Abstract

One-time password is currently used as one of the user authentication mechanisms. To avoid the username and password vulnerability, the two-way authentication mechanism has come into being, to provide security to the user at the login time. Many online service providers are using the two-way authentication mechanism as a key to identify whether the login user or service request person is a right one or not. To add more security to the user session, the Session Identification (SID) has been used. The user authentication and the user authorization are important for online transactions and web-related transaction services. Existing OTP methods are widely used by many service providers as it is, or with a little modification. This paper proposes Request-based One-Time Password (ROTP) as a new type of OTP mechanism and in the SID, the ROTP value is used as Active Session Identification (ASID) value. Inside Data Ownership Country Access (IDOCA) and Outside Data Ownership Country Access (ODOCA) data access permission rights are assigned to authorize the users. The proposed method satisfies the evaluation parameter and gives the satisfied result in the testing level environment.
A Framework for User Authentication and Authorization using Request based One Time Passkey and User Active Session Identification

References


**Index Terms**

Computer Science Security

**Keywords**

Session Identification, One-Time Password, User Authentication, Web Services, Cloud Security.