Abstract

Technological advancements in cloud computing due to increased connectivity and exponentially proliferating data has resulted in migration towards cloud architecture that employ dynamic load and access balancing. Cloud computing is technology where the clients' can use high end services in form of software that reside on different servers and access data from all over the world. With a promising technology like this, it certainly abandons clients' privacy, management of data and services, putting new security threats towards the assurance of data in cloud. However, there are some security concerns when clients handle and share data in the cloud-computing environment. The security threats such as maintenance of data integrity, data hiding and data safety dominate clients concerns when the issues of cloud security come up. The big data and time-consuming encryption calculations related to applying any encryption method have proved as a hindrance in this field.

Cryptography is knowledge of protecting the information for providing encryption techniques. In this paper, Cloud computing security framework was tested. The framework ensures a trusted cloud environment that controlled by both the client and the cloud environment. The proposed solution secures the movement of data between client and cloud end. the non-breakability of
ElGamal based on Elliptic curve cryptography for data encryption/decryption was used along with Diffie Hellman based on elliptic curve mechanism for connection establishment. The data integrity verification is done by introducing a message digest tag for updating data based on SHA-256. The proposed encryption mechanism uses the combination of elliptical cryptography and SHA-256 methods.

References

- Xiao-Yong Li1, Li-Tao Zhou2,Yong Shi1, Yu Guo, "A trusted computing environment model in cloud architecture", Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, Qingdao, 11-14 July 2010
- Ms. Ritu Patidar, 2 Mrs. Rupali Bhartiya, "Implementation of Modified RSA Cryptosystem Based on Offline Storage and Prime Number", IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
Cloud Computing Security Framework based on Elliptical Curve


Index Terms

Computer Science Distributed Systems

Keywords

cloud computing Elliptic curve Diffie Hellman based on Elliptic curve cloud storage Security cryptography

ElGamal
hash256
ECDSA
DSA.