PRIVACY PRESERVING RANKED MULTI KEYWORD SEARCH FOR MULTIPLE DATA OWNERS IN CLOUD COMPUTING

Project Reference No.: *49S_BE_1324*

College : Amruta Institute of Engineering and Management Sciences, Bidadi
Branch : Department Of Computer Science and Engeneering
Guide(S) : Prof. Shruthi N
Prof. Srinivasa R
Student(S) : Mr. Tejas S R
Mr. Adarsh B M
Mr. Rahul V
Mr. Dharibasava

Keywords:

Cloud Computing, Privacy Preserving, Multi-keyword Search, CP-ABE, Data Security.

Introduction:

Cloud computing has become a fundamental technology for storing and managing large-scale data due to its scalability, flexibility, and cost-effectiveness. Organizations across domains such as healthcare, finance, and smart grids rely on cloud platforms to store sensitive information. However, outsourcing data to the cloud raises serious concerns regarding data privacy and security, especially when multiple users need to access shared data. Traditional encryption techniques protect data but limit efficient searching over encrypted content.

To address this issue, researchers have proposed various secure search mechanisms, including Attribute-Based Encryption (ABE), which provides fine-grained access control. However, existing systems often lack efficient support for multi-keyword search and ranking over encrypted data, particularly in multi-owner environments.

The proposed project introduces a Privacy-Preserving Ranked Multi-Keyword Search (PRMKS) system that allows users to securely search encrypted data stored in the cloud. The system supports multiple data owners and ensures that data remains confidential during both storage and retrieval. By integrating Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with efficient search algorithms, the system enables secure, accurate, and ranked search results without revealing sensitive information.

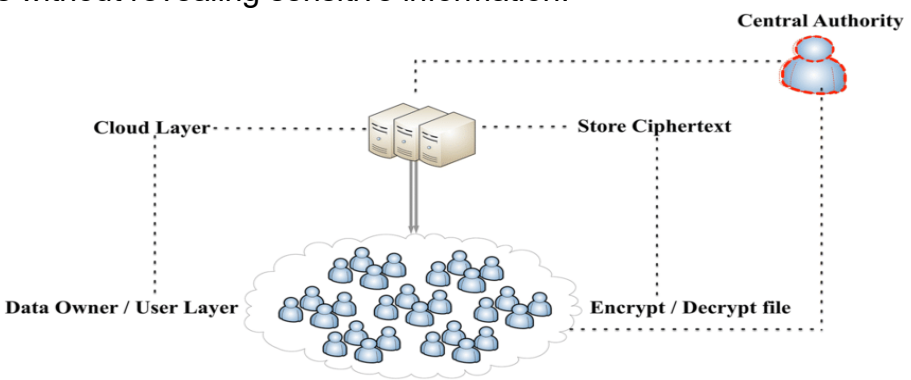

Figure 1: System Architecture of Privacy-Preserving Ranked Multi-Keyword Search in Cloud Computing

Objectives:

1. To design a secure cloud storage system using encryption.
2. To implement privacy-preserving multi-keyword search.
3. To support multiple data owners with secure access control.
4. To improve search efficiency using ranking mechanisms.
5. It aims to enable efficient multi-keyword search over encrypted data while supporting multiple data owners.
6. The project also focuses on implementing CP-ABE to provide fine-grained access control and secure data sharing.

Methodology:

The system uses CP-ABE for encryption and secure access control. Data is divided into blocks and encrypted before uploading to the cloud. Users perform multi-keyword search queries, and results are ranked based on relevance. Parallel processing is used to enhance performance.To improve efficiency, large data files are divided into smaller blocks, and each block is encrypted independently. This allows parallel processing of encryption and transmission, reducing overall system latency. The Attribute Authority (AA) manages user attributes and ensures that only authorized users receive valid private keys.When a user wants to access data, they submit a multi-keyword search query. The system processes the query using a secure search mechanism that matches keywords without decrypting the data. A ranking algorithm is applied to retrieve the most relevant files based on keyword similarity. The cloud server returns the encrypted results, and only authorized users can decrypt them using their private keys.The system is implemented using Python, Flask for backend processing, MySQL for database management, and PyCryptodome for cryptographic operations. This combination ensures scalability, efficiency, and strong security.

Result and Conclusion:

The proposed system ensures secure data sharing and efficient search over encrypted data. It successfully preserves user privacy while improving performance and scalability in multi-user environments. Experimental observations show that the use of parallel encryption significantly reduces processing time compared to traditional methods. The ranking mechanism improves user experience by providing relevant results quickly. The system also ensures that unauthorized users cannot access or decrypt sensitive data.Overall, the project proves that integrating CP-ABE with secure search techniques enhances both performance and security. The results confirm that the system is scalable and suitable for real-world applications where privacy is critical. The project concludes that privacy-preserving search systems are essential for modern cloud environments and can effectively address data security challenges.

References:

1. Sahai and Waters, "Fuzzy Identity-Based Encryption"
2. Vipul Goyal et al., "Attribute-Based Encryption for Fine-Grained Access Control"

3. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” *IEEE Symposium on Security and Privacy*, 2007.
4. N. Cao et al., “Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data,” *IEEE INFOCOM*, 2011.
5. K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” *IEEE Internet Computing*, 2012.
6. Research papers on CP-ABE and cloud security

Future Scope:

Future improvements include integrating AI-based search optimization, enhancing scalability for big data, and implementing real-time secure data analytics. Another improvement could involve implementing blockchain technology to enhance data integrity and transparency. The system can be adapted for mobile platforms to increase accessibility for users. Additionally, advanced ranking algorithms can be introduced to further optimize search performance.Security can be strengthened by incorporating multi-factor authentication and intrusion detection mechanisms. The project can also be extended to support cross-cloud environments and hybrid cloud architectures.Overall, the proposed system has strong potential for future development and can evolve into a fully scalable, enterprise-level cloud security solution.