**BASE PAPER TITLE:**

**A Hybrid Cloud Approach for Secure Authorized Deduplication**

**OUR PROPOSED TITLE:**

**An enhanced multi-layered cryptosystem based Secure and Authorized deduplication model in Cloud Storage system**

**BASE PAPER ABSTRACT:**

Data deduplication is one of important data compression techniques for eliminating duplicate copies of repeating data, and has been widely used in cloud storage to reduce the amount of storage space and save bandwidth. To protect the confidentiality of sensitive data while supporting deduplication, the convergent encryption technique has been proposed to encrypt the data before outsourcing. To better protect data security, this paper makes the first attempt to formally address the problem of authorized data deduplication. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself. We also present several new deduplication constructions supporting authorized duplicate check in a hybrid cloud architecture. Security analysis demonstrates that our scheme is secure in terms of the definitions specified in the proposed security model. As a proof of concept, we implement a prototype of our proposed authorized duplicate check scheme and conduct testbed experiments using our prototype. We show that our proposed authorized duplicate check scheme incurs minimal overhead compared to normal operations.

**OUR PROPOSED ABSTRACT:**

In this paper, we present a scheme that permits a more fine-grained trade-off. The intuition is that outsourced data may require different levels of protection, depending on how popular it is: content shared by many users, such as a popular song or video, arguably requires less protection than a personal document, the copy of a payslip or the draft of an unsubmitted scientific paper. As more corporate and private users outsource their data to cloud storage providers, recent data breach incidents make end-to-end encryption an increasingly prominent requirement. Unfortunately, semantically secure encryption schemes render various cost-effective storage optimization techniques, such as data deduplication, ineffective. We present a novel idea that differentiates data according to their popularity. Based on this idea, we design an encryption scheme that guarantees semantic security for unpopular data and provides weaker security and better storage and bandwidth benefits for popular data. This way, data deduplication can be effective for popular data, whilst semantically secure encryption protects unpopular content. We show that our scheme is secure under the Symmetric External Decisional Diffe-Hellman Assumption in the random oracle model.

**EXISTING SYSTEM:**

* Data deduplication systems, the private cloud is involved as a proxy to allow data owner/users to securely perform duplicate check with differential privileges.
* Such an 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.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Traditional encryption, while providing data confidentiality, is incompatible with data deduplication.
* Identical data copies of different users will lead to different ciphertexts, making deduplication impossible.

**PROPOSED SYSTEM:**

In this paper,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 ciphertext 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.

**ADVANTAGES OF PROPOSED SYSTEM:**

* The user is only allowed to perform the duplicate check for files marked with the corresponding privileges.
* We present an advanced scheme to support stronger security by encrypting the file with differential privilege keys.
* Reduce the storage size of the tags for integrity check. To enhance the security ofdeduplication and protect the data confidentiality,

**BASE PAPER ARCHITECTURE:**

****

**OUR PROPOSED ARCHITECTURE:**

****

****

Proposed multi-layered scheme

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Floppy Drive : 1.44 Mb.
* Monitor : 15 VGA Colour.
* Mouse : Logitech.
* Ram : 512 Mb.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/7.
* Coding Language : JAVA/J2EE
* IDE : Netbeans 7.4
* Database : MYSQL

**REFERENCE:**

Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou,“**A Hybrid Cloud Approach for Secure Authorized Deduplication**”,IEEE Transactions on Parallel and Distributed Systems.