Re-Encryption Scheme of Secure Data Sharing for Dynamic Groups in the Cloud

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 170
Number 7

Year of Publication: 2017

Authors:
Ajit N. Pawar, Sonal Fatangare

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 want to access the information from the cloud. It also prevents access of clients after their revocation and protects from collusion attack. Proposed system provides guarantee for secure sharing of data files when they are outsourced with double encryption and particular security key distribution mechanism. Re-encryption of messages provides the data security and prevents other security attacks like man in the middle attack. If an attacker tries to decrypt the message using an 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