Abstract

Cloud Storage System has a collection of storage servers provides long-standing storage services over the internet. Data privacy becomes a major concern in cloud storage system because user stores their data in third party cloud system. An encryption scheme available for data privacy but it limits the number of functions done in storage system. Building a secure storage system that supports multiple functions is tough when the storage system is distributed and has no central authority. A new idea is proposed proxy re-encryption scheme for decentralizes erasure code for defending the distributed system. The distributed storage system not only supports secure and robust data storage and recovery, but client onward his information in the storage servers to another user without retrieving the data back. The important technical part is that the proxy re-encryption scheme supports encoding operations over encrypted data as well as forwarding operations over encoded and encrypted data. Our schemes fully integrate encoding, encrypting, and onward.
- Giuseppe Ateniese, Kevin fu, Amherst Matthew Green, Susan Hohenberger, February 2006. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage. The Johns Hopkins University, University of Massachusetts, The Johns Hopkins University and Massachusetts Institute of Technology.


**Index Terms**

Computer Science  
Security

**Keywords**

Ciphertext  
Plaintext Key translation  
Proxy re-encryption