Abstract

Continuous changes in the membership of data sharing giving security and privacy preservation are still challenging issues, especially for an untruth cloud due to the collusion attack. It is based on the secure key distribution without assuming any secure communication channel. We propose a secure re-encryption scheme of data sharing scheme without assuming secure communication channel for dynamic groups in the cloud. The system provides fine-grained access control for any clients who wants to access the information from cloud. It also prevents access of clients after their revocation and protect from collusion attack. Proposed system provide guarantee for secure sharing of data files when they are outsourced with double encryption and particular security key distribution mechanism. Re-encryption of message provides the data security and prevents other security attacks like man in middle attack. If an attacker tries to decrypt the massage using untruth cloud, it will not possible for them. Users can achieve an effective and economical way for data sharing among group members in the cloud with efficient manner and little management cost.
References


Index Terms

Computer Science  Security
Keywords