Abstract

In order to assure confidentiality of sensitive information stored in public clouds, a commonly embrace approach is to encrypt the information before uploading it to the cloud. Since the cloud does not know the keys used to encrypt the information, the confidentiality of the information from the cloud is assured. However, as many organizations are required to enforce fine-grained access control to the information, the encipher mechanism should also be able to provide fine-grained encryption-based access control. Proposed work solves the key escrow
problem and revocation problem of the previous systems and performs only a single encryption of each data item and minimize the overhead at the data owner.

References

- Seung-Hyun Seo, Mohamed Nabeel "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds" IEEE transactions on knowledge and data
 Novel Approach for improving Security and Confidentiality in Public Clouds using Certificateless Encryption


Index Terms

Computer Science
Security

Keywords
Cloud Computing  Public Key Cryptography  Certificate Less  Data Sharing