Abstract

Exponential increase in data inside endeavors is making a gush in the storage requirements and its security. Typical encrypting techniques of separable nature suffer against powerful adversaries due to the exponential improvement of computing power. Therefore, some cloud storage systems apply erasure coding in addition to encryption to prevent adversaries from revealing or/and controlling stored information. Nevertheless, still a powerful adversary can extract useful information from a compromised server. In this paper, a new storage scheme is introduced implying an All-Or-Nothing (AON) encryption mode to separately randomize the encrypted blocks and hashing the resulted pseudorandom blocks altogether afterwards, and with the aid of the salting technique, called Replicated BYTE, integrity is ensured. The scheme will be called Randomized AON plus Replicated BYTE (RAON-RB). By employing systematic Reed Solomon erasure coding, the proposed scheme will be more applicable to distributed systems. The proposed scheme is secure even if all but one storage servers have been compromised and even if the encryption key is disclosed. Moreover, to resist share modification and localize faulty server(s), the proposed scheme verifies the received shares before they are
involved in the reconstruction process, and hence, the scheme can save superfluous computations as well.

References


**Index Terms**

Computer Science | Security

**Keywords**

Cloud computing, distributed storage, AON encryption, non-separable block cipher, Reed Solomon erasure code, hashing.