Blockchain-Based Multi-User Dynamic Verifiable Searchable Encryption For Secure Cloud Storage

M. Barath[1], Mrs. K. Vijayalakshmi[2]
[2]Assist professor, MCA., M.Phil., B.Ed.
Thirumalai Engineering College, Kilambi - Kanchipuram

Abstract- *Cloud computing has become the dominant platform for scalable data storage and distributed services. Despite its advantages, outsourcing sensitive data to untrusted cloud servers introduces confidentiality and integrity risks. Dynamic Searchable Symmetric Encryption (DSSE) enables users to search encrypted data without revealing plaintext information, yet most existing schemes assume single-user environments or semi-honest servers. This paper presents a blockchain- based multi-user dynamic verifiable searchable encryption framework designed for malicious cloud settings. The proposed system stores lightweight index metadata on a blockchain to ensure tamper- proof verification while preserving storage efficiency. A Cuckoo filter- based index combined with a Merkle hash tree enables efficient and verifiable search operations. Secure multi-user key management is achieved using Diffie– Hellman key exchange, eliminating reliance on centralized trust authorities.*

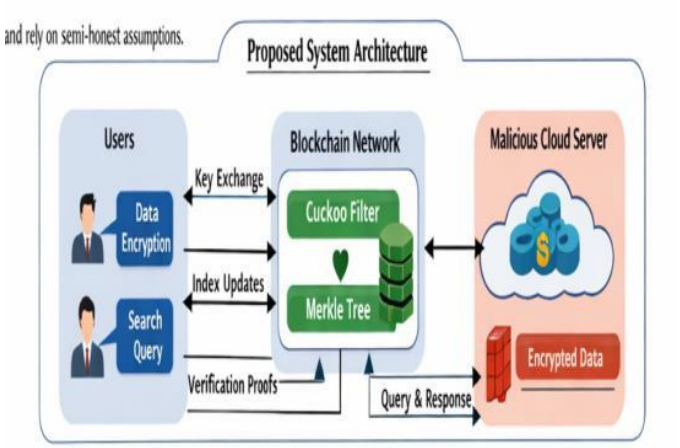
Keywords: Searchable Encryption, Blockchain, Cloud Security, Dynamic SSE, CuckooFilter, Merkle Hash Tree, Verifiable Search

I. INTRODUCTION

Cloud storage services provide scalable and cost-effective infrastructure for modern data management. However, storing sensitive information on external servers raises serious concerns regarding data privacy, integrity, and trust. Encryption protects confidentiality but complicates efficient retrieval. Searchable Encryption (SE) addresses this limitation by enabling search over encrypted data. Dynamic SSE further supports updates such as insertion and deletion. Nevertheless, many existing systems lack efficient multi- user support and strong verification mechanisms under malicious server assumptions. Blockchain technology offers immutability and decentralized trust, motivating its integration into secure cloud storage models.

II. PROPOSED SYSTEM ARCHITECTURE

A. System Layers



1. **User Layer:** Authorized users generate keys via Diffie–Hellman and interact with encrypted datasets.
2. **Client-Side Layer:** Performs local encryption and generates secure indices using Cuckoo filters and Merkle hash trees.
3. **Cloud Server Layer:** Stores encrypted data and processes search tokens without learning underlying keywords.
4. **Blockchain Layer:** Uses Hyper ledger Fabric to store
immutable indices and verification metadata, ensuring tamper-proof logs.

III. IMPLEMENTATION DETAILS

The system prototype is developed using **ASP.NET and C#** within the **Visual Studio** environment, with **SQL Server** as the backend.

- **Key Exchange:** Diffie- Hellman protocol ensures secure user-specific key distribution.
- **Verification:** A combination of Cuckoo filters and Merkle trees allows users to cryptographically verify search results.
- **Blockchain Integration:** Chaincode execution ensures honest operation processing and prevents collusion.

IV. PERFORMANCE EVALUATION

The use of blockchain for metadata storage rather than full datasets significantly reduces on-chain storage costs. The architecture achieves:

- **Collusion Resistance:** Protects against malicious servers and TPAs.
- **Dynamic Efficiency:** Supports secure insertion and deletion operations even with frequent updates.

V. CONCLUSION

This paper presented a blockchain-based multi-user dynamic verifiable searchable encryption framework for secure cloud storage. By integrating efficient indexing structures with decentralized verification, the proposed model enhances security, scalability, and resistance against malicious cloud behavior. The architecture demonstrates practical applicability for privacy- preserving cloud environments.

VI. ACKNOWLEDGMENTS

The author expresses sincere gratitude to the project guide, faculty members, and institution for their continuous support, valuable guidance, and encouragement throughout the development of this research work. Special thanks are extended to peers and colleagues for their constructive feedback and technical assistance.

REFERENCES

[1] D. Song, D. Wagner, and Perrig, "Practical Techniques for Searches on Encrypted Data," IEEE Symposium on Security and Privacy, 2000.
[2] R. Curtmola et al., "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," ACM CCS, 2006.
[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, 2012.
[4] M. Mitzenmacher, "Cuckoo Filters: Better Than Bloom," ACM CoNEXT, 2014.
[5] G. Wood, "Ethereum: A Secure Decentralized Transaction Ledger," 2014.
[6] Hyperledger Fabric Documentation, Linux Foundation.