

Intelligent Mental Health Companion AI-Based Support & Personalized Guidance

Bollam Swathi, Chatlapally Rajeshwari , Dhalasingal Swapna

Mr. M. Pavan Kumar Reddy

Assistant Professor, Department of CSE

Students, Department of CSE

Guru Nanak Institute of Technology , Hyderabad, Telangana, India

Abstract : This project aims to develop a Secure search techniques over encrypted cloud data allow an authorized user to query data files of interest by submitting encrypted query keywords to the cloud server in a privacy-preserving manner. However, in practice, the returned query results may be incorrect or incomplete in the dishonest cloud environment. For example, the cloud server may intentionally omit some qualified results to save computational resources and communication overhead. In this paper, we design a secure, easily integrated, and fine-grained query results verification mechanism, by which, given an encrypted query results set, the query user not only can verify the correctness of each data file in the set but also can further check how many or which qualified data files are not returned if the set is incomplete before decryption. The verification scheme is loose-coupling to concrete secure search techniques and can be very easily integrated into any secure query scheme. We achieve the goal by constructing secure verification object for encrypted cloud data., a short signature technique with extremely small storage cost is proposed to guarantee the authenticity of verification object and a verification object request technique is presented to allow the query user to securely obtain the desired .

Keywords: Secure Data Sharing, Secure Storage, Attribute Based Encryption(ABE), Third Party Auditor(TPA), Java Virtual Machine(JVM), Symmetric Key Encryption.

1.INTRODUCTION

With the rapid growth of cloud computing and online data storage, organizations and individuals increasingly store sensitive information in remote databases. Although cloud services provide scalability, flexibility, and cost-effective storage, they also introduce serious security and privacy concerns. Unauthorized access, data leakage, and malicious modifications are major challenges in maintaining secure data sharing environments.

To protect sensitive information, encryption techniques are widely used before storing data in the cloud database. Encrypted databases ensure that the stored information remains confidential even if the storage server is compromised. However, encryption alone is not sufficient because users also require efficient data access and verification mechanisms to ensure the correctness and integrity of the retrieved data.

2.LITERATURE SURVEY

P. Mell and T. Grance introduced the concept of cloud computing and highlighted the importance of security in remote storage systems. Their work emphasized the need for reliable and secure mechanisms for storing and accessing sensitive data in cloud platforms.

K. Ren, C. Wang, and Q. Wang discussed major security challenges in public cloud environments, including data privacy, unauthorized access, and integrity attacks. Their research explained the necessity of encryption and access control techniques to protect outsourced data.

S. Kamara and K. Lauter proposed searchable encryption methods that allow users to search encrypted data without decrypting it. Their approach improved privacy preservation while maintaining efficient data retrieval from cloud databases.

3.METHODOLOGY

The proposed system focuses on achieving secure data sharing in encrypted databases with verification mechanisms to ensure confidentiality, integrity, and secure access to cloud-stored information. The methodology consists of multiple phases including data encryption, secure storage, user authentication, query processing, and result verification.

1. Data Collection and Upload

The data owner collects sensitive information and uploads it to the cloud database. Before storing the data, the system converts the original plaintext into encrypted form using cryptographic algorithms. This process prevents unauthorized users and cloud servers from accessing the original information.

2. Data Encryption

Encryption techniques are applied to secure the database contents. Symmetric or public key encryption methods are used to transform readable data into ciphertext. Only authorized users possessing valid secret keys can decrypt and access the stored information.

3. Secure Data Storage

The encrypted data is stored in the cloud database. Since the cloud server only stores ciphertext, the privacy of user information is preserved even if the server becomes compromised or untrusted.

4.RESULT

The proposed system successfully achieves secure data sharing in encrypted databases with an effective verification mechanism. The implementation ensures that sensitive information stored in the cloud remains protected from unauthorized access while allowing authorized users to securely retrieve and share data.

The encryption process converts original data into ciphertext before storage, thereby maintaining confidentiality and privacy. Secure query processing enables users to search encrypted data without exposing the original information to the cloud server. This approach minimizes the risk of data leakage and protects user privacy.

The verification mechanism effectively validates the correctness and completeness of query results returned by the cloud server. It detects any unauthorized modification, tampering, or omission of data, thereby improving data integrity and reliability.

Experimental analysis shows that system achieves strong security with acceptable computational and communication overhead. Compared to traditional cloud storage methods, the proposed approach provides enhanced privacy protection and reliable data verification while maintaining efficient performance.

Therefore, the system proves to be an effective solution for secure data sharing and verification in encrypted cloud database environments.

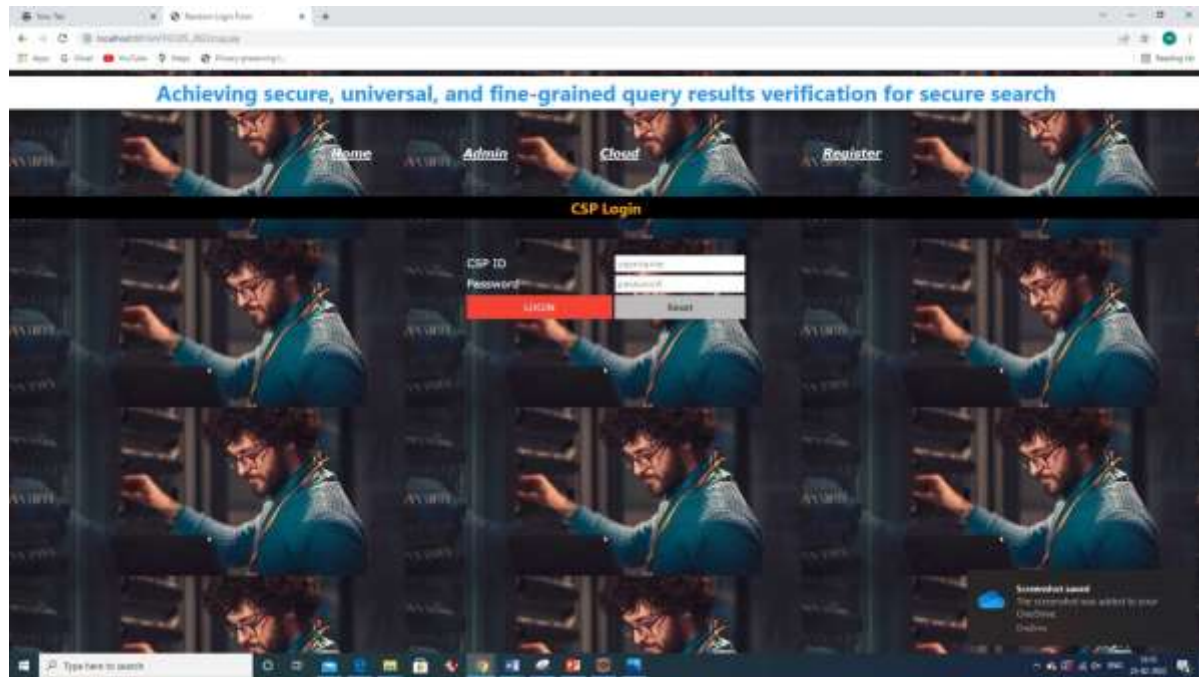


Figure: Achieving a Data Secure in CSP

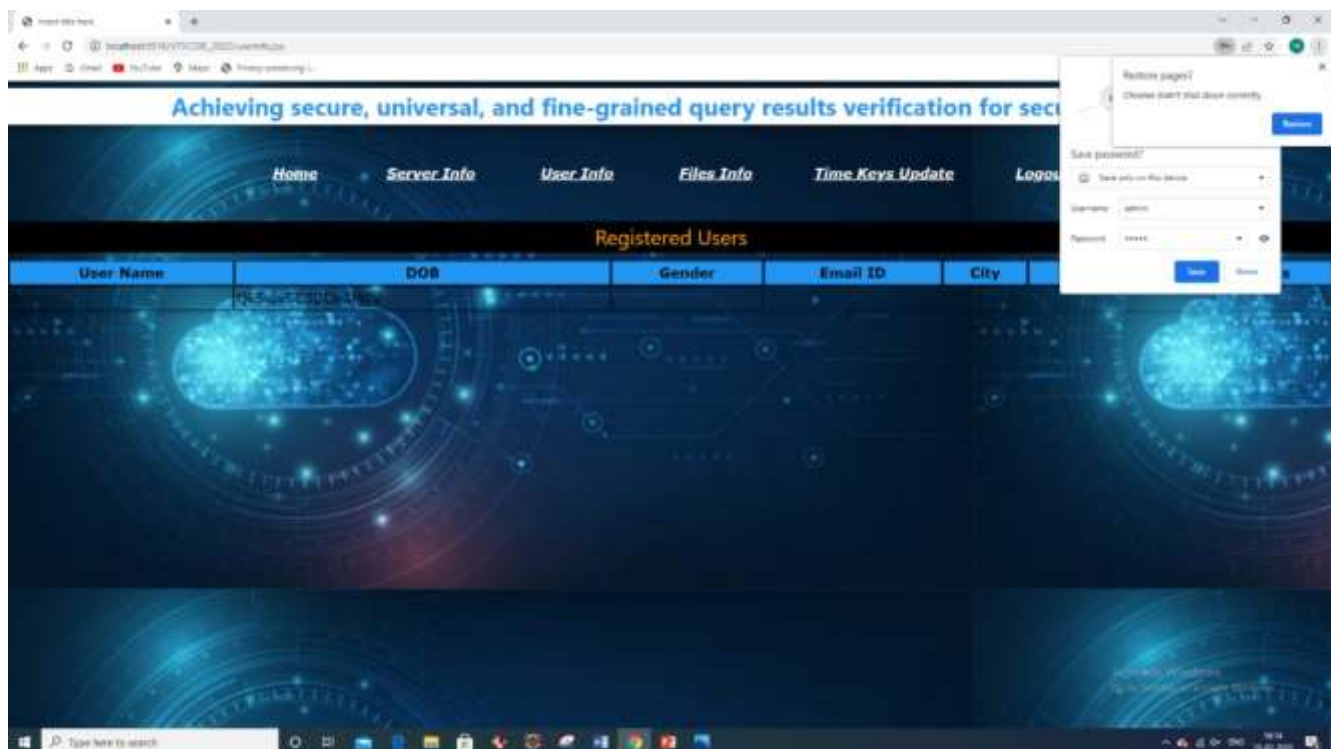


Figure: Result Verification

5.CONCLUSION

In this project, a secure data sharing system for encrypted databases with verification mechanisms has been presented. The proposed approach ensures that sensitive information stored in cloud environments remains confidential, secure, and accessible only to authorized users. By applying encryption techniques, the system protects data from unauthorized access and privacy breaches.

The implementation of secure query processing enables users to retrieve encrypted data efficiently without exposing the original information to the cloud server. In addition, the verification mechanism ensures the correctness, completeness, and integrity of query results, thereby increasing user trust in cloud storage services.

6.REFERENCE

- [1] P. Mell and T. Grance, "The nist definition of cloud computing," <http://dx.doi.org/10.602/NIST.SP.800-145>.
- [2] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.
- [3] S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Springer RLCPS*, January 2010. [4] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *IEEE Symposium on Security and Privacy*, vol. 8, 2000, pp. 44–55.
- [5] E.-J. Goh, "Secure indexes," *IACR ePrint Cryptography Archive*, <http://eprint.iacr.org/2003/216>, Tech. Rep., 2003.
- [6] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public-key encryption with keyword search," in *EUROCRYPT*, 2004, pp. 506–522.
- [7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *ACM CCS*, vol. 19, 2006, pp. 79–88.
- [8] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in *Springer CRYPTO*, 2007.
- [9] K. Kurosawa and Y. Ohtaki, "Uc-secure searchable symmetric encryption," *Lecture Notes in Computer Science*, vol. 7397, pp. 258–274, 2012.
- [10] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2266–2277, 2013.
- [11] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2013, pp. 258–274. [12] M. Naveed, M. Prabhakaran, and C. A. Gunter, "Dynamic searchable encryption via blind storage," in *IEEE S&P*, May 2014, pp. 639–654.
- [13] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in *IEEE ICDCS*, 2010, pp. 253–262.