Abstract

In world of Internet, the concept of group data sharing is gaining very high popularity. The privacy and security of group data sharing are the main issues which are to be considered while using this concept. Due to the semi-trust nature of the third party, it cannot be trusted and hence, security models used traditionally cannot be directly applied to the framework of cloud based group sharing. In this paper, implemented framework for a secure group sharing for public cloud, which can take the advantages of Cloud Server’s help very effectively. Only difference is that the chances of data insecurity would be reduced and the threat of data being exposed to attackers and cloud provider would be reduced simultaneously. Framework is formed by combining Proxy signature, enhanced TGDH and proxy re-encryption together into protocol. The use of proxy signature technique is that the group leader can grant the privilege of group management to one or more chosen group members. With the help of cloud servers, the enhanced TGDH scheme enables the group to update and negotiate group key pairs thus all group members need not to be online all the time. By using proxy re-encryption most of
intensive operations which are to be performed computationally can be handed over to the cloud servers without the threat of disclosure of any private information. The security requirements for public cloud based secure group sharing are fulfilled by our proposed scheme with high efficiency and it can be proved by the extensive security and performance analysis.

References


Index Terms

Computer Science Distributed Systems

Keywords

TGDH (Tree-based Group Diffie-Hellman), PRL (Privileged revocation List), GL (Groupleader), GM (Groupmembers), GA (Groupadmin), PUDs (Personal Domains), PHR (Personal health records).