Abstract

The internet framework and thousands of users are dealing with cloud for sensitive information over cloud computing nowadays providing exciting features due to the services. In terms of security and the access control mechanisms, cloud server management is a challenging task due to sensitivity of data deployed in clouds.

For the Key Distribution and also data administration when a course of fine-grained access control on data is demanded by the users and the scaling factor must be well enough the cloud server suffers from the processing overhead. To maintain scalability, data confidentiality as well as fine graininess of access control mechanisms at the same time on the risk of uncertainty is the main issue. As based on quality of data the system provides and generates access policies and then afterward gives servers by maintaining the security and encryption of data the permission of data owner and modifier to unauthorized cloud servers by maintaining the security and encryption of data. By taking a combination of decentralized key policy and attribute-based Encryption (KP-ABE) this thing can be overcome. The proposed system will be robust and
secure. The technique referred is known as Deduplication of data (removal of repeated copies), also removal of copies of continuously repeating data is necessary, one of the most important data compression technique widely used in cloud storage to recover the space and bandwidth of cloud. A big support is provided by using convergent encryption technique to the protection of the confidentiality of sensitive data by performing authorized duplicate check in hybrid cloud storage architectures.

References


Index Terms

Computer Science Security
Keywords

Cloud Storage, Access control, Key Distribution Centre, Data Deduplication, KP-ABE.