Abstract

The proposed system supports single sign-on in an inter-cloud environment where users can manage in different cloud environments and provide a single set of credentials to access different Saas cloud applications provided by different cloud service providers without re-authentication. Single sign-on defines the ability to authenticate only once in a distributed network and to access several protected services and resources without re-authentication. To achieve this feature, the system supports federated identity management systems. The federated identity management system crosses organizational boundaries. To manage identities of users in this case, a cooperative contract needs to be set up between multiple identity providers, using a centralized approach. The proposed system uses a third-party auditor or a third cloud to synchronize the identities of users among different clouds. As user data are transferred or exchanged between different cloud environments, the chance of stealing data is increased. To avoid this, the system is secure from some attacks like identity theft, denial of service, etc., and also maintains a secure channel to transfer/exchange information between different clouds.
References

2. “Secure Inter-cloud SSO (SSO) using IIDs” by Bernd wattendorfer, Arne Tauber E-Government Innovation Center (EGIZ) Graz University of Technology Graz, Austria.

Index Terms
Computer Science Security

Keywords
SSO, Authorization, Authentication, Re-authentication, Cloud environment, IID, Electronic
identification, Federated identity management, Identity federation.