Abstract

In cloud computing there is problem associated with whole life of cloud data. For storage three important aspects of data is Data confidentiality, Data integrity and availability. Data encryption is used for confidentiality. Now, after this encryption data is sent to storage. Now, after the user supplies its key than the data is opened. Thus to provide user based security control for cloud provider is the primary objective of this effort and can be achieved by Homomorphic encryption. Key management is another problem because the user is not expert to manage keys. The user has faced such problems. To develop a security architecture and implement client based confidentiality tool for storage in cloud computing and evaluate traditional security solutions and identify their remaining issues by which overall performance gets degraded. We will implement homomorphic encryption using improved KP-ABE system to achieve data confidentiality.

References

1. Shucheng Yu , “Achieving Secure, Scalable, and Fine-grained Data Access Control in
Hybrid Approach for Cloud Storage with Attribute based Encryption

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

Index Terms

Computer Science

Distributed Systems
Keywords

Cloud, Cloud Security, Data privacy, ABE, KP-ABE, Cloud Storage