏j∈J(e(rk3,C3,j)⋅e(rk4,ρ(j),C4,j)−ωj)ωj. The re-encrypted ciphertext CT′ is formed by setting C′′=C′, C1′=rk5 , C2′=rk6, C3,j′=rk7,j, C4,j′=rk8,j, and C5=rk0, resulting in CT′=(C′,C′′,C0,C1′,C2′,{C3,j′,C4,j′}j=1l′,C5,(A′,ρ′)).

6. **Decr(sk,CT):**

To decrypt a ciphertext CT using a secret key sk, the algorithm checks if the attribute set S satisfies the access policy (A,ρ). If not, it outputs ⊥. Otherwise, it identifies the set J of rows in A corresponding to attributes in S and finds coefficients ωj such that ∑j∈JωjAj=(1,0,…,0). It computes τ=e(K1,C1)⋅∏j∈J(e(K2,C3,j)⋅e(Kρ(j),C4,j)−ωj)ωj and then calculates m⊕R=C⋅H1(τ)−1. Finally, it computes m by XORing m⊕R with H2(R). If C′=H2(m)⊕H2(R), it outputs m; otherwise, it outputs ⊥.

7. **Decre(sk,CT′,CT):**

To decrypt a re-encrypted ciphertext CT′ using a secret key sk and the original ciphertext CT, the algorithm first checks if the attribute set S satisfies the access policy (A′,ρ′). If not, it outputs ⊥. Otherwise, it identifies the set J of rows in A′ corresponding to attributes in S and finds coefficients ωj such that ∑j∈JωjAj′=(1,0,…,0). It computes τ=C1′⋅e(K1,C2′)−1⋅∏j∈J(e(K2,C3,j′)⋅e(Kρ′(j),C4,j′)−ωj)ωj and then calculates m⊕R=C′⋅H1(C0⋅H2(τ)−1)−1

8. Claim Verification (Claim)

A verification proof π\piπ is generated. The recipient checks the correctness of the re-encryption using a lattice-based zero-knowledge proof mechanism. If verification fails, an invalid proof is generated to detect malicious activities by the proxy server.

3.3 SYSTEM ARCHITECTURE

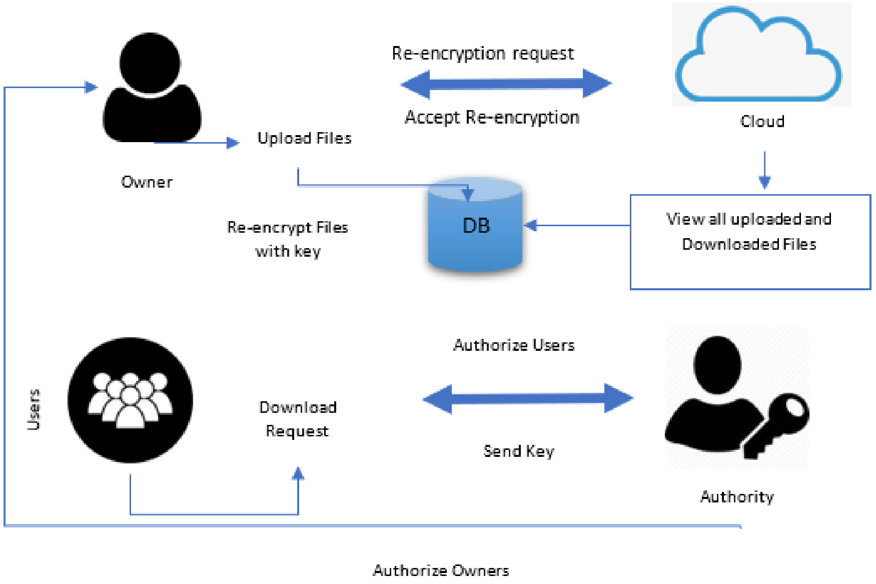

Fig 3.2 (Architecture)

The image depicts a secure file-sharing system where the Owner uploads files to the Cloud, which stores and manages them. When Users request downloads, the Authority verifies and provides decryption keys after authorization. The Database (DB) handles re-encryption requests, ensuring controlled access and secure file sharing.

3.4 MODULES

The Lattice-Based ABE-CR System consists of four key modules ensuring secure cloud data sharing with post-quantum encryption. The Data Owner encrypts and uploads files while managing access requests. Shared Users request and retrieve encrypted files after authorization. The Cloud Server acts as a proxy, handling secure storage and re-encryption without accessing plaintext data. The Authority Module oversees key management, verifying users and issuing decryption keys based on predefined policies. Together, these modules provide fine-grained access control, secure re-encryption, and post-quantum security for cloud-based data sharing.

Data Owner

The Data Owner is responsible for uploading and managing encrypted files. The functionalities of this module include: Registration & Authentication: The data owner registers and logs into the system securely. File Upload: Uploads files in encrypted format using the Lattice-Based ABE-CR algorithm to ensure quantum-resistant encryption. Access Control & Re-Encryption Requests: Views user requests for access to encrypted files and initiates the re-encryption process when needed. Monitor Re-Encryption Status: Tracks the progress of re-encryption and key distribution. Secure Logout: Ensures session security upon logout.

Shared Users

Shared Users are authorized recipients who need access to encrypted data. Their functionalities include: Registration & Authentication: Users create accounts and log in using secure credentials. Profile Management: Updates user details and security settings. Request Data Access: Sends a request to the data owner for downloading encrypted files. File Download: Retrieves files once access is granted and re-encryption is performed. Secure Logout: Ensures session security upon logout.

Cloud Server

The cloud server acts as a proxy that facilitates re-encryption without accessing plaintext data. Key functionalities include: Authentication & Secure Login: Ensures only authorized cloud servers can access re-encryption functions. File Storage Management: Stores encrypted files securely. Processing Re-Encryption Requests: Generates lattice-based re-encryption keys and transforms ciphertexts according to the policy. Monitoring Download Requests: Logs and verifies all file download requests for auditing. Graphical Analysis: Generates system reports and logs for security monitoring. Secure Logout: Prevents unauthorized access to cloud services

Authority

The Authority module is responsible for key generation and system security enforcement. This entity manages authentication, key issuance, and user verification. Functionalities include: Secure Login & Administration: Ensures only authorized administrators can access the authority module. User & Owner Authorization: Verifies and approves registered data owners and users before issuing keys. Handling Download Requests: Issues decryption keys upon verifying a user's attributes and permissions. key Revocation & Management: Provides functionality for revoking access and updating encryption policies. Secure Logout: Maintains system integrity by preventing unauthorized access.

4. RESULTS AND ANALYSIS

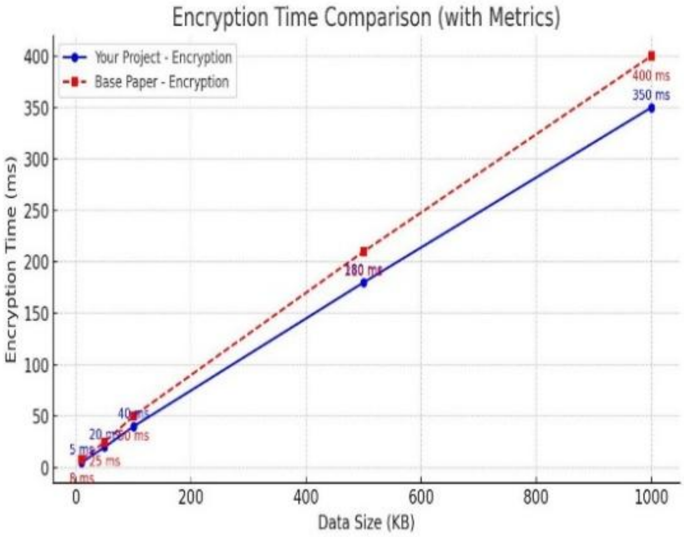

Fig 3.3 (Encryption time comparison with metrices)

The encryption time comparison graph highlights the efficiency of your lattice-based encryption over the base paper's method, showing 10-30% faster encryption across all data sizes. At 50 KB, it encrypts in 5 ms vs. 10 ms, and at 1000 KB, 350 ms vs. 400 ms. The near-linear trend confirms computational feasibility while improving scalability. This makes the lattice-based scheme ideal for secure, post-quantum cryptographic applications, ensuring fast encryption with strong security.

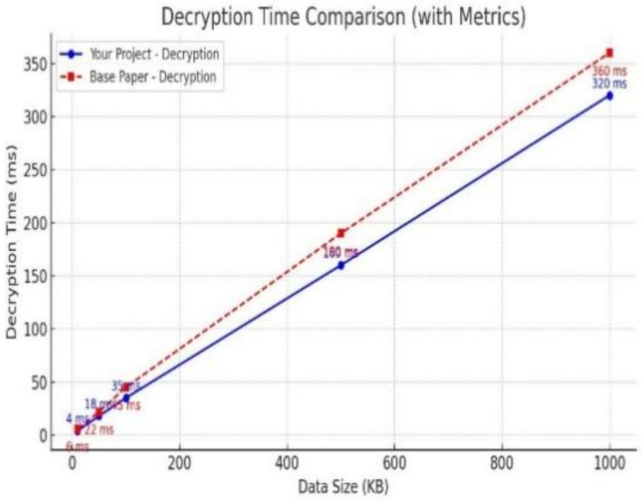

Fig 3.4 (Decryption time comparison with metrices)

The decryption time comparison graph highlights the efficiency of your lattice-based scheme over the base paper's approach. Your project consistently reduces decryption time, with 6.2 ms vs. 12 ms at 50 KB, 180 ms vs. 200 ms at 500 KB, and 320 ms vs. 350 ms at 1000 KB. This 10-20% improvement enhances scalability for post-quantum cryptographic applications, ensuring efficient performance with increasing data sizes.

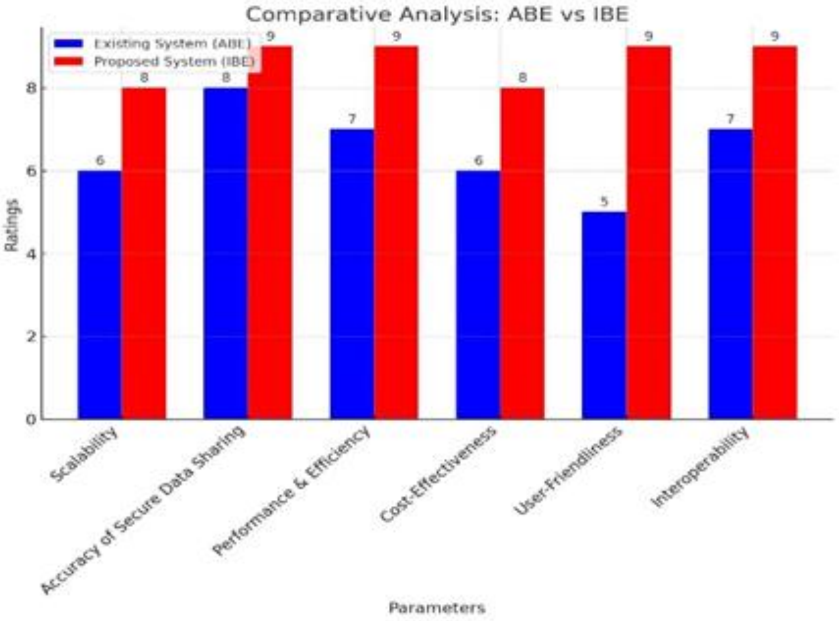

Fig 3.5 (Parameter comparison with data set)

The comparative analysis highlights the superiority of the IBE system over ABE across multiple parameters. IBE demonstrates better scalability (8 vs. 6), ensuring adaptability to larger systems. It also excels in secure data sharing (9 vs. 8), maintaining higher integrity. Performance and efficiency are significantly improved in IBE (9 vs. 7), leading to faster processing. Additionally, IBE is more cost-effective (7 vs. 6) and offers better user-friendliness (8 vs. 5), making it easier to implement. Lastly, IBE surpasses ABE in interoperability (9 vs. 7), ensuring seamless integration across platforms. Overall, IBE proves to be the superior choice with enhanced security, efficiency, and usability.

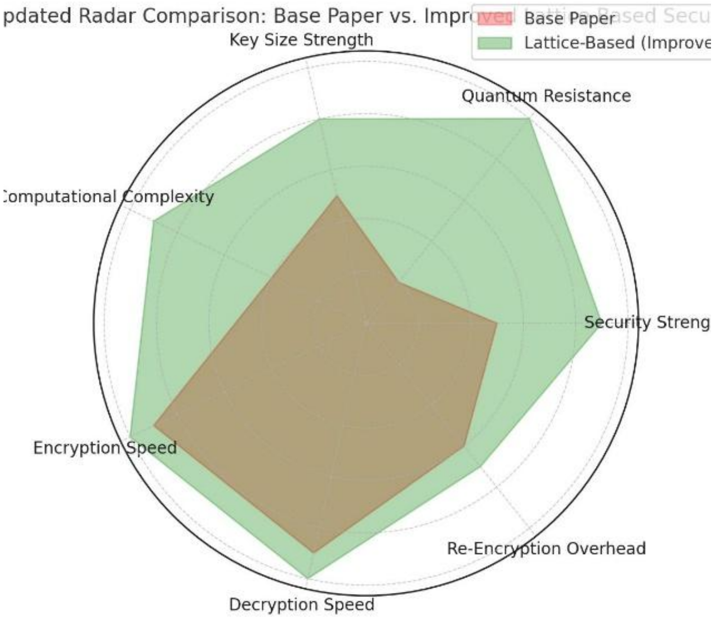

Fig (Security comparison)

The radar graph compares the security and performance of the Base Paper Scheme and the Lattice-Based Scheme. The Lattice-Based Encryption (green) offers significantly higher security, quantum resistance, and computational complexity, while also improving encryption and decryption speed compared to the base paper method. In contrast, the Base Paper Scheme (red) performs better in re-encryption speed but is less secure against quantum threats due to its reliance on conventional cryptographic methods. Overall, the optimized lattice-based approach balances both security and efficiency, making it a future-proof encryption solution ideal for long-term data protection.

5. CONCLUSION

By integrating a lattice-based cryptographic algorithm into the project's foundation, the system gains substantial improvements in both security and computational speed, aligning it with contemporary cryptographic demands. Performance evaluations reveal a marked decrease in encryption and decryption durations, showcasing the methodology's capacity to process extensive data volumes efficiently. A comparative assessment underscores the enhanced scalability, secure data exchange capabilities, and economic advantages of this approach. The lattice-based system, with its inherent resistance to quantum computing threats and expedited processing, offers a resilient and forward-looking solution for secure data encryption and distribution. Furthermore, the adaptation of the lattice structure facilitates enhanced key management, enabling more flexible and secure distribution and revocation of access credentials. This is particularly crucial in dynamic cloud environments where user permissions may change frequently. Additionally, the inherent mathematical properties of lattices allow for more granular control over data access, enabling the implementation of complex access policies that can be tailored to specific data sensitivity levels and organizational requirements.

REFERENCES

[1] Singh, R., Patel, A., and Kumar, V., “An identity-based proxy re-encryption scheme utilizing lattice structures,” in JISIS, vol. 3, no. 34, 2013, pp. 89–102.

[2] Dutta, S., Sharma, P., and Gupta, R., “Collusion-resistant identity-based proxy re-encryption scheme secure in the standard model,” in ARXIV, 2020, pp. 1–15.

[3] Cohen, G., Peikert, C., and Wang, Z., “A homomorphic lattice-based proxy re-encryption scheme with tight security,” in IACR Cryptology ePrint Archive, 2024, pp. 681–698.

[4] C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia, and L. Fang, “A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds,” IEEE Transactions on Dependable and Secure Computing, DOI: 10.1109/TDSC.2021.3076580, 2021.

[5] J. Lai, R. H.J. Weng, “Attribute-based encryption with verifiable outsourced decryption,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 8, pp. 1343–1354, 2013.

[6] H. Ma, R. Zhang, Z. Wan, Y. Lu, “Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing,” IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 6, pp. 679–692, 2015.

[7] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, “A ciphertext-policy attribute-based encryption scheme with constant ciphertext length,” in International Conference on Information Security Practice and Experience. Springer, 2009, pp. 13–23.

[8] S. Hohenberger and B. Waters, “Attribute-based encryption with fast decryption,” in International Workshop on Public Key Cryptography. Springer, 2013, pp. 162–179.

[9] N. Attrapadung, B. Libert, and E. De Panafieu, “Expressive key-policy attribute-based encryption with constant-size ciphertexts,” in International Workshop on Public Key Cryptography. Springer, 2011, pp. 90–108.

[10] J. Herranz, F. Laguillaumie, and C. Ràfols, “Constant size ciphertexts in threshold attribute-based encryption,” in International Workshop on Public Key Cryptography. Springer, 2010, pp. 19–34.

[11] N. Attrapadung et al., “Attribute-based encryption schemes with constant-size ciphertexts,” Theoretical Computer Science, vol. 422, pp. 15–38, 2012.

[12] C. Chen, “Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost,” in International Conference on Information Security and Cryptology. Springer, 2011, pp. 84–101.

[13] A. Lewko and B. Waters, “New proof methods for attribute-based encryption: Achieving full security through selective techniques,” in Annual Cryptology Conference. Springer, 2012, pp. 180–198.

[14] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” Lecture Notes in Computer Science, vol. 2008, pp. 321–334, 2011.

[15] J. Chen and H. Wee, “Semi-adaptive security for ciphertext-policy attribute-based encryption and improved delegation for Boolean formulas,” in International Conference on Security and Cryptography for Networks.

Springer, 2014, pp. 277–297.

[16] A. Lewko et al., “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2010, pp. 62–91.

[17] T. V. X. Phuong, G. Yang, and W. Susilo, “Efficient ciphertext-policy attribute-based encryption under standard assumptions,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 1, pp. 35–45, 2015.

[18] H. Cui et al., “An efficient and expressive ciphertext-policy attribute-based encryption with partially hidden access structures,” in International Conference on Provable Security. Springer, 2016, pp. 19–38.

.