Abstract
Cloud computing has many strong economic advantages, but clients are reluctant to trust a third-party cloud provider. To confront these security concerns, data can be transmitted and stored in encrypted form. There are challenges regarding the conditions of the generation, distribution, and usage of encryption keys in cloud systems, such as the safe place of keys. These idiosyncrasies lead to difficulties in achieving effective and scalable key management. In this work, a model for key management based on the principle of dynamic data re-encryption is practiced to a cloud computing system in a unique way to address the demands of a cloud environment. The proposed model is highly scalable, secure and efficient in a cloud computing reference, as keys are handled by the client for trust reasons, resource-intensive data re-encryption is handled by the cloud provider, and key distribution is minimized to conserve communication costs on. Attribute-based encryption is proposed to allow users access to cloud based on the satisfaction of required characteristics such that the higher computation load from cryptographic operations is assigned to the cloud provider. A versioning history mechanism effectively manages keys for a constantly changing user population and cross checks the session-ID of user. Furthermore a data de-duplication mechanism is added in order to allow efficient storage in cloud scenarios. Finally, an implementation on commercial cloud platform is used to validate the performance of the model.

References

- Prof. RakeshMohanty, Niharjyoti Sarangi, Sukant Kumar Bishi, “A Secured Cryptographic Hashing Algorithm,” VSSUT, Burla, Orissa, India
- G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy

Index Terms

Computer Science
Distributed Systems

Keywords

Re-encryption  Attribute-based Encryption  Cloud Security  Cloud Computing