Authenticated Deduplication System with differential privilege user checks in cloud

Authenticated Deduplication System with differential privilege user checks in cloud

**ABSTRACT:**

Data deduplication is one of useful data compression scheme for eliminating redundancy in the storage, and has been very popular and cheap in cloud system to reduce the cloud size and save speed. For Security of sensitive data with supporting deduplication, the convergent encryption technique has been introduced to encrypt the data before uploading.

To better protect data security, proposed system address the problem of authorized data deduplication. Different from existing deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself. We also present new deduplication schemes supporting authorized duplicate check in public and private cloud architecture.

Although data deduplication brings a lot of benefits, security and privacy concerns arise as user’s sensitive data are susceptible to both inside and outside attacks.

Aiming at efficiently solving the problem of deduplication with differential privileges in cloud computing, we consider a hybrid cloud architecture consisting of a public cloud and a private cloud unlike existing systems.

In the proposed system if a file has been uploaded by a user with a duplicate hash value then file will be uploaded on cloud only if he have file and privilege.

**INTRODUCTION:**

One critical challenge of cloud storage services is the management of the ever-increasing volume of data. Data deduplication is a specialized data compression

technique for eliminating duplicate copies of repeating data in storage. The technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent..

Deduplication can take place at either the file level or the block level. For file-level deduplication, it eliminates duplicate copies of the same file. Deduplication can also take place at the block level, which eliminates duplicate blocks of data that

occur in non-identical files. Although data deduplication brings a lot of benefits,

security and privacy concerns arise as users’ sensitive data are susceptible to both insider and outsider attacks.

Convergent encryption has been proposed to enforce data confidentiality while making deduplication feasible. It en-crypts/decrypts a data copy with a convergent key, which is obtained by computing the cryptographic hash value of the content of the data copy. To prevent unauthorized access, a secure proof of ownership protocol is also needed to provide the proof that the user indeed owns the same file when a duplicate is found. After the proof, subsequent users with the same file will be provided a pointer from the server without needing to upload the same file.

A user can download the encrypted file with the pointer from the server, which can only be decrypted by the corresponding data owners with their convergent keys. Thus, convergent encryption allows the cloud to perform deduplication on the cipher texts and the proof of ownership prevents the unauthorized user to access

File.

**EXISTING SYSTEM**

Previous deduplication systems cannot support differential authorization duplicate check, which is important in many applications. There is only a single cloud in the existing system which makes very hard deduplication process. Existing deduplication system cannot prevent the privilege private key sharing among users.

**DISADVANTAGES OF EXISTING SYSTEM**

* Various loose points in the existing system.
* There is no concept of hybrid cloud.
* Data can be stolen due to various bucks and errors**.**

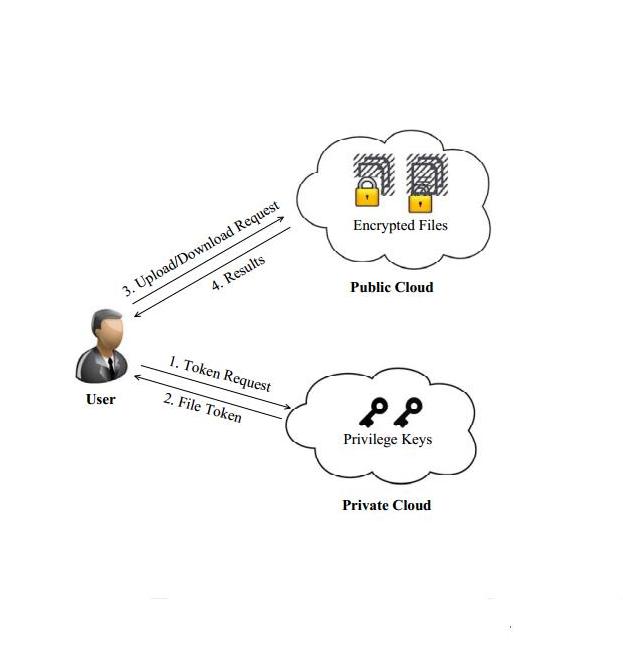
**PROPOSED SYSTEM**

Aiming at efficiently solving the problem of deduplication with differential privileges in cloud computing, we consider a hybrid cloud architecture consisting of a public cloud and a private cloud. Unlike existing data deduplication systems, the private cloud is involved as a proxy to allow data owner/users to securely per-form duplicate check with differential privileges. Such architecture is practical and has attracted much attention from researchers. The data owners only outsource their data storage by utilizing public cloud while the data operation is managed in private cloud.

A new deduplication system supporting differential duplicate check is proposed under this hybrid cloud architecture where the S-CSP resides in the public cloud. The user is only allowed to perform the duplicate check for files marked with the corresponding privileges.

Furthermore, we enhance our system in security. Specifically, we present an advanced scheme to support stronger security by encrypting the file with differential privilege keys. In this way, the users without corresponding privileges cannot perform the duplicate check. Furthermore, such unauthorized users cannot decrypt the cipher text even collude with the S-CSP. Security analysis demonstrates that our system is secure in terms of the definitions specified in the proposed security model

**SYSTEM ARCHITECTURE:**



**TECHNIQUE AND ALGORITHMS:**

* AES(Encryption and Decryption)
* MD5 for Hashing.

**ADVANTAGES OF PROPOSED SYSTEM**

* Reduces the load of a cloud server in a huge amount as duplicate files are not uploaded.
* Private cloud a new entity introduced for facilitating user’s se-cure usage of cloud service.
* The speed of the server is increases.

**HARDWARE & SOFTWARE REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

· **System** : Pentium IV 2.4 GHz.

**· Hard Disk**  : 250 GB.

· **Floppy Drive** : 1.44 Mb.

· **Monitor** : 15 VGA Color.

· **Mouse** : Logitech.

· **Ram**  : 1 GB

**SOFTWARE REQUIREMENTS:**

· **Operating system** : Windows XP Professional.

· **Coding Language** : Java (Jdk 1.6), JSP, Servlet.

· **Database** : My-SQL 5.0