Abstract

The storage and retrieval of data over cloud computing is a big issue. For the storage and retrieval of data, cloud computing uses the concept of authentication and authorization. The process of authentication and authorization uses primary and secondary authentication systems. In the primary authentication system, login ID and password are used, in secondary login, the OTP and some other verification code is used. In both login systems, the OTP code and primary information of the user are trapped, and the security process of the cloud environment is compromised. In this paper, a model of secured access based on the concept of fake and genuine users is proposed. In the case of a fake user, the received file is fake. This file is generated by the system. For the authentication of genuine and fake users, the concept of a shared key is used. The shared key gives the option of retrieval of data over the cloud environment. The proposed model is implemented in Java software and uses Java RMI tool for access of remote machine.

References

**Index Terms**

Computer Science  
Information Sciences
Keywords

Authentication, cryptography, Sharing of Key.