Abstract

Storage-as-a-Service offered by cloud service providers (CSPs) enables customers to store and retrieve almost unlimited amount of data by paying fees metered in GB/month. For an increased level of scalability, availability and durability, some customers may want their data to be replicated on multiple servers across multiple data centers. In this paper, we propose a pairing-based provable multicopy data possession (PB-PMDP) scheme, which provides an evidence that all outsourced copies are actually stored and remain intact. Moreover, it allows authorized users (i.e., those who have the right to access the owner’s file) to seamlessly access the file copies stored by the CSP, and supports public verifiability. The proposed scheme is proved to be secure against colluding servers. We illustrate the performance of the PB-PMDP scheme through theoretical analysis, which is then validated by experimental results on a commercial cloud platform. The verification time of the proposed scheme is practically independent of the number of file copies. Additionally, we discuss how to identify corrupted copies by slightly modifying the proposed PB-PMDP scheme.

- Amazon elastic compute cloud (Amazon EC2). http://aws.amazon.com/ec2/.
- Amazon simple storage service (Amazon S3). http://aws.amazon.com/s3/.

Index Terms

Computer Science
Distributed Systems

Keywords
Cloud computing outsourcing data storage data replication cryptographic data protocols integrity verification techniques.