IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710


# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304258 |

# DSDDR: Data Secure De-Duplication and Recovery Based on Private Key Encryption

**Meenakshi Simha, Ramdas Dheeraj, K Nithin Kumar, K Rohith Reddy**

Assistant Professor, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

**ABSTRACT:** This dissertation proposes a novel method for secure data de-duplication in multi-user cloud storage systems. Utilizing Private Key Encryption, it enhances security by encrypting identical data with each user's unique key, mitigating privacy breaches. The system emphasizes user-centric security, integrating private keys for encryption and decryption, granting users control over access permissions. By eliminating redundant data, storage utilization is optimized, reducing overheads and operational costs. Robust server-side encryption algorithms ensure security without burdening client devices. The solution is scalable and adaptable, catering to diverse cloud storage setups, from small-scale to large-scale infrastructures.

## I. INTRODUCTION

In the modern digital realm, organizations grapple with the dual challenge of managing vast data volumes while upholding stringent security standards. "Data Secure De-Duplication and Recovery Based on Private Key Encryption" offers a pioneering solution by integrating encryption, de-duplication, and recovery mechanisms. At its core, private key encryption ensures data confidentiality by utilizing a single, confidential key for both encryption and decryption, thwarting unauthorized access.

By incorporating private key encryption into the de-duplication process, this approach merges data efficiency with security. Duplicate data blocks are encrypted using unique private keys, ensuring secure storage and retrieval only by authorized users. This strategy mitigates the risk of data exposure, even in scenarios of unauthorized access to storage repositories.

Moreover, the system fortifies data resilience through robust recovery mechanisms, facilitating swift and reliable data restoration in various scenarios. By optimizing storage resources without compromising security, enhancing operational efficiency, and bolstering data resilience, organizations can navigate digital challenges with confidence and agility. "Data Secure De-Duplication and Recovery Based on Private Key Encryption" signifies a pivotal advancement in data management, equipping organizations to safeguard their digital assets and harness the full potential of data-driven insights.

## II. RELATED WORK

**1. Text file feature extraction in encrypted domain:** Leveraging encryption techniques similar to private key encryption, this work focuses on efficient retrieval of encrypted data, ensuring confidentiality and security.

**2. Secure Text file retrieval with multiple keys:** This approach mirrors the project's emphasis on user-centric security by employing encryption with multiple keys, granting users control over access permissions and ensuring data confidentiality.

**3. Instant Crypto Gram:** The proposed secure picture retrieval service aligns with the project's goal of securely retrieving data from cloud servers while maintaining user privacy through encryption techniques.

**4. Epcbir:** This research shares similarities with the project's focus on robust server-side encryption algorithms and

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304258 |

efficient data retrieval mechanisms in cloud computing environments.

**5. Content-based multi-source encrypted file retrieval in clouds with privacy preservation:** This work emphasizes the importance of preserving privacy while enabling efficient data retrieval, which resonates with the project's goal of user-centric security and data resilience.

## III. PROPOSED SYSTEM

In the proposed system, RSA encryption serves as the cornerstone of data security, offering a robust safeguarding mechanism for text files. Each text file is encrypted using a unique public-private key pair, ensuring stringent confidentiality and integrity measures. With RSA encryption, files are encoded with their respective public keys, while the corresponding private keys are securely stored, accessible only to authorized users. This asymmetric encryption scheme provides a robust defense against unauthorized access and tampering, bolstering the overall resilience of the system against potential cyber threats.

Encrypted text files are securely stored in a backup database, shielding sensitive information from external threats. In the event of database crashes or data loss, the encrypted backup files can be retrieved and decrypted using their associated private keys, facilitating seamless restoration to the original database. This ensures data integrity and confidentiality throughout the backup and recovery process, providing users with peace of mind regarding their sensitive information's security.

Moreover, the utilization of RSA encryption not only enhances data security but also streamlines recovery processes, minimizing downtime and ensuring business continuity. The system's architecture is designed to efficiently handle recovery operations, allowing for swift restoration of data without compromising security measures. Stringent access controls are implemented to safeguard private keys, preventing unauthorized decryption attempts and mitigating the risk of data breaches.

Overall, the incorporation of RSA encryption significantly enhances the system's security posture, offering a robust and effective means to protect sensitive text files throughout their lifecycle. From encryption to storage and recovery, the system ensures comprehensive data protection, aligning with industry best practices and regulatory requirements for information security.

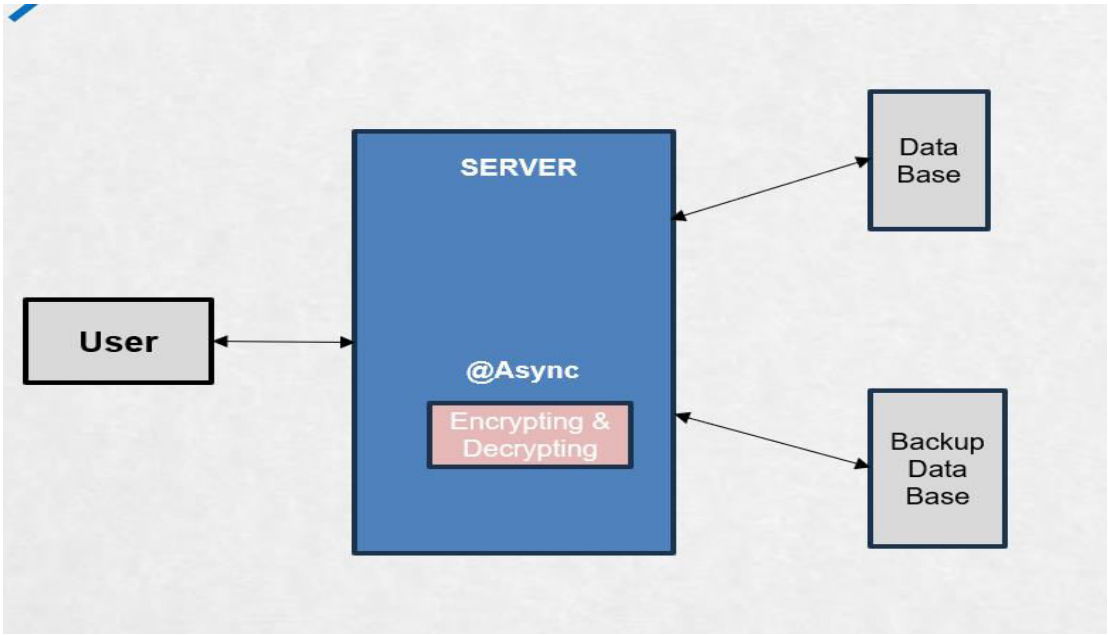



Figure 1 Architectural Diagram

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304258 |

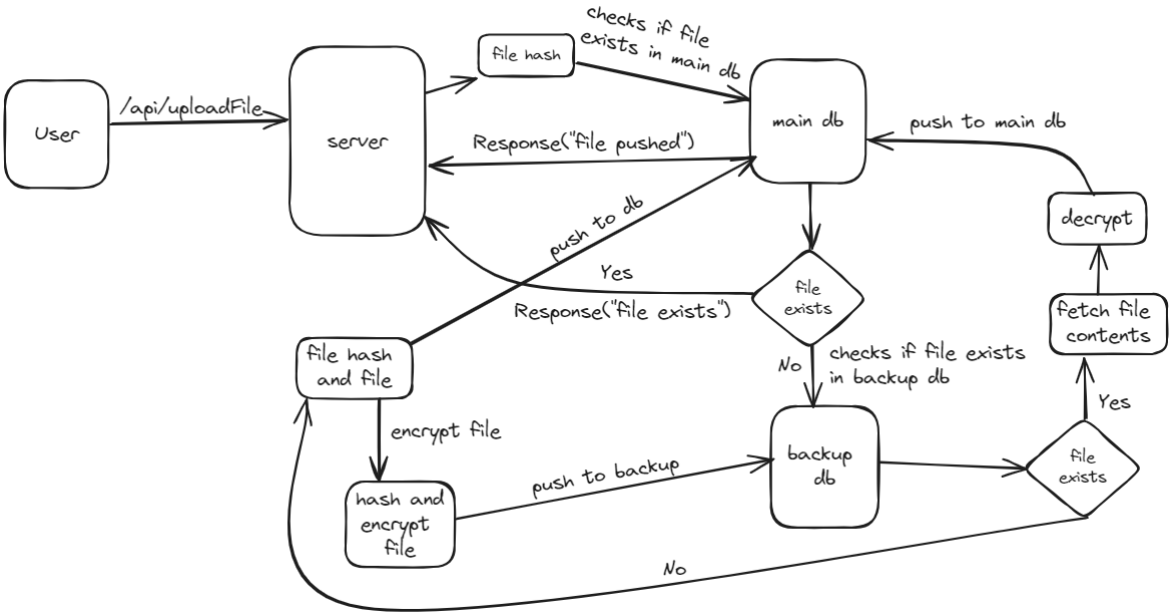
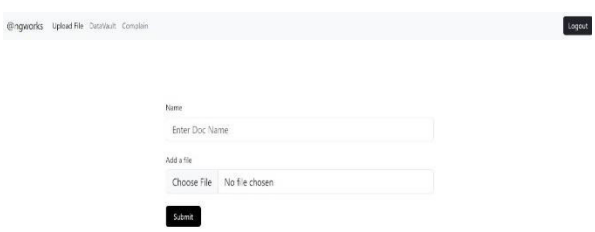
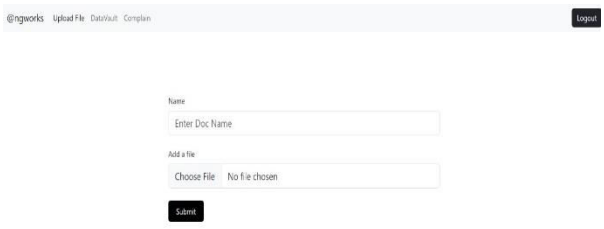



Figure 2 Dataflow Diagram

## IV. RESULTS




The user can upload the text file and also recover the lost file using our fetch techniques.

## V. CONCLUSION

The outlined process for secure data deduplication, complemented by private key encryption, represents a comprehensive and sophisticated solution for managing text files within the platform. By encrypting newly uploaded text files and storing them securely in the backup storage, the system ensures confidentiality and protection against unauthorized access. Concurrently, the storage of metadata containing unique identifiers in both the backup and original Firestore databases enables efficient detection of duplicate uploads, ensuring data integrity throughout the process. This meticulous approach to managing file duplicates underscores the platform's commitment to optimizing resource utilization while preserving data coherence and accessibility for users.

In instances of duplicate file detection, the system's selective copying and decryption of matched encrypted files from the backup database demonstrate a strategic balance between storage efficiency and data integrity. Leveraging private key encryption throughout the process maintains stringent security measures, ensuring that only authorized

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304258 |

parties with the corresponding decryption key can access and decrypt the file content. Through this methodical approach, the platform achieves secure data deduplication, mitigating storage overhead while upholding confidentiality and integrity standards. Overall, this process represents a robust and efficient solution for managing text files securely within the platform, enhancing user experience and bolstering overall data security.

## REFERENCES

[1]. W. Zhang, B. Qin, X. Dong, and A. Tian, ''Public-key encryption with bidirectional keyword search and its application to encrypted emails,'' Comput. Standards Interfaces, vol. 78, Oct. 2021, Art. no. 103542.
[2]. B. Chen, L. Wu, S. Zeadally, and D. He, ''Dual-server public-key authenticated encryption with keyword search,'' IEEE Trans. Cloud Comput., vol. 10, no. 1, pp. 322–333, Jan. 2022.
[3]. R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, ''A new general framework for secure public key encryption with keyword search,'' in Proc. 20th Australas. Conf., E. Foo and D. Stebila, Eds. Brisbane, QLD, Australia, 2015, pp. 59–76.
[4]. Y. Lu and J. Li, ''Lightweight public key authenticated encryption with keyword search against adaptively-chosen-targets adversaries for mobile devices,'' IEEE Trans. Mobile Comput., vol. 21, no. 12, pp. 4397–4409, Dec. 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details