Abstract

The problem of secure data transmission on cloud environments is addressed in the proposed security model. The data security is quite important on cloud environments because they belong to the users. The security layer is defined or implemented between the cloud user and server end to ensure the security of data being exchanged between them. In this research, a key exchange scheme has been proposed to ensure the security of cloud platforms. The proposed model under this research project presents improved random key management architecture, which may be called efficient multi-level complex key sharing and authorizing model (EMCKS) for the cloud platforms. In particular, the proposed model allows only authorized applications and/or users to use the keys. Using simple devices, administrators can remotely issue authenticated commands to EMCKS and verify system output. In this research, we will develop the proposed scheme named EMCKS for corporate key management technique adaptable for the clouds by making it efficient and quicker. In addition, it also has to be improved to work with Cloud server and client nodes, which enforces the proposed scheme to create a secure environment based cloud platforms. The proposed scheme has been noticed providing hardened security than the other key management architectures as it is based on non-predictive key generation mechanism. The results have shown the effectiveness of the proposed model in terms of elapsed time.
A Novel Cryptographic Key Distribution Scheme for Cloud Platforms

References

- Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma, "Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)", July 2012, Kuala Lumpur, Malaysia.

**Index Terms**

Computer Science  
Distributed Systems

**Keywords**

Cloud security authentication key management secure access channel security