Abstract

Cloud storage auditing is viewed as an imperative service to corroborate the veracity of the data in public cloud. Existing auditing protocols are all based on the supposition that the client’s secret key for auditing is completely protected. Such assumption may not always be held, due to the probably weak sense of security and/or low security settings at the client. In most of the current auditing protocols would inevitably become unable to work when a secret key for auditing is exposed. It is investigated on how to reduce the damage of the client’s key revelation in cloud storage auditing, and provide the first handy elucidation for this new problem setting. Formalized the definition and the security model of auditing protocol with key-exposure resilience and propose such a protocol. Utilized and developed a novel authenticator construction to support the forward security and the property of block less verifiability using the current design. The security proof and the performance analysis show that the projected protocol is protected and well-organized.

Index Terms

Computer Science

Distributed Computing
Keywords

Data storage, cloud storage auditing, cloud computation, key exposure resistance