The popularity and widespread use of Cloud have brought great convenience for data sharing and data storage. The data sharing with a large number of participants take into account issuers like data integrity, efficiency and privacy of the owner for data. In cloud storage services one critical challenge is to manage ever-increasing volume of data storage in cloud. To make data management more scalable in cloud computing field, deduplication a well-known technique of data compression to eliminating duplicate copies of repeating data in storage over a cloud. Even if data deduplication brings a lot of benefits in security and privacy concerns arise as user's sensitive data are susceptible to both attacks insider and outsider. A convergent encryption method enforces data confidentiality while making deduplication feasible. Traditional deduplication systems based on convergent encryption even though provide confidentiality but do not support the duplicate check on basis of differential privileges. This paper presents, the idea of authorized data deduplication proposed to protect data security by including differential privileges of users in the duplicate check. Deduplication systems, users with differential privileges are further considered in duplicate check besides the data itself. To support stronger security the files are encrypted with differential privilege keys. Users are only allowed to perform the duplicate check for files marked with the corresponding privileges to access. The user can verify his/her presence of file after deduplication in cloud with the help of a third party.
A Secured and Authorized Data Deduplication in Hybrid Cloud with Public Auditing

 auditor by auditing the data. Further auditor audits and verifies the uploaded file on time. Therefore, this paper creates benefits to both the storage provider and user by deduplication technique and auditing technique respectively.

References


Index Terms

Computer Science

Distributed Systems
Keywords
Authorized check duplicates confidentially auditing.