Abstract

Cloud computing is recently developed new emerging technology for complex systems with massive-scale services sharing among numerous users, where user can rent the storage and computing resources of server provided by a company. Users only require a terminal, a smartphone or tablet connected to the internet. Cloud can store huge amount of data, so the mobile users do not have to carry their data. Therefore, security of data, privacy of user and authentication of both users and services is a significant issue for the trust and security of cloud computing. In order to achieve safe storage, we proposed a secure cloud storage scheme providing access to the data using RSA public-key encryption algorithm and digital signature scheme. In this scheme, the cloud verifies the authenticity of the series without knowing the user’s identity before storing data. Access control feature is also added by which only a valid users are able to decrypt the stored information. This scheme also prevents replay attack and supports creation, modification, and reading data stored in cloud. Time based user Revocation scheme is also used. Also we compared performance of our system with the 3DES system on the basis of encryption and decryption of data.
References

18. S. Jahid, P. Mittal, and N. Borisov, “EASiER: Encryption-Based Access Control in Social
Secure Data Storage in Cloud by Decentralized Access Control


Index Terms

Computer Science    Circuits and Systems

Keywords

Cloud computing, Access control, User revocation.