Abstract

This paper presents a survey on Proxy re-encryption techniques with respect to secure cloud data and its application. To keep sensitive user data confidential against untrusted servers, cryptographic methods are used to provide security and access control in clouds. As the data is shared over the network, it is needed to be encrypted. There are many encryption schemes that provide security and access control over the network. Proxy re-encryption enables the semi-trusted proxy server to re-encrypt the ciphertext encrypted under Alice’s public key to another ciphertext encrypted under Bob’s public key. The re-encryption is done without the server being able to decrypt the ciphertext. Cloud services and applications should follow the standard security measures including data confidentiality, integrity, privacy, robustness and access control. In this paper the proxy re-encryption (PRE) schemes, Conditional PRE, Identity based PRE and Broadcast PRE, Type based PRE, Key private PRE, Attribute based PRE, Threshold PRE and its role in securing the cloud data are explained.

References


18. Lidong Zhou, Michael A. Marsh, Fred B. Schneider, and Anna Redz, Distributed blinding
for ElGamal reencryption, Cornell Computer Science Department, 2004.


22. Emura, K., Miyaji, A., Omote, A timed-release proxy re-encryption scheme IEICE Transactions, 98-A(8), 1682-1695 (2011)

Index Terms

Computer Science Distributed Systems

Keywords

Proxy re-encryption, cloud storage, data confidentiality