**A Secure Data Forwarding In Multiple**

**Server for Cloud Storage**

**Abstract** **–**

Cloud storage could be a service model during which information in maintained, managed and saved remotely and created out there to user over a network. Having your information keep offsite within the cloud makes it accessible from anyplace while not the effort of maintaining your own native storage and file-serving systems. It makes all the distinction in a very disaster, too. This cloud storage system, having assortment of storage servers these are providing future storage service over the net. Storing the information into third party’s cloud system causes concern over information confidentiality. During this cloud some general encoding schemes shield information confidentiality, but conjointly limit the practicality of the storage system as a result of a number of operations are supported over encrypted information. The most objective of this project is constructing a secure storage system that supports multiple functions is difficult once the storage system is distributed and has no central authority. During this project we tend to propose a threshold proxy re-encryption theme and integrate it that a decentralized erasure code specified a secure distributed storage system is developed. The distributed storage system not solely supports secure and sturdy information storage and retrieval, however conjointly lets a user forward his information within the storage servers to a different user without retrieving the information back. The most technical contribution is that the proxy re-encryption theme supports cryptography operations over encrypted messages furthermore as forwarding operations over encoded and encrypted messages. Our methodology totally integrates encrypting, encoding, and forwarding. We tend to analyze and recommend appropriate parameters for the amount of copies of a message dispatched to storage servers and also the range of storage servers queried by a key server. These parameters permit a lot of versatile adjustment between the amount of storage servers and hardiness. Erasure cryptography supports the forwarding theme and applicable in decentralized distributed system. A decentralized erasure code is employed to make sure the information hardiness within the distributed cloud storage system. In erasure codes, the copy of the message is keep within the every storage servers. If one in all the storage servers is failed, the message are often retrieved by one in all the extant server.

**Existing System**

General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. Storing data in a third party’s cloud system causes serious concern on data confidentiality. In the existing system, constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority.

**DISADVANTAGES OF EXISTING SYSTEM**

There are three problems in the above straightforward integration of encryption and encoding. First, the user has to do most computation and the communication traffic between the user and storage servers is high. Second, the user has to manage his cryptographic keys. If the user’s device of storing the keys is lost or compromised, the security is broken. Finally, besides data storing and retrieving, it is hard for storage servers to directly support other functions. For example, storage servers cannot directly forward a user’s messages to another one. The owner of messages has to retrieve, decode, decrypt and then forward them to another user.

**Proposed System**

In the proposed system, we propose a threshold proxy re-encryption scheme and integrate it with a decentralized erasure code such that a secure distributed storage system is formulated. By using the threshold proxy re-encryption scheme, we present a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back. The main technical contribution is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. Our method fully integrates encrypting, encoding, and forwarding. We propose a new threshold proxy re-encryption scheme and integrate it with a secure decentralized code to form a secure distributed storage system. The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages. The tight integration of encoding, encryption, and forwarding makes the storage system efficiently meet the requirements of data robustness, data confidentiality, and data forwarding. Accomplishing the integration with consideration of a distributed structure is challenging. Our system meets the requirements that storage servers independently perform encoding and re-encryption and key servers independently perform partial decryption. Moreover, we consider the system in a more general setting than previous works. This setting allows more flexible adjustment between the number of storage servers and robustness.

**Advantages:**

The threshold proxy re encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way. To decrypt a message of k blocks that are encrypted and encoded to n code word symbols, each key server only has to partially decrypt two code word symbols in our system. By using the threshold proxy re-encryption scheme, we present a secure cloud storage system that provides secure data storage and secure data forwarding functionality in a decentralized structure. Moreover, each storage server independently performs encoding and re-encryption and each key server independently perform partial decryption. Our storage system and some newly proposed content addressable file systems and storage system are highly compatible. Our storage servers act as storage nodes in a content addressable storage system for storing content addressable blocks.