# AUTHORIZED REDUNDANT CHECK SUPPORT IN A HYBRID CLOUD ENVIRONMENT

Tirupattura Jaswanth Babu, M S Shashidhara

*Student, Professor, Department of Computer Application*

*A.M.C.Engineering College, Bengaluru, India*

## Abstract

*Data deduplication stands as a crucial technique in data compression to eliminate redundant copies of recurring data. Its widespread use in cloud storage effectively minimizes storage space and optimizes bandwidth consumption. To ensure the confidentiality of sensitive data while facilitating deduplication, a convergent encryption approach has been developed to encrypt the data before outsourcing. This research represents the pioneering effort to explicitly address the concept of authorized data deduplication, aiming to enhance data security. Unlike conventional deduplication systems, our approach incorporates the differential privileges of users in the duplicate check process, in addition to analyzing the data itself. Furthermore, we present various innovative deduplication architectures that enable authorized duplicate check within a hybrid cloud framework. Through security analysis, we demonstrate that our approach meets the security requirements outlined in the proposed security model. As a proof of concept, we have implemented a prototype of our authorized duplicate check mechanism and conducted test bed experiments. The results showcase that our proposed technique for authorized duplicate check incurs minimal overhead compared to typical operations.*

## INTRODUCTION

The cloud computing industry is currently experiencing remarkable growth, offering immense benefits in the field of virtualization and simplifying the deployment of models like client/server architectures. The level of assistance it provides surpasses our expectations, offering a diverse range of services including web services, software services, distributed computing, grid computing, utility computing, and autonomic computing. Cloud computing grants users access to a comprehensive suite of facilities and services, featuring a user-friendly architecture, reduced operational costs, and a delivery platform accessible to both individuals and businesses. Service-oriented architecture (SOA) and virtualization technologies have been adapted to align with the principles of cloud computing. Leading entities like Amazon, which originated as an online bookstore, exemplify the fundamental essence of cloud outsourcing to a third party. However, the proliferation of technology offering diverse on-demand services through virtualization brings about certain security concerns. Despite the cloud's provision of security measures at various levels, it is not without vulnerabilities. These weaknesses encompass inadequate security and access control, insecure data transmission over networks, and potential access to sensitive information by multiple virtual machines. The majority of users express anxiety when utilizing cloud computing due to apprehensions regarding potential consequences

### . Writing REVIEW

#### 1. EXISTING SYSTEM

• When the administrator approves a user in a deduplication system, they are allocated a specific set of privileges during the system initialization phase.

• Although standard encryption ensures the data's confidentiality, it is unsuitable for data deduplication due to its incompatibility with the process.

• In this scenario, achieving deduplication is unattainable as different cipher messages will be generated for identical data copies created by multiple users.

**2. PROPOSED SYSTEM**

• The architecture of data duplication systems has garnered significant attention from researchers due to its practical applications.

• In this context, the private cloud serves as an intermediary, facilitating secure duplicate check operations while maintaining distinct user privileges.

• The sole aspect of the data owner's obligations that is outsourced is the storage of their data, which is accomplished via the utilization of public cloud services.

## MODULES:

**1 .Data Users Module**
**2 .Cloud Service Providers**
**3 .Private Cloud Module**
**4 .Secure Deduplication System**

**> DESCRIPTION OF MODULES**

**1. Cloud Service Provider**

Cloud Service Provider (CSP)

In this module, we introduce the Cloud Service Provider component, which represents a company providing public cloud data storage services.

The CSP undertakes the responsibility of data outsourcing and storage on behalf of the users.

To optimize storage expenses, the CSP implements deduplication techniques to eliminate redundant data storage, retaining only distinct information.

For the purposes of this study, we make the assumption that the CSP is consistently accessible online and possesses abundant storage capacity and computational resources.

**2.Module for Data Users**

An end-user refers to an entity seeking to delegate their data storage needs to the CSP, enabling future access.

Within a deduplication-enabled storage system, the end-user uploads solely unique data and refrains from uploading duplicate data to preserve upload bandwidth. This principle applies regardless of whether the duplicate data originates from the same end-user or different users.

In an authorized deduplication system, each end-user is granted a specific set of permissions during the system initialization phase. To facilitate authorized deduplication while considering varying privileges, each file is protected using a convergent encryption key and privilege keys

**3.Module for Private Cloud**

Diverging from the conventional deduplication architecture in cloud computing, a novel entity has been introduced to enhance user protection when utilizing cloud services.

In particular, due to constrained computational resources on the data user/owner's side and concerns regarding the practical trustworthiness of the public cloud, the private cloud serves as an intermediary, providing a dedicated execution environment and infrastructure that bridges the gap between the user and the public cloud.

Within this context, the private cloud assumes responsibility for managing the private keys associated with privileges and handling user file token requests. Through the private cloud interface, users can securely submit files and queries for storage and computation, respectively.

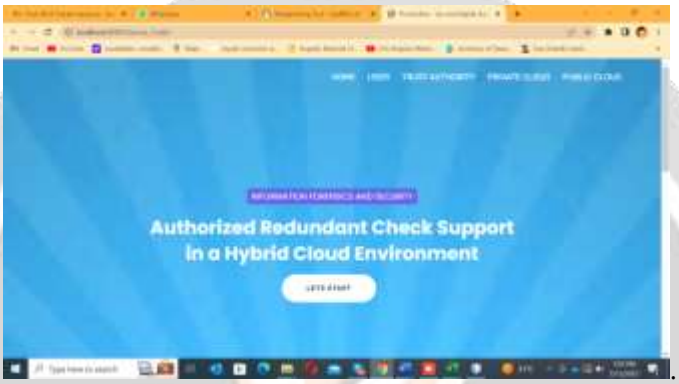
**4.System for Secure Deduplication**

We address various privacy aspects that require protection, encompassing: i) the integrity of duplicate-check tokens. Two types of adversaries are considered: external adversaries and internal adversaries.

As illustrated below, the external adversary can be regarded as an internal adversary without any privileges.

If a user holds privilege p, it is imperative that the adversary is unable to forge and generate a valid duplicate token with a different permission p′ for any file F where p does not match p′. Furthermore, unless the adversary requests a token using its own privilege from the private cloud server, it is prohibited from forging and generating a valid duplicate token with privilege p for any queried F

**RESULTS**




## CONCLUSION

Throughout the duplicate-checking process, it was postulated that the concept of authorized data deduplication could enhance data security by incorporating the diverse privileges held by different users. Furthermore, we showcased several innovative deduplication architectures that enable authenticated duplicate checks within a hybrid cloud framework. In these novel deduplication architectures, the private cloud server generates duplicate check tokens for files using unique private keys. Security analysis results indicate that our schemes exhibit resilience against the types of attacks outlined in the proposed security model. These attacks can originate from both internal and external sources.

**REFERENCES**

"OpenSSL Project. http://www.openssl.org/.

[2] P. Anderson and L. Zhang. Swift and secure backups for portable computers leveraging encrypted deduplication technology. Proceedings of the USENIX LISA Conference in the Year 2010.

[3] M. Bellare, S. Keelveedhi, and T. Ristenpart. "Dupless": A server-assisted encryption approach for deduplicated storage. Presented at the USENIX Security Symposium in 2013.

[4] M. Bellare, S. Keelveedhi, and T. Ristenpart. Efficient utilization of message-locked encryption and secure data deduplication. Pages 296-312 in the 2013 edition of EUROCRYPT.

This publication was authored by M. Bellare, C. Namprempre, and G. Neven, as referenced in footnote number 5. Security proofs for identity-based signers and signer identification approaches. Pages 1-61 appeared in Volume 22, Number 1 of the Journal of Cryptology in 2009.

J. Stanek, A. Sorniotti, L. Kencl, and E. Androulaki conducted this research. A reliable and secure deduplication technique specifically designed for cloud storage. As per the 2013 Technical Report, an issue was identified.