Abstract

Cloud computing is one of the emerging and promising field in Information Technology. It provides services to an organization over a network with the ability to scale up or down their service requirements. Cloud computing services are established and provided by a third party, who having the infrastructure. Cloud computing having number of benefits but the most organizations are worried for accepting it due to security issues and challenges having with cloud. Security requirements required at the enterprise level forces to design models that solves the organizational and distributed aspects of information usage. Such models need to present the security policies intended to protect information against unauthorized access and
modification stored in a cloud. The proposed work describes the approach for modeling the security requirements from the perspective of job functions and tasks performed in an organization by applying the cryptography concepts to store data on cloud with the smallest amount of time and cost for encryption and decryption processes. In this work, we used RSA and AES algorithm for encryption and decryption of data and role based access control model is used to provide access according to the role played by user. This paper also shows the mathematical model for calculating the trust of the user. This model gives the uploading rights to the user when he/she recommended by the Administrator and Owner when users exceeds the specified experience and trust threshold value.

References

- R. Sandhu. The next generation of access control models: Do we need them and what should they be? In SACMAT'01, May 2001, page 53
- Prof. S. A. Ubale, Dr. S. S. Apte, Comparison of ACL Based Security Models for securing resources for Windows operating system,IJSHRE Volume 2 Issue 6, Page No 63.

Index Terms

Computer Science  Security

Keywords

Role Based Access Control  AES  RSA  Cloud computing  Trust Management.