Literature Survey

**#1 A Secure Data De duplication Scheme for Cloud Storage**

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 de duplication, 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 de duplication 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 Di e-Hellman Assumption in the random oracle model.

**Disadvantages**

1. Less security due to single cloud
2. There is no Reconstruction method to overcome the attacked data retrieval.

**#2. Fast and Secure Laptop Backups with Encrypted De-duplication**

Many people now store large quantities of personal and corporate data on laptops or home computers. These often have poor or intermittent connectivity, and are vulnerable to theft or hardware failure. Conventional backup solutions are not well suited to this environment, and backup regimes are frequently inadequate. This paper describes an algorithm which takes advantage of the data which is common between users to increase the speed of backups, and reduce the storage requirements. This algorithm supports client-end per-user encryption which is necessary for confidential personal data. It also supports a unique feature which allows immediate detection of common sub trees, avoiding the need to query the backup system for every file. We describe a prototype implementation of this algorithm for Apple OS X, and present an analysis of the potential effectiveness, using real data obtained from a set of typical users. Finally, we discuss the use of this prototype in conjunction with remote cloud storage, and present an analysis of the typical cost savings.

**Disadvantages**

1. We cannot deploy this system in IAAS based cloud
2. There is no common public key to share data .

**#3 A Secure Cloud Backup System with Assured Deletion and Version Control**

Cloud storage is an emerging service model that enables individuals and enterprises to outsource the storage of data backups to remote cloud providers at a low cost. However, cloud clients must enforce security guarantees of their outsourced data backups. We present Fade Version, a secure cloud backup system that serves as a security layer on top of today’s cloud storage services. Fade Version follows the standard version-controlled backup design, which eliminates the storage of redundant data across different versions of backups. On top of this, Fade Version applies cryptographic protection to data backups. Specifically, it enables fine-grained assured deletion, that is, cloud clients can assuredly delete particular backup versions or files on the cloud and make them permanently inaccessible to anyone, while other versions that share the common data of the deleted versions or files will remain unaffected. We implement a proof-of-concept prototype of Fade Version and conduct empirical evaluation atop Amazon S3. We show that Fade Version only adds minimal performance overhead over a traditional cloud backup service that does not support assured deletion.

**Disadvantages**

1. There is no de duplication technique to overcome the duplicate data
2. Only 64 bit key is using in the cloud storage for both public and secret key.

**#4 Security Proofs for Identity-Based Identification and Signature Schemes**

This paper provides either security proofs or attacks for a large number of identity-based identification and signature schemes defined either explicitly or implicitly in existing literature. Underlying these are a framework that on the one hand helps explain how these schemes are derived, and on the other hand enables modular security analyses, thereby helping to understand, simplify and unify previous work.

**Disadvantages**

1. Less security signature schemes
2. The identity based identification scheme is used for data deduplication.

**#5 Twin Clouds: An Architecture for Secure Cloud Computing**

Cloud computing promises a more cost effective enabling technology to outsource storage and computations. Existing approaches for secure outsourcing of data and arbitrary computations are either based on a single tamper-proof hardware, or based on recently proposed fully homomorphic encryption. The hardware based solutions are not scalable, and fully homomorphic encryption is currently only of theoretical interest and very inefficient. In this paper we propose architecture for secure outsourcing of data and arbitrary computations to an un trusted commodity cloud. In our approach, the user communicates with a trusted cloud (either a private cloud or built from multiple secure hardware modules) which encrypts and verifies the data stored and operations performed in the un trusted commodity cloud. We split the computations such that the trusted cloud is mostly used for security-critical operations in the less time-critical setup phase, whereas queries to the outsourced data are processed in parallel by the fast commodity cloud on encrypted data.

**Disadvantages**

1. Less security due to homomorphic encryption
2. There is un trusted cloud is used to store all the data where client side de duplication is not possible.