



Segshare:Secure group file sharing in the cloud using enclaves

Prof.Ninad More¹, Omraj Nichal², Akash Shinde³, Abhishek Ahire⁴, Anuj Bhojane⁵

D. Y. Patil Institute Of Engineering & Technology, Pune¹⁻⁵

Abstract— This paper introduces a solution called Tenant-Oriented Duplication Integrity Checking Scheme (TDIC) to address the challenges faced in the Software-as-a-Service (SaaS) environment. In SaaS, tenants often create multiple customized duplicates of their data and distribute them across different data nodes for reliability. However, untrustworthy service providers can manipulate or delete the tenants' data, and they may store fewer copies than required. To overcome these issues, TDIC proposes a challenge-response model based on tuples sampling. It also introduces a new authentication structure called Tenant Duplication Authentication Structure (TDAS) that relies on tenant physical tuples. By incorporating homomorphism labels, TDIC enables data duplication verification without the need for local copies. Moreover, TDIC utilizes periodic random sampling to reduce complexity in constructing verification objects on the service provider's side and minimize unnecessary communication overhead. Overall, TDIC offers an effective approach to ensuring data integrity in SaaS by introducing a tuples sample-based challenge-response model and leveraging TDAS with homomorphism labels. It simplifies the verification process and enhances security in the face of untrustworthy service providers.

Keywords: CloudComputing,Saas,Encyption,Data Sharing

I. INTRODUCTION

Ensuring data integrity in the Software-as-a-Service (SaaS) environment is crucial due to concerns regarding the trustworthiness of remote service providers. These providers have the potential to manipulate or delete tenants' data, posing a threat to data security. Moreover, as all data replicas appear identical, untrustworthy providers can deceive tenants by storing fewer copies than required. The existing research primarily focuses on independent data storage modes rather than shared ones, such as in SaaS. The traditional approach of file partitions is not effective in shared physical storage modes as it compromises data isolation and complicates integrity verification. In order to address these challenges, tenants require a mechanism to verify the integrity of their remote data without the need for possessing local copies. This ensures that the data stored by service providers remains intact and secure, even in a shared storage environment like SaaS.

II. MOTIVATION

Data deduplication is a process that reduces storage capacity needs by eliminating excessive data copies. It can be performed in two ways: inline deduplication, which happens during data writing into the storage system, and background deduplication, which removes duplicates after the data has been written to disk.

III. PROBLEM DEFINITION

A proposed solution aims to enhance reliability and security in cloud-based deduplication systems by integrating distributed storage servers. This approach improves fault tolerance and ensures data confidentiality through secret sharing techniques. To enable deduplication, a cryptographic hash value is computed and sent to each storage server as a fingerprint for the stored fragment.

SOFTWARE REQUIREMENT

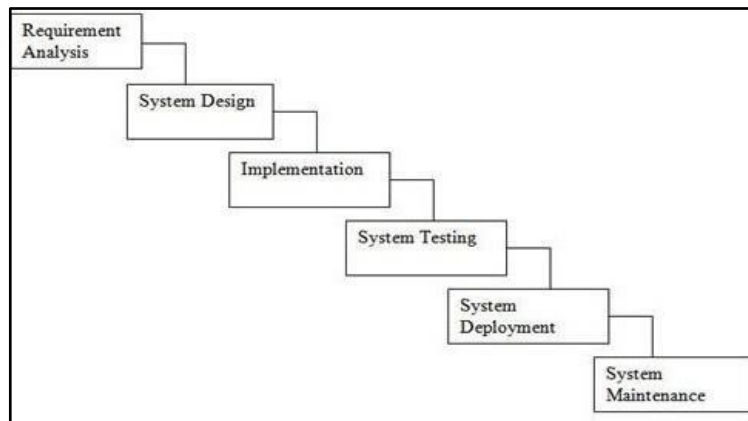
Purpose and Scope of Document

The software requirements specification (SRS) is a crucial document that describes the software system to be developed. It outlines the intended functionality and performance expectations while specifying the necessary requirements for the project. The SRS ensures that the software aligns with the objectives and needs of stakeholders.



Data deduplication is highly advantageous, but ensuring the security of client data poses challenges. Existing encryption methods do not support information deduplication, as they require individual customers to encrypt data with their own keys. This study aims to create identical data duplicates for ten different customers, addressing this limitation.

The SRS includes components such as a purpose statement and a comprehensive list of requirements. Its primary goal is to define the software's objectives and fulfill the needs of stakeholders, including businesses and users.. Moreover, it aims to detect ciphertext effectively, rendering deduplication impossible.



Software Quality Attributes

1. Our software possesses several quality attributes, as described below:
2. Adaptability: The software can be easily adapted by all users.
3. Availability: The software is freely accessible to all users, ensuring easy availability.
4. Maintainability: Software developers can easily maintain the project after its deployment, addressing any errors that may occur.
5. Reliability: The software demonstrates superior performance, enhancing its reliability.
6. User Friendliness: Being a GUI application, the software generates user-friendly output, ensuring a pleasant user experience..

IDE :Eclipse

Best Integrated Development Environment as it gives possible suggestions at the time of typing code snippets that makes typing feasible and fast

Coding Language :Java

Operating System : Windows 7 or more

Latest Operating System that supports all type of installation and development Environment.

RAM : 4 GB or above

Hard Disk : 20 GB

Processor : Intel I3 Processor and above

❖ SDLC Model

The article examines SDLC models, including Agile, and their role in software development. It highlights the initial analysis phase, encompassing technology selection and team workload. SDLC models form a crucial part of software development, representing a continuous process from project initiation to retirement. These models are diverse, falling into distinct groups with unique characteristics and limitations.

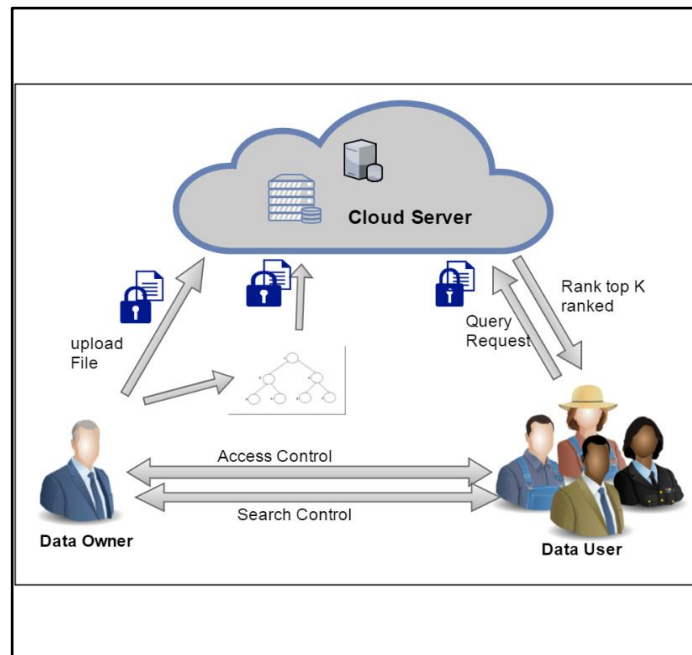


Fig - System Architecture

Overview of Project Modules

This chapter provides an overview of the time taken for each task in the project, such as the preliminary survey, literature survey, software requirements, system design, implementation, testing, and report submission. It also focuses on the stakeholder list, which includes information about the project type, customer, user, and project members involved.

1. Admin Module:

- Enables user registration, login, and account management.
- Allows searching and purchasing products.
- Provides access to transaction history and additional information.

2. View and Authorize Users Module:

- Allows the admin to view registered users and their details.
- Provides authorization authority to the admin.

3. View Charts Results Module:

- Offers functionalities like product search ratio, keyword search results, and product review rank results.

4. Ecommerce User Module:

- Users register and store their details in the database.
- Allows login and operations such as adding products, viewing product reviews, and transaction history.

5. End User Module:

- Users register and login with authorized credentials.
- Operations include managing accounts, searching and purchasing products, and viewing transaction history..

LIMITATIONS :-

One drawback of Post-Process Deduplication is that it stores all data in full, resulting in the same space occupation as non-deduplicated data. Size reduction is only achieved after the scheduled execution of the Deduplication operation.

APPLICATIONS :-

In data deduplication, redundant data is identified and eliminated, allowing for storage of a single instance. This technique helps in reducing storage requirements by analyzing data and identifying duplicate byte patterns.

ASSUMPTIONS AND DEPENDENCIES:-


The authenticated model in data deduplication utilizes general convergent encryption and assumes users have access to encryption keys and management methods. Block-level deduplication is used to reduce storage space. Encryption keys are generated based on a consistent configuration of data dependency from the chunk data..



OUTPUT

Text Encrypted data with Authorized Deduplication

Home | Registration | Admin



Cloud Storage

Sidebar Menu

- Home
- Registration
- Admin

User Login

User Id:

Password:

Login

Text Encrypted data with Authorized Deduplication

Home | Registration | Admin



Cloud Storage

Sidebar Menu

- Home
- Registration
- Admin

Registration Form

First Name: Last Name:

E-mail id: Date of Birth:

Phone No: Address:

User id: Role:

Password:

Register Reset

Text Encrypted data with Authorized Deduplication

Home | Upload File | Download File | Share File | Operation on File | Graph | Logout



Cloud Storage

Sidebar Menu


- Home
- Upload File
- Download File
- Share File
- Operation on File
- Graph
- Logout

Welcome abc

Cloud computing provides seemingly unlimited virtualized resources to users as services across the whole Internet, while hiding platform and implementation details. Today's cloud service providers offer both highly available storage and massively parallel computing resources at relatively low costs. As cloud computing becomes prevalent, an increasing amount of data is being stored in the cloud and shared by users with specified privileges, which define the access rights of the stored data. One critical challenge of cloud storage services is the management of the ever-increasing volume of data.

Text Encrypted data with Authorized Deduplication

Home | Upload File | Download File | Share File | Operation on File | Graph | Logout



Cloud Storage

Sidebar Menu

- Home
- Upload File
- Download File
- Share File
- Operation on File
- Graph
- Logout

Welcome abc

Choose File To Upload

Student

Choose File No file chosen

submit



CONCLUSION

Our research proposes DupLESS, a system for secure outsourced storage with deduplication. It combines a CE-type base MLE scheme with message-derived keys obtained from a shared key server. This ensures resistance to brute-force attacks and efficient data retrieval.

FUTURE SCOPE

In DupLESS, clients securely interact with the key server (KS) using a protocol for oblivious pseudo-random functions (PRFs). This ensures that the KS can incorporate secret material into per-message keys without gaining knowledge about clients' stored files. The system provides strong security against external attacks on the storage system and communication channels, with no leaked information beyond file lengths, equality, and access patterns. Even if components of the system are compromised, the security of DupLESS gracefully degrades. If a client is compromised, decrypting another client's ciphertext requires an online brute-force attack, which can be slowed down by a rate-limited KS. If the KS is compromised, the attacker still needs to perform an offline brute-force attack, maintaining security similar to traditional schemes.

Despite its enhanced security, DupLESS has a modest impact on performance and storage requirements compared to the base system. This is achieved through optimization of the client-to-KS protocol and minimizing interactions with the storage system. DupLESS can seamlessly integrate with various storage systems, as demonstrated by our prototypes for Dropbox and Google Drive.

In summary, DupLESS ensures secure interactions between clients and the key server, providing strong security guarantees while maintaining acceptable performance and storage requirements.

REFERENCES

- 1 Bitcasa, infinite storage. <http://www.bitcasa.com/>.
- 2 Ciphertite data backup. <http://www.ciphertite.com/>.
- 3 Dropbox, a file-storage and sharing service. <http://www.dropbox.com/>.
- 4 Dupless source code. <http://cseweb.ucsd.edu/users/skeelvec/dupless>.
- 5 The Flud backup system. <http://flud.org/wiki/Architecture>.
- 6 GNUnet, a framework for secure peer-to-peer networking. <https://gnunet.org/>.
- 7 Google Drive. <http://drive.google.com>.
- 8 ADYA, A., BOLOSKY, W., CASTRO, M., CERMAK, G., CHAIKEN, R., DOUCEUR, J., HOWELL, J., LORCH, J., THEIMER, M., AND WATTENHOFER, R. Farsite: Federated, available, and reliable storage for an incompletely trusted environment. ACM SIGOPS Operating Systems Review 36, SI (2002), 1–14.
- 9 AMAZON. Amazon Elastic Block Store (EBS). <http://aws.amazon.com/ebs>.