International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Ensuring Privacy and Recovery: Public Key Encryption for Secure Data De-Duplication with Keyword Search

Ms. Rajashree Sutrawe, Gundlapally Harika, Karthik Reddy, Megansh
CSE, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India
CSE, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India
CSE, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

ABSTRACT
In the current era of information explosion, user's demand for data storage is increasing, and data on the cloud has become the first choice of users and enterprises. Clous storage facilitates the backup and sharing of data, efficiently reducing user's storage expenses. The duplicate data of different users is stored multiple times, leading to a sudden decrease in the storage utilization of cloud servers. Data stored in plaintext form can directly remove duplicate data, while cloud servers are semi-trusted and usually need to achieve secure de-duplication and recover data in cipher text for different users, and relationship of trapdoor are equal in cipher text to achieve secure de-duplication. The proposed scheme is secure and efficient through security analysis and experimental simulation analysis.

Keywords: Data De-duplication, Mobile Edge Computing, Authentication, Security, Cryptographic Techniques, Data Integrity.

I. INTRODUCTION

As a major service provided by cloud computing technology, cloud storage enables users to backup and share data easily and quickly, which can efficiently reduce users' storage expenses and improve work efficiency. With the increasing maturity of cloud computing technology. There are many Cloud Service Providers (CSP) in the market, such as Baidu Cloud, Amazon Cloud, and other famous CSPs

Public key encryption emerges as a foundational tool in this quest, offering a robust mechanism to protect data integrity and confidentiality in transit and at rest. At its core, public key encryption leverages asymmetric cryptographic techniques, where each user possesses a pair of keys: a public key for encryption and a private key for authorized parties possessing the corresponding private key can decrypt it, but also enables secure data sharing and storing without necessitating a prior exchange of secret keys. In the context of secure data de-duplication with keyword search, integrating public key encryption fortifies privacy by allowing users to securely

upload and query data while preventing unauthorized access. Moreover, the inherent separation of keys facilitates recovery in the event of key compromise or loss, enabling seamless restoration of data accessibility
Without sacrificing security. By harnessing the power of public key encryption, organizations can forge a path towards robust data protection, bolstering trust and resilience in their data management practices.

The introduction may touch upon the challenges posed by traditional encryption methods in scenarios where data deduplication and keyword search functionalities are required simultaneously. It would likely introduce the concept of public key encryption as a potential solution to

address these challenges, highlighting its ability to provide both security and efficiency in scenarios involving data deduplication and keyword search operations. Additionally, it might briefly discuss the objectives and contributions of the proposed approach.

II. METHODS AND MATERIAL

Proxy re-encryption:
Proxy re-encryption is a cryptographic technique that allows a proxy entity to transform ciphertext encrypted under one public key into ciphertext encrypted under another public key. This technique can be utilized to delegate search operations to a trusted proxy server without revealing the original search query.

Advanced Encryption Standard:
Advanced Encryption Standard operates on fixed-size blocks of data, typically 128 bits in length, and supports three different key lengths: 128, 192 and 256 bits. The algorithm consists of several rounds of secret encryption keys. Each round consists of four distinct operations: Sub Bytes, Shift Rows, Mix Columns, and Add Round Key.

AES is widely used regarded for its security, efficiency, and simplicity, making it suitable for implementation in both software and hardware across a wide range of computing platforms. It has become the cornerstone of modern cryptography and is used extensively to secure data transmission, storage, and communication in various applications and industries.

I. RESULTS AND DISCUSSION

System Implementation and Functionality:
This subsection outlines the successful implementation of the proposed system, including the integration of public key encryption, secure data deduplication, and keyword search functionalities. It discusses the key components of the system architecture, such as encryption algorithm used, deduplication techniques employed, and mechanisms for keyword search.

Privacy Preservation:
The discussion delves into how the implemented system effectively preserves the data privacy. It examines how encryption mechanism safeguard sensitive information ensuring that only authorized users can access the decrypted data. It also explores how privacy is maintained during duplication and keyword search operations.

Efficiency and Performance:
It evaluates the efficiency and performance of the system in terms of storage optimization, search speed, and computational overhead. It discusses the impact of encryption and deduplication on data storage requirements and examines the computational cost of keyword search operations. It also explores strategies for optimizing system performance while maintaining security.

Recovery Mechanism:
It explores the recovery mechanisms implemented in the system to ensure data accessibility in case of emergencies. It discusses key management practices, including key generation, distribution, and recovery procedures. It also addresses how the system handles key loss or compromise scenarios, ensuring continuous access to encrypted data.

A. Literature Survey

Title: "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data"
Author(s): Cong Wang, Ning Cao, Kui Ren, and Wenjing Lou
Year: 2012
Description:
This work introduces a practical solution for secure ranked keyword search over encrypted cloud data. While not specially focused on data duplication, the techniques presented could be adapted to incorporate deduplication functionality, contributing to the broader discussion on privacy-preserving search over encrypted data.

Title:" Privacy-Preserving Public Auditing for Secure Cloud Storage"
Author(s): Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou
Year:2010

Description:

Although primarily concerned with public auditing for cloud storage, this project discusses the techniques for ensuring data integrity and privacy in outsourced storage scenarios. The concepts and cryptographic primitives presented are relevant to the broader context of secure data management, including deduplication and keyword search functionalities.

B. System Architecture

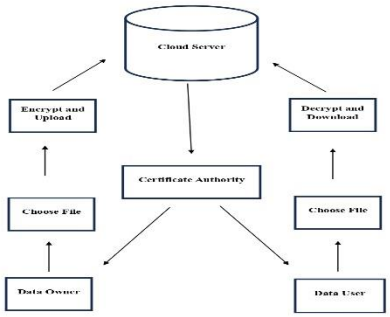
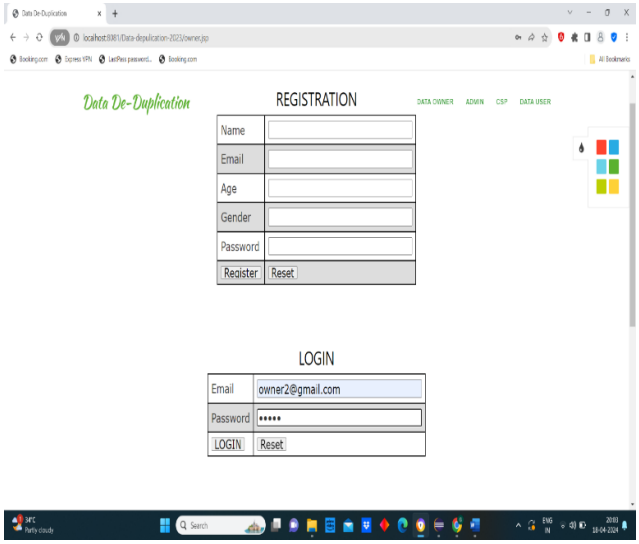


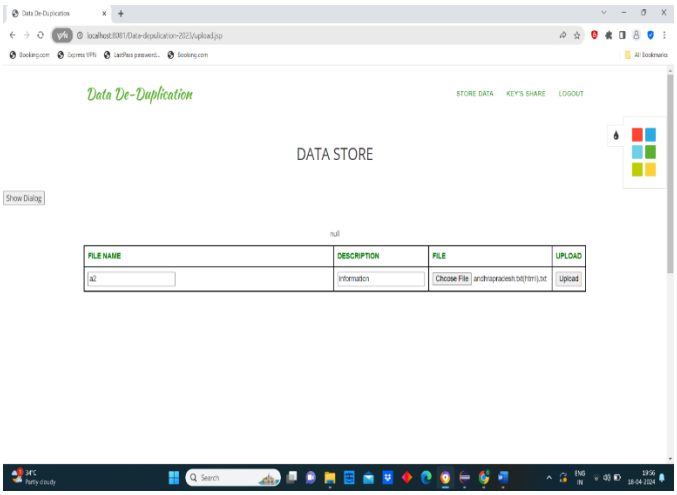
Fig:Data Deduplication

C. Figures and Tables

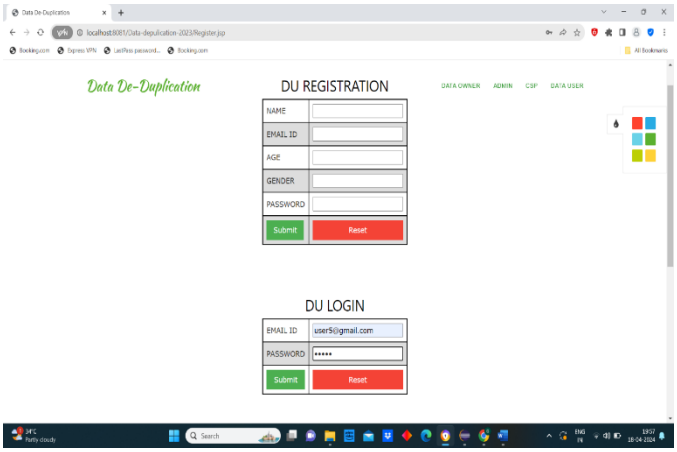


Owner Registration and Login Page:

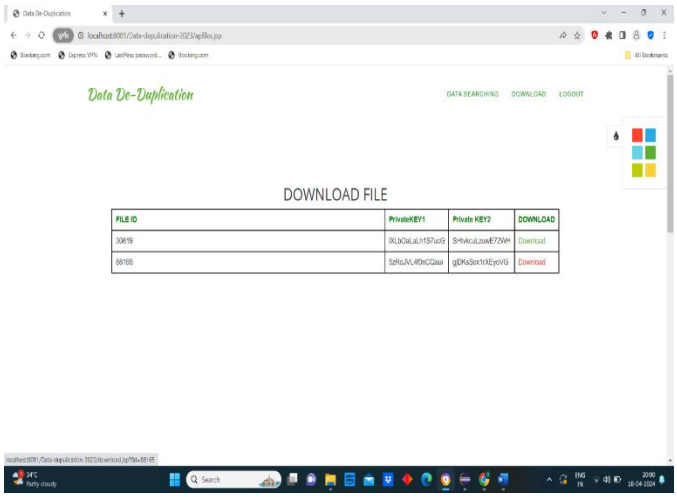
Storing Data:



User Registration and Login Page:



Downloading File:



IV.CONCLUSION

It provided a robust solution for safeguarding sensitive information. By leveraging advanced encryption techniques, secure storage infrastructure, and key management systems, we've bolstered the integrity of data transmission and protected cryptographic keys from unauthorized access. Additionally, comprehensive testing and validation have been conducted to identify and mitigate potential vulnerabilities, ensuring compliance with privacy regulations and industry standards

V. REFERENCES

[1] Boneh, D., Crescenzo, G. , Ostrovsky , R. , & Persiana, G. (2004). Public key encryption with keyword search. In EUROCRYPT (Vol. 3027, pp. 506-522).

[2] Bellare, M., Boldreva, A., & O'Neill, A. (2007). Deterministic and efficiently searchable encryption. In CRYPTO (Vol. 4622, pp. 535-522).

[3] Wang, C., Cao, N., Ren , K., & Lou, W. (2011). Secure deduplication with efficient and reliable convergent key management. 1469-1481.

[4] Juels, A., & Kaliski Jr, B. S. 92007). Pros: Proofs of retrievability for large files. In ACM conference on computer and communications security (pp. 584-597).