Abstract

Storage-as-a-Service (SaaS) offered by cloud service providers is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and mitigates the burden of large local data storage at the organization's end. However, the fact that data owners no longer physically possess their sensitive data raises new challenges to the tasks of data confidentiality and integrity in cloud computing systems. Many researchers have focused on the problem of provable data possession (PDP), and proposed different schemes to audit data on remote storage sites.

In this paper, we investigate the concept of PDP and provide an extensive survey for different PDP schemes on a single cloud server. Moreover, the paper discusses the design principles for various PDP constructions, highlights some limitations, and present a comparative analysis for numerous PDP models. We classify PDP schemes into protocols for static data, and models that support outsourcing of dynamic data.
References

6. B. Krebs, “Payment processor breach may be largest ever.”
7. 82x 362, 2006.
12. 82x 107, D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” in ASIACRYPT ’01: Proceedings of the 7th International Conference on the Theory and


Index Terms

Computer Science

Distributed Systems
Keywords

Cloud computing, Outsourcing Data Storage, Cryptographic Protocols, Data Integrity, Verification Techniques