Abstract

Cloud security is the most critical task while considering its working environment, i.e. outsourced, distributed and utility based. In such cases making the users data confidential, increases the trust over the system. Also the security procedure does not make the availability affected in any ways. The users of these kind of systems is always retained the services and securities preliminaries with respect to the data itself. As the cloud user can access its data frequently and if here some encryption is used which requires decryption and the repetitive process continues to increase the overheads. It requires some mechanism in which encryption is performed and if the user requires to perform some operations on secure file without decrypting it can be fulfilled. Thus homomorphic encryption lets the user facilitates about the performing operations on encrypted data which reduces the complexity of confidentiality operations. Also to prevent Cloud Servers from being able to learn both the data file contents and user access privilege information used to generate key along with the fastest access of secured data by using Attribute-based encryption (ABE).
References

2. Srijith “Towards Secure Cloud Bursting, Brokerage and Aggregation” 2010 Eighth IEEE European conference on web services
3. Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE “Privacy-Preserving Public Auditing for Secure Cloud Storage, IEEE-2012
20. GALS System Design: Side Channel Attack Secure Cryptographic Accelerators

Index Terms

Computer Science Security

Keywords

Attribute Based Encryption, Cloud Storage, Data Storage, Holomorphic.