Study on Enhancing Security in Multi-Users Encrypted Data Queries

Vidhi Mehta; Ankit Parkhi; Aman Chaudhari
Department of Master in Computer Application,
G H Raisoni College of Engineering and Management,
Maharashtra, India

Abstract: This study examines at the difficulties and developments in improving the security of encrypted data queries with multiple users in cloud systems. Ensuring safe and effective access to encrypted data in multi-user environments has become essential as cloud computing continues to dominate numerous industries. The intricate requirements of multi-user systems are frequently not met by conventional encryption solutions, especially when it comes to data privacy and access control. Recent developments in cryptographic methods, including attribute-based encryption, proxy re-encryption, and homomorphic encryption, have made major progress in protecting data while preserving query functionality. By enabling secure query processing on encrypted data without requiring decryption, these techniques lower the possibility of data leakage. Furthermore, hybrid encryption models and AI-driven access policies support dynamic and adaptable data access, while the use of blockchain technology for decentralized access management provides improved transparency, immutability, and security. Scalability, computational effectiveness, and real-time processing are still major obstacles, though. In order to increase security, scalability, and performance in multi-user encrypted data queries, this study proposes a hybrid encryption architecture that combines blockchain-based authentication, fully homomorphic encryption (FHE), and attribute-based encryption (ABE). By addressing the shortcomings of existing solutions, the suggested framework seeks to offer a dependable, scalable solution that guarantees private and secure data access in multi-user cloud environments.

Keywords: Encrypted Data Queries, Multi-User Access Control, Data Security, Privacy-Preserving Queries, Cryptographic Techniques, Secure Data Sharing.

1. Introduction

In today's mutual connected world, the division and collaboration of data between many parties has become crucial to different applications and industries. As cloud computing and data outsourcing have grown in popularity, it has become increasingly difficult to provide safe and effective access to encrypted data in multi-user settings. As more businesses shift their data to cloud platforms, it's critical to protect data privacy while enabling authorized users to conduct inquiries. Although they work well for single-user access, traditional encryption techniques frequently fail in situations where there are several users with different degrees of authorization and intricate access control needs [3][4].

By processing encrypted data without completely decrypting it, recent developments in cryptographic approaches including homomorphic encryption, attribute-based encryption, and proxy re-encryption have decreased the danger of data disclosure [1][5][7]. Specifically, attribute-based encryption offers fine-grained access control mechanisms that are crucial in multi-user systems, while homomorphic encryption permits operations on encrypted data and supports secure queries [4][7]. In addition,

DOI: https://doi.org/10.5281/zenodo.15505252

decentralized access control systems that improve access rights' transparency, immutability, and auditability have been created by the incorporation of blockchain technology [1][6][9].

Furthermore, hybrid encryption techniques combined with AI-driven access management have demonstrated potential in accommodating changing access needs, hence enhancing cloud environments' privacy and usability [2]. These systems still have issues with scalability, computational effectiveness, and flexibility in response to changing access regulations, though. By utilizing the advantages of sophisticated encryption methods, decentralized control systems, and intelligent access policy management, this study investigates a thorough strategy for improving the security of multi-user encrypted data searches in order to address theseissues.

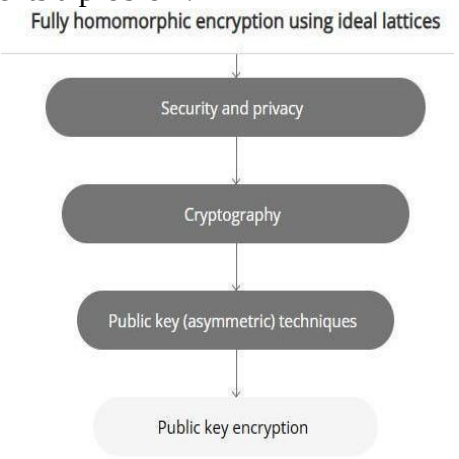
The goal of this project is to help provide a safe, scalable, and reliable framework for multi-user encrypted data querying that maintains data privacy without sacrificing efficiency. By analyzing current methods and pointing out their drawbacks, we suggest ways to enhance security, effectiveness, and flexibility in actual multi-user cloud environment.

2. Literature Survey

Numerous encryption solutions have been investigated to enable encrypted queries in light of the increasing demand for safe data processing in cloud environments. These methods seek to minimize computational overheads while striking a compromise between security, efficiency, and access control. This survey highlights the advantages and disadvantages of several important techniques, such as blockchain-based decentralized authentication, fully homomorphic encryption (FHE), attribute- based encryption (ABE), and proxy re-encryption (PRE) [3].

2.1 Fully Homomorphic Encryption (FHE)

A cryptographic approach called Fully Homomorphic Encryption (FHE) enables calculations to be done directly on encrypted data without the need for decryption. The first workable FHE system was presented by Gentry (2009), allowing for arbitrary calculations while maintaining anonymity. This innovation makes safe cloud computing possible, enabling users to work with private information without disclosing it to outside parties. However, FHE is unsuitable for real- time applications due to its high ciphertext growth and substantial processing expenses. To increase performance, researchers have suggested modifications such leveling and bootstrappable FHE; nonetheless, in multi-user applications, the overhead still presents a problem.



2.2 Attribute-Based Encryption (ABE)

Sahai and Waters (2005) created attribute-based encryption (ABE), which improves access control by linking decryption keys to attributes rather than particular identities. A data owner encrypts data using an access policy in an ABE scheme, making sure that only users who possess the same qualities can decode it. Applications like healthcare and finance, where fine-grained access control is necessary, benefit greatly from this strategy. To give access control greater flexibility, variants such as Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE) have been created. Notwithstanding its benefits, ABE has

DOI: https://doi.org/10.5281/zenodo.15505252

efficiency issues with attribute revocation and key management, especially in large-scale systems.

2.3 Integration of FHE, ABE, and Blockchain for Secure Queries

Even while encrypted data queries have advanced, current solutions frequently have significant computing overheads or are ineffective in multi-user settings. This paper suggests an integrated system that combines blockchain for decentralized authentication, ABE for access control, and FHE for secure query processing. Users can run encrypted searches without disclosing private information by utilizing FHE. Selective decryption according to user attributes is made possible by ABE's fine- grained access control. By offering a decentralized, tamper-proof authentication method, blockchain improves security by reducing the dangers connected with centralized key management.

3. Methodology

Ensuring data security and effective access control has become crucial due to the growing dependence on cloud computing and distributed systems. Even though traditional encryption methods are good at maintaining the security of data, they frequently cause problems with query execution and access control. This study offers a hybrid encryption architecture that combines Attribute-Based Encryption (ABE) for fine-grained access control and Fully Homomorphic Encryption (FHE) for safe query execution in order to overcome these difficulties. Additionally, decentralized access management using blockchain-based authentication is used to improve security. Optimizing query execution, implementing role-based access control policies, and assessing system security and performance are the main objectives of the suggested methodology. The framework seeks to offer a scalable and effective solution for safe data processing in cloud environments by utilizing these cutting-edge cryptographic algorithms [3].

3.1 Blockchain-based Authentication

The framework uses blockchain technology for decentralized authentication to strengthen security and access management. By using smart contracts to handle access control and user authentication, a centralized authority is no longer necessary. This decentralized method ensures data integrity through immutable ledger entries, preventing unwanted access and boosting system confidence. Unauthorized changes are practically impossible because the blockchain records each access request and permission that is granted. Additionally, by keeping an auditable record of every access transaction, blockchain technology guarantees accountability and transparency. This method greatly lowers security threats like unauthorized privilege escalation and identity spoofing.

3.2 Optimized Query Execution

Preserving computing efficiency is one of the major obstacles while working with encrypteddata.The suggestedmethodologyusesoptimizedhomomorphic operations to solve this problem, allowing for safe and effective query execution on encrypted datasets. The system candomathematical operations on ciphertextsdirectly by utilizing FHE, which eliminates the need for intermediate decryption stages. Moreover, parallel processing methods and algorithmic improvements are combined to reduce computational cost and improve processing performance. These enhancements guarantee that the encryption strategy maintains its viability for real-world applications without causing appreciable performance snags.

3.3 Access Control Policies

The framework uses role-based encryption models to impose a methodical and safe access control system. Predefined roles are

DOI: https://doi.org/10.5281/zenodo.15505252

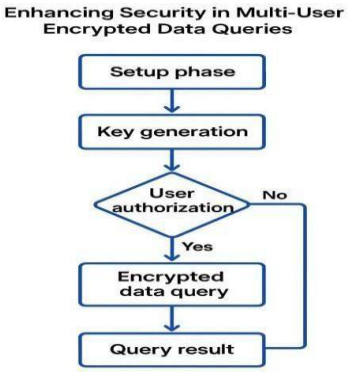
allocated to users, and these roles determine their access privileges. ABE and role-based access work together to prevent unwanted access and guarantee that only authorized users can decode particular datasets. By limiting decryption capabilities to users who possess the necessary qualities, this paradigm reduces the dangers related to data disclosure. In order to keep security rules flexible in response to evolving needs, the framework dynamically modifies access control policies according to user roles and privileges.

3.4 Security Evaluation

The suggested framework's security resilience is evaluated against a range of possible dangers, such as replay attacks, collusion attacks, and unauthorized modifications. Blockchain-based immutability and cryptographic integrity checks prevent unauthorized changes and guarantee that no changes are made covertly. By using multi-layered encryption techniques that limit data decryption to particular qualities, collusion attacks in which several malevolent individuals try to pool their privileges to obtain illegal access are avoided. Furthermore, nonce-based authentication and timestamp verification are employed to prevent replay attacks and make sure that previously recorded requests cannot be exploited fraudulently to obtain access.

3.5 Performance Testing

A cloud-based testing environment is set up to analyze several performance metrics in order to assess the suggested framework's practical viability. Improvements in security, system scalability, and query execution time are the main factors that are looked at. By running searches on massive encrypted datasets and contrasting the results with more conventional encryption techniques, the effectiveness of homomorphic operations is evaluated. To find out if the system can accommodate more users and data requests without seeing a noticeable drop in performance, scalability tests are carried out. Lastly, security evaluations examine the framework's ability to reduce risks and preserve data privacy. The outcomes of these tests guarantee that the framework satisfies security and performance criteria while offering insights into its efficacy in practical deployments.



4. Conclusion

In conclusion, protecting multi-user encrypted data queries in cloud settings is still a major problem for contemporary data management systems. This study emphasizes how crucial it is to combine decentralized frameworks, dynamic access control systems, and sophisticated encryption techniques in order to ensure both data secrecy and effective, permitted access. Secure query processing on encrypted data is made possible by methods like homomorphic encryption and proxy re-encryption, while attribute-based encryption offers fine-grained access control that is appropriate for intricate multi-user settings.

Through the implementation of decentralized, impenetrable access control and visible audit trails, blockchain technology provides an extra degree of protection. Additionally, the flexibility and privacy of cloud-based systems are improved by the use of AI-driven and hybrid encryption techniques, which provide flexibility to shifting user roles and access requirements.

Even though the outcomes of current

DOI: https://doi.org/10.5281/zenodo.15505252

solutions are encouraging, issues with scalability, computing efficiency, and support for real-time data access still persist. By examining practical solutions, assessing these issues, and suggesting future development paths, this study adds to the expanding area. In the future, creating reliable and secure multi-user encrypted data query systems will require the cooperation of distributed architecture, intelligent access control, and cryptography innovation.

5. Reference

[1] Mandal, S., Banerjee, A., & Das, A.K.(2025) "Secure Multi-User Data Querying With Blockchain and Homomorphic Encryption for IoT-Based Cloud.

[2] Ahmed, I., Bhatti, S., & Zohdy, M. A. (2025) "Hybrid Encryption and AI-Driven Access Control for Privacy-Preserving Cloud Data Sharing.

[3] Liu, Y., Zhang, H., Wang, R., et al. (2024) "Secure and Efficient Multi-User Searchable Encryption Scheme with Fine-Grained Access Control for Cloud Storage."

[4] Rajendran, N., & Vinothina, V. (2024) "Enhanced Attribute-Based Encryption with Dynamic Policy Updates in Multi-Owner Cloud Storage."

[5] Patel, R., & Srivastava, M. (2024) "Secure Delegatable Search on Encrypted Data Using Proxy Re-Encryption in Cloud."

[6] Chen, J., Tan, Y., & Shen, Z. (2023) "Blockchain-Based Secure Access Control for Encrypted Medical Data in Cloud Environments."

[7] Zhao, L., Liu, Q., & Gao, Y. (2023) "Efficient Attribute-Based Encryption with Revocation in Cloud Storage."

[8] Wang, S., Yu, L., & Ren, K. (2023) "Towards Real-Time Encrypted Data Processing: Lightweight FHE for Cloud Applications."

[9] Khan, M. A., Ullah, I., & Habib, M. A. (2023) "Blockchain-Based Role-Driven Access Control for Distributed Cloud Storage."

[10] Khan, M. A., Ullah, I., & Habib, M. A. (2023) "Blockchain-Based Role-Driven Access Control for Distributed Cloud Storage."

DOI: https://doi.org/10.5281/zenodo.15505252