Abstract

The growing popularity of cloud based services is prompting organizations to consider shifting applications and data onto cloud. However, organizations dealing with highly sensitive information are apprehensive of moving its applications & data to public cloud owing to concern about security of its information. It is hence incumbent on service providers that only legitimate Users will access its services and resources in cloud.

Verifying authenticity of remote users is a necessary pre-requisite in a cloud environment before allowing access to secure resources/services/applications. The simplest & most commonly used user authentication mechanism is password based authentication. However, Users tend to choose easy to remember password, and many a times use same password for multiple accounts, which makes it often the weakest link in security. Furthermore, service providers authenticating Users on the basis of password, stores password verification information in their databases and such authentication schemes with verification table are known to be vulnerable to various attacks.

From the perspective of authentication requirements, service providers in a cloud environment can be broadly categorized into two. Those service providers dealing with highly sensitive information and working in a regulated environment can be grouped into category one – as in those offering services for sectors like health care, finance. These providers require a strong and secure authentication mechanism to authenticate its users, without any additional functionality. Similarly, there is a second category of service providers dealing with secure information but operate in a collaborative environment – as providers providing their applications bundled through a web portal. To provide the Users with a
seamless authentication experience, while accessing multiple services during a session, the second category of service providers prefer to have Single Sign-on functionality.

Two-factor authentication technology overcomes the limitations of password authentication and decreases the probability that the claimant is presenting false evidence of its identity to verifier. If different service providers set up their own two-factor authentication services, Users have to do registration and login process repeatedly. Also, Users accessing multiple cloud services may be required to hold multiple authentication tokens associated with various service providers.

Authentication factors such as crypto-tokens and smart cards with cryptographic capabilities have been vastly used as a second authentication factor. However, Users are required to always carry these authentication tokens which make it cumbersome from practical usability perspective. Also its usage involves cost thus restricting its adoption to corporate environments. The authentication process can be made more user-convenient if the authentication factor chosen is such that it is commonly used by all types of Users. Leveraging the use of mobile phone as an authentication factor can help address issue of user convenience at no extra cost while improving the security of authentication schemes.

Though, there has been an increasing focus on strengthening the authentication methods of cloud service users, there is no significant work that discusses an authentication scheme that can be adopted by the two categories of cloud Service Providers.

Taking cognizance of aforesaid issues related to secured authentication in cloud environment, this research focused on designing secure Two-Factor authentication schemes that can be adopted by the two categories of service providers. This
research carried out in different levels, proposes authentication architecture and protocols for the two categories of service providers.

At the first level, research proposes Direct Authentication architecture for cloud Service Providers who prefer to authenticate its users by using a strong authentication mechanism and does not require Single Sign-On (SSO) functionality. For those Providers who prefer to provide its user with a SSO functionality the research proposes Brokered Authentication architecture.

The next level of research focuses on proposing User Authentication Protocols for both Direct Authentication Service Providers (DASPs) and Brokered Authentication Service Providers (BASPs). The research proposes use of strong, Two-Factor Authentication Protocols without Verifier Table. The suggested protocols, provides Users with flexibility of using a Password and either a Crypto-token or a Mobile-token to authenticate with Service Providers. The proposed approach eliminates the requirement of the User to remember multiple identities to access multiple services and provides the benefit of a higher level of security on account of second authentication factor and non-maintenance of verifier table at server.

Access to different services offered by multiple service providers using a single authentication token requires interoperability between providers. Also, the Service Providers will have to address the task of issuing the second authentication factor to Users. As a result, the research intends to propose the utilization of proposed two-factor authentication scheme within a specific environment which includes a trusted entity called an Identity Provider (IdP), with whom Users and Service Providers will be registered. The IdP is responsible for issuing and managing the second authentication factor.
In brokered authentication, the IdP playing the role of an authentication broker also provides Single Sign-on functionality. The Security Assertion Markup Language (SAML) is used by BASPs and the IdP to exchange authentication information about Users.

A major objective of this research is to propose an authentication model that can be adopted by both categories of service providers. Hence, this research proposes an authentication framework for cloud which supports an integrated authentication architecture that provides the service providers with the flexibility to choose between direct and brokered authentication. The integrated two-factor authentication protocol, which does not require the server to maintain a verifier table, supported by the framework allows users to do a single registration and access services of both direct & brokered authentication service providers using the same crypto-token/mobile-token.

To verify claims about security strengths of the proposed authentication protocols, security analysis is done using theoretical intuition. The proposed protocols are found to offer desirable security features such as resistance to replay attack, stolen verifier attack, guessing attack, user impersonation attack etc. To verify the efficiency of the proposed protocols, the communication and computation costs are compared with similar schemes and it is seen that the costs are comparable. To validate the resistance of protocols to authentication attacks, they are analyzed using automated verification tool called ‘Scyther” and the protocol strength is verified by “no attacks” results.