Cryptology ePrint Archive: Report 2011/447

On Verifying Dynamic Multiple Data Copies over Cloud Servers

Ayad F. Barsoum and M. Anwar Hasan

Abstract: Currently, many individuals and organizations outsource their data to remote cloud service providers (CSPs) seeking to reduce the maintenance cost and the burden of large local data storage. The CSP offers paid storage space on its infrastructure to store customers' data. Replicating data on multiple servers across multiple data centers achieves a higher level of scalability, availability, and durability. The more copies the CSP is asked to store, the more fees the customers are charged. Therefore, customers need to be strongly convinced that the CSP is storing all data copies that are agreed upon in the service contract, and the data-update requests issued by the customers have been correctly executed on all remotely stored copies.

In this paper we propose two dynamic multi-copy provable data possession schemes that achieve two main goals: i) they prevent the CSP from cheating and using less storage by maintaining fewer copies, and ii) they support dynamic behavior of data copies over cloud servers via operations such as block modification, insertion, deletion, and append. We prove the security of the proposed schemes against colluding servers. Through theoretical analysis and experimental results, we demonstrate the performance of these schemes. Additionally, we discuss how to identify corrupted copies by slightly modifying the proposed schemes.

Category / Keywords: cryptographic protocols / Cloud computing, outsourcing data storage, dynamic data integrity, cryptographic protocols

Date: received 15 Aug 2011

Contact author: afekry at engmail uwaterloo ca