Optimizing the Algorithm for Secure and Dynamic Cloud Storage using MHT

Abstract

With the consistently increasing demand of storing data backup online by millions of users, cloud computing - which provides resources both hardware and software as a service through a network (usually internet) has gained much momentum and attention. Storing data on cloud services relieves the user from the task of storing data locally. As beneficial as it sounds, cloud storage comes along with the quintessential need to protect the stored data from threats such as loss of confidential data and denial of service. The purpose of this research paper is provide a mechanism which uses tokens and distributed forward error correction coded data. The mechanism not only provides the assurance of a secure storage but also provides with the identification of error or the wrongful server simultaneously. Considering the user to store data dynamically, we have also felicitated the dynamic operations such as insertion, deletion and appending blocks. In comparison to previous works, our algorithm can be more flexible with the use of Merkle Hash Tree (MHT) rather than contiguous block data structure.

References

- Kevin D. Bowers, Ari Juels, and Alina Oprea, Proofs of retrievability: theory and


Index Terms

Computer Science
Distributed System

Keywords

Cloud storage  security of data  dynamic data  data integrity.