Identity-based Remote Data Integrity Checking with Perfect Data Privacy Preserving for Cloud Storage

Objective:

Main objective of the system is to building data integrity over distributed cloud computing environment and enhancing the system in accordance with user privacy.

Abstract:

Remote data integrity checking (RDIC) enables a data storage server, say a cloud server, to prove to a verifier that it is actually storing a data owner's data honestly. To date, a number of RDIC protocols have been proposed in the literature, but most of the constructions suffer from the issue of a complex key management, that is, they rely on the expensive public key infrastructure (PKI), which might hinder the deployment of RDIC in practice. In this paper, we propose a new construction of identity-based (ID-based) RDIC protocol by making use of key-homomorphic cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication framework in PKI based RDIC schemes. We formalize ID-based RDIC and its security model including security against a malicious cloud server and zero knowledge privacy against a third party verifier. The proposed ID-based RDIC protocol leaks no information of the stored data to the verifier during the RDIC process. The new construction is proven secure against the malicious server in the generic group model and achieves zero knowledge privacy against a verifier.

Introduction:

Here ,we investigated a new primitive called identity-based remote data integrity checking for secure cloud storage. We formalized the security model of two important properties of this primitive, namely, soundness and perfect data privacy. Both the numerical analysis and the implementation demonstrated that the proposed protocol is efficient and practical.

We consider three security properties namely completeness, security against a malicious server (soundness), and privacy against the TPA (perfect data privacy) in identity-based remote data integrity checking protocols. Following the security notions due to Shacham and Waters, an identity-based RDIC scheme is called secure against a server if there exists no polynomial-time algorithm that can cheat the TPA with non-negligible probability and there exists a polynomial-time extractor that can recover the file by running the challenges response protocols multiple times. Completeness states that when interacting with a valid cloud server, the algorithm of ProofCheck will accept the proof.