Abstract

Cloud computing has rapid growth globally cause of the facet provided by the service not only scalability but also capacity management that subject to storage huge amount of data. Major issue will going to arrived at the time of storing this much bulky data on a cloud because data integrity may lost at the time of data retrieval. First, Anyone canister to challenge in the intention to verification of data integrity of certain file so that appropriate authentication process will going to miss between cloud service provider and third party auditor (TPA). Second, as the BLS signature obligated for fully dynamic updates of data over data blocks of fixed sized which causes re-computation and updating for an entire block of authenticator which origin not only higher storage but also communication overheads. In order to keep security as a vital issue because malicious party may scarf data at the time of data flows this can be addressed by means of symmetric key encryption. Similarly, in order to increase the speed and efficiency at the time of data retrieval for huge amount of data MapReduce plays vital role and the because of replication over the HDFS maintain data integrity with the full support of dynamic updates.
References


19. Y. He, S. Barman, and J.F. Naughton, “Preventing Equivalence Attacks in Updated, Anonymized Data,” in Proc. 27th IEEE Int’l Conf. on Data Engineering (ICDE), 2011, pp. 529-540.

Index Terms

Computer Science Databases

Keywords

Cloud computing, authorized auditing, big data, Hadoop, provable data possession, fine-grained updates