Cryptology ePrint Archive: Report 2011/538

Secure Cloud Storage with Encrypted Data using File-Based Authentication

Jia Xu and Ee-Chien Chang and Jianying Zhou

Abstract: Cloud storage service is gaining popularity in recent years. Client-side deduplication is widely adopted by cloud storage services like Dropbox and MozyHome, to save bandwidth and storage. Security flaws, which may lead to private data leakage, in the current client-side deduplication mechanism are found recently by Harnik, Pinkas, and Shulman-Peleg (S\&P Magazine, '10).

This paper presents a notion of \emph{File Based Authentication}, that is, a user authenticates himself/herself using the file he/she possesses as the secret information. File Based Authentication can be applied to protect confidentiality of users' sensitive data file in the cloud storage from both the third party attackers and the semi-honest cloud server itself. The proposed solution enables efficient client-side deduplication (across users) and client-side sharing of encrypted data in the cloud storage, where the encryption key is chosen by a user \emph{independently} \ \ (without negotiation with other owners of the same data file)\ \ and is kept secret from the cloud storage server and its client software.

Furthermore, the surprising part is that, a secure cloud storage system without pre-registration for users can be constructed based on the proposed solution: All owners of a file F share an a priori account with hash value $h(F)$ as identity and sensitive file F as password, without knowledge of each other and without registration on the cloud storage server, since the first uploading of F (in encrypted form) to the cloud will function as the registration of account $(h(F), F)$ in the cloud storage server.

Category / Keywords: applications / Privacy, Client-side deduplication, Proofs of Ownership, Client-side Sharing, File-based Authentication, Registration-free Cloud Service

Date: received 1 Oct 2011, last revised 18 Nov 2011

Contact author: jiaxu2001 at gmail com

Note: This paper attempts to address the same problem as "Proofs of Ownership in Remote Storage Systems (To appear in CCS '11)", in a different setting where all data files in the cloud are encrypted using user-chosen keys which are secret from the cloud server.