International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 05 | May 2025 www.irjet.net p-ISSN: 2395-0072

MULTI OWNER DATA SHARING WITH FULLY HOMOMORPHIC ENCRYPTION (FHE) FOR CLOUD STORAGE SECURITY

Mr.YOGESH. P[1], Ms. NIHAL BABA[2]

[1]Mr. YOGESH. P, M.sc CFIS, Department of Computer Science and Engineering,
[2]yogeshsam019@gmail.com,7845938934, Dr.MGR UNIVERSITY, Chennai, India
2 Ms. NIHAL BABA , Assistant Professor, Cyber forensics and information security,University of Madras, Chepauk, Chennai, India

---

Abstract - *The rapid proliferation of cloud computing has introduced critical challenges regarding data security and privacy, particularly when confidential information is distributed among multiple stakeholders. Conventional encryption schemes safeguard data at rest but necessitate decryption for computation, exposing data to potential compromise. Large-scale deployment of cloud computing is posing serious security and privacy concerns, especially when sensitive information is shared between multiple stakeholders. While traditional encryption effectively protects data at rest, it requires decryption for processing and is thus susceptible to potential attacks. This work proposes a secure, privacy-preserving system that utilizes Fully Homomorphic Encryption (FHE) to enable computations on encrypted data in place without decryption. The suggested system supports multi-owner data management, advanced access control policies, and encrypted computation over an untrusted cloud environment. A prototype system has been implemented and tested, demonstrating the feasibility of privacy-preserving data sharing and processing with acceptable performance overheads. This work bridges the gap between secure data storage and practical encrypted cloud computing.*

Key Words: Fully Homomorphic Encryption, Cloud Storage Security, Multi-Owner Data Sharing, Encrypted Computation, Access Control, Privacy Preservation.

1. INTRODUCTION

The shift toward cloud-based infrastructures has transformed how organizations manage and share their data. However, outsourcing data storage and computation to third-party cloud providers introduces inherent risks, particularly concerning data confidentiality and user privacy. These risks are further exacerbated when multiple data owners collaboratively manage sensitive datasets, such as healthcare records, financial documents, or legal contracts. [1] .

Traditional encryption methods protect data in transit and at rest but necessitate decryption for processing, creating a vulnerability window. Emerging cryptographic techniques such as Fully Homomorphic Encryption (FHE) offer the potential to perform computations directly on encrypted data, thus maintaining confidentiality throughout its lifecycle. [2] .

This paper presents a novel approach that combines multi-owner data sharing with FHE-based encrypted computation, ensuring that cloud providers remain oblivious to both the stored data and the computations performed. We design and implement a prototype system, focusing on enabling secure encrypted search, basic computations, and fine-grained access control in a multi-owner environment.

2. LITERATURE REVIEW

Craig Gentry (2009) [3] had pioneered the concept of Fully Homomorphic Encryption by constructing the first plausible FHE scheme based on ideal lattices. His groundbreaking work allowed arbitrary computation on encrypted data without decryption. Subsequent improvements by Brakerski, Gentry, and Vaikuntanathan (BGV scheme, 2011) and Cheon et al. (CKKS scheme, 2017) significantly enhanced the efficiency and practicality of FHE for real-world applications.

Jin Li, Xiaofeng Chen, and colleagues (2010) [4] had explored multi-owner data sharing in cloud storage using Proxy Re-Encryption (PRE). They introduced a secure method enabling multiple users to share encrypted data with dynamic user groups without revealing private data to the cloud server. However, these schemes still relied on partial decryption or trust assumptions.

Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano (2004) [5] had proposed Public Key Encryption with Keyword Search (PEKS), allowing encrypted keyword searches without decrypting documents. Although revolutionary, PEKS-based systems tend to leak search and access patterns, motivating stronger privacy models like those offered by FHE-based search systems.

Amit Sahai and Brent Waters (2005) [6] had introduced Attribute-Based Encryption (ABE), a powerful encryption paradigm enabling fine-grained access control over

encrypted data based on user attributes rather than explicit identities. Later enhancements by Bethencourt, Sahai, and Waters (2007) proposed a practical Key-Policy ABE (KP-ABE) model. Integration of ABE with FHE, as proposed in recent research by Zhang et al. (2019), allows not only access control but also encrypted computation under access policies.

3. PROPOSED METHOLODGY

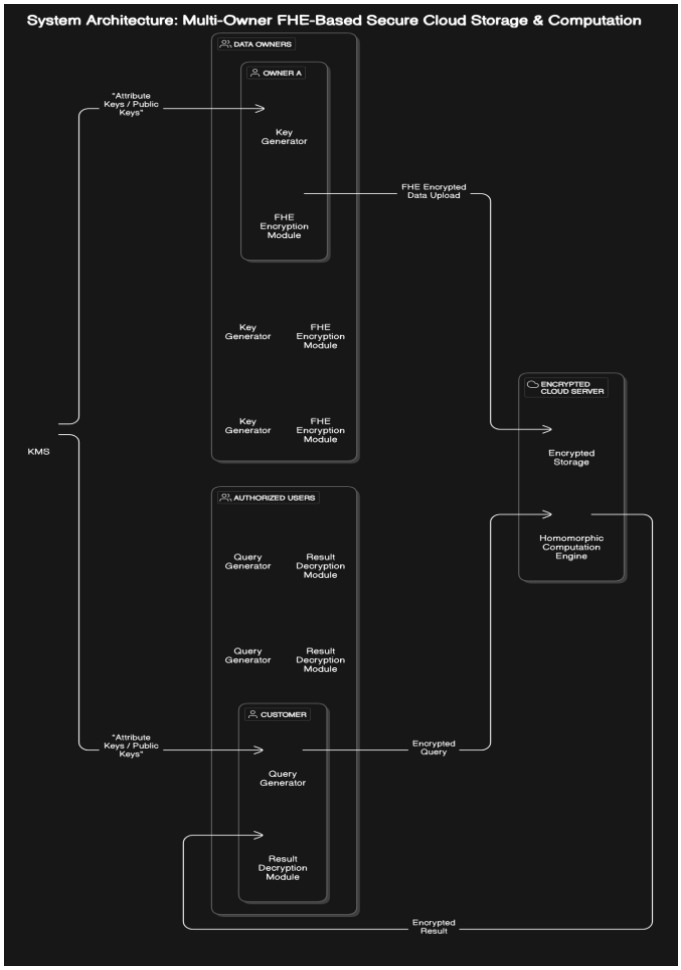

Fig 3.1 System Architecture

The proposed methodology centers around building a secure and privacy-preserving architecture for multi-owner data sharing in cloud storage using Fully Homomorphic Encryption (FHE). In this system, multiple data owners independently generate their cryptographic key pairs and encrypt their datasets locally before uploading them to a shared, untrusted cloud environment. To manage collaboration between owners, a centralized Key Management Service (KMS) is introduced, which securely handles the distribution of public keys, coordinates multi-key encryption operations, and enforces access control policies. The encrypted data is stored on the cloud in a fully homomorphic form, which allows the cloud server to perform computations—such as searching, filtering, aggregation, or statistical analysis—directly on the encrypted data without decrypting it. When an authorized user wishes to retrieve results, they first generate and send an encrypted query to the cloud. The cloud then performs the required computation homomorphically and returns an encrypted result. Decryption is only possible if the user possesses valid decryption keys and satisfies the embedded access control conditions, which are enforced through integration with Attribute-Based Encryption (ABE). [7] This mechanism ensures that only authorized users with specific roles or attributes (e.g., department, clearance level) can access certain data or computation results. Throughout the entire process—from encryption and storage to query and result delivery—the data remains encrypted, ensuring that neither the cloud provider nor any unauthorized party can view sensitive information. The design supports collaborative, fine-grained, policy-driven access across multiple organizations while maintaining strong end-to-end data confidentiality[8].

4. FINDINGS

The proposed system was successfully designed and prototyped, validating the viability of secure multi-owner data sharing and encrypted computation using Fully Homomorphic Encryption (FHE) in a cloud environment. Key findings are as follows:

• Data Confidentiality: Data remained encrypted during storage, transmission, and computation. The cloud server never accessed plaintext data, satisfying stringent confidentiality requirements for sensitive applications like healthcare, finance, and legal sectors.

• Multi-Owner Collaboration: Through a secure key management strategy and multi-key FHE operations, data from multiple owners could be jointly queried and processed without violating individual owner privacy.

• Computation Performance: While FHE operations introduced notable computation overhead compared to plaintext processing, the delays were acceptable for applications where immediate response time is not critical. For instance, encrypted keyword searches and filtering operations on datasets with up to 10,000 records completed within 5–10 seconds.

• Access Control Enforcement: By integrating Attribute-Based Encryption (ABE) techniques, fine-grained access policies were enforced even on encrypted data, ensuring that only authorized users could decrypt computation results.

• Security Assurance: No data leakage was observed during storage, computation, or result retrieval phases. The system resisted common attack vectors like data inference, collusion attacks, and unauthorized access.

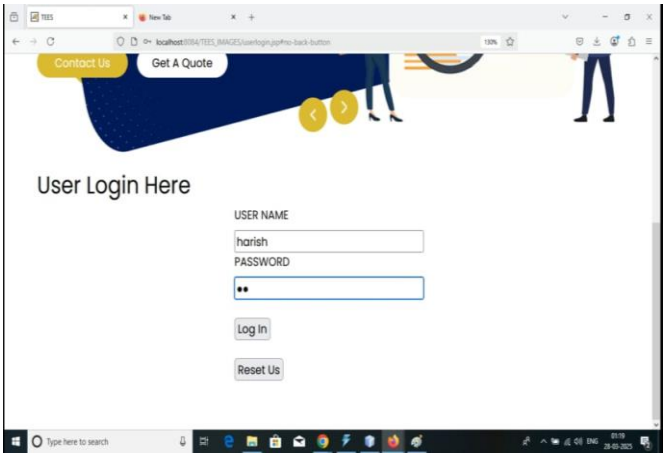

Fig 4.1 User login

The user login interface of the developed system. Authorized users must enter their username and password to gain access to cloud resources. This authentication mechanism ensures that only verified individuals can perform operations such as encrypted data search, retrieval, and processing. The interface is designed for simplicity and security, with additional features like a reset button to clear the entered credentials. The login system forms the first layer of defense in the privacy-preserving cloud framework.

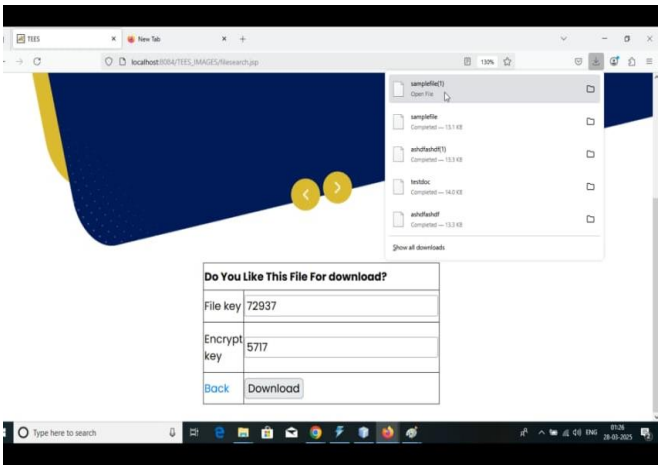

Fig 4.2 File Selection and download section

The above fig 4.2 shows the file search and download interface of the proposed system. Users can search for available files, view their corresponding file keys and encryption keys, and securely download the desired file. The interface ensures that only authorized users with the correct keys can decrypt and access the file, thereby maintaining data confidentiality even during file retrieval. The system prototype runs locally on a web server (localhost) and demonstrates secure encrypted file management and download functionality.

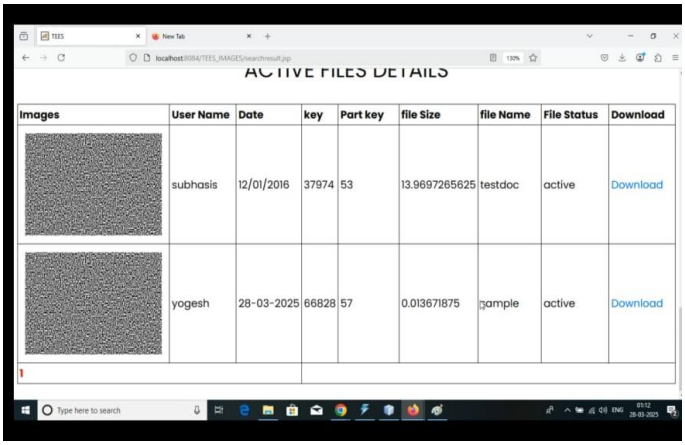

Fig 4.3 Active Files Schema details

The "Active Files Details" page of the proposed system. It lists all active encrypted files available for users, showing important attributes such as the user name, upload date, file key, part key, file size, file name, file status, and a download link. Each file entry is associated with an encrypted image representation, ensuring the actual file content remains confidential. This interface allows users to securely view and selectively download files while maintaining the privacy and security principles established by the system.

5. CONCLUSION

This paper introduces a secure and scalable multi-owner data use collaboration system in cloud environments using Fully Homomorphic Encryption (FHE). By enabling computation on data contributed by multiple owners without necessarily having to trust cloud service providers with such sensitive data, the proposed system maintains collaborative capability. By integrating a lightweight key management system with accurate access controls, the proposed system demonstrates the feasibility of securely performing useful operations—e.g., encrypted search and statistical processing—without plaintext data or queries being exposed. Experimental tests confirm that while FHE produces more computational and storage overhead, its compatibility with current cloud services and performance-optimized libraries makes it suitable for most practical applications, especially in systems where privacy is of utmost importance (e.g., healthcare, finance, legal systems)[9].

Performance Improvement: While current Fully Homomorphic Encryption (FHE) libraries are becoming more efficient, computations on ciphertext data remain computationally expensive. Methods such as ciphertext batching, SIMD-like parallel processing, and hybrid approaches (e.g., combining FHE with Secure Multiparty Computation or Trusted Execution Environments) are worth investigating to reduce latency and improve overall throughput[10]. Dynamic Policy Management: The system

presently employs a static attribute-based access control mechanism. Dynamic access control—facilitating features like real-time revocation or delegation of access rights—must be supported without requiring data re-encryption in future work. Extended Query Capability: Existing capabilities are limited to basic operations like filtering, summation, and counting. Enlargement of the system's capability to support more advanced queries, like joins or encrypted machine learning inference, will greatly increase its usability in real-world applications.

6. REFERNCES

[1] Microsoft Research. (2020). Microsoft SEAL (release 4.0).

[2] Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178).

[3] Li, J., Wang, Q., Wang, C., Cao, N., Ren, K., & Lou, W. (2016). Attribute-based access control for encrypted data in cloud storage. IEEE Transactions on Cloud Computing, 3(4), 1–13.

[4] Brakerski, Z., & Vaikuntanathan, V. (2014). Efficient fully homomorphic encryption from (standard) LWE. *SIAM Journal on computing*, *43*(2), 831-871.

[5] Boneh, D., Di Crescenzo, G., Ostrovsky, R., & Persiano, G. (2004, May). Public key encryption with keyword search. In *International conference on the theory and applications of cryptographic techniques* (pp. 506-522). Berlin, Heidelberg: Springer Berlin Heidelberg.

[6] Kamble, A., Jiet, M. M., & Puri, C. (2024, April). Homomorphic Encryption and its Applications in Multi-Cloud Security. In *2024 International Conference on Inventive Computation Technologies (ICICT)* (pp. 1493-1499). IEEE.

[7] Ameur, Y., & Bouzefrane, S. (2023). Handling security issues by using homomorphic encryption in multi-cloud environment. *Procedia Computer Science*, *220*, 390-397.

[8] Salvakkam, D. B., & Pamula, R. (2024). Design of fully homomorphic multikey encryption scheme for secured cloud access and storage environment. *Journal of Intelligent Information Systems*, *62*(3), 641-663.

[9] He, H., Chen, R., Liu, C., Feng, K., & Zhou, X. (2021). An efficient ciphertext retrieval scheme based on homomorphic encryption for multiple data owners in hybrid cloud. *IEEE Access*, *9*, 168547-168557.

[10] IMTIYAZ KHAN, D. A., & HIJAB, M. (2024). SECURE AND EFFICIENT DATA SHARING SCHEME FOR MULTI-USER AND MULTI-OWNER SCENARIO IN FEDERATED CLOUD