EFFECTIVE MANAGEMENT OF IDAAS ISSUES IN FEDERATED CLOUD ENVIRONMENT USING SAML AND QR-CODE

Sunitha Pachala¹, Dr Rupa Ch², Dr L.Sumalatha³
¹PhD Scholar, Dept of CSE, JNTU College of Engg, Kakinada, India
²Asst.Professor, Dept of CSE, Dhanekula Institute of Engg & Technology, Vijayawada, India
³Professor, Dept of CSE, Velagapudi Ramakrishna Sidhartha Engg. College, Vijayawada, India

Abstract: Managing various IDaaS issues i.e especially Identity and Access Management (IAM) services in cloud environment poses many challenges for enterprises and business organizations. Various Cloud based Identity Management Systems (IDMSs) have been proposed as of now. Yet, many of those systems are neither extensively accepted nor well-chosen eminently reliable due to their constraints in terms of extension, security, and their usability, configuration and deployment. Keywords: IDaaS, Identity and Access Management (IAM), WAMP Server, Single Sign-on (SSO), Authentication, Authorization, Cloud Service Providers (CSPs).

Keywords: IDaaS, Cloud Security, Identity and Access Management (IAM), Federated Identity Management, IdPs, Security Attacks, Multi factor authentication, Image Authentication, QR Code.

1. Introduction

Security has always been a concern for many organizations and business enterprises and facing challenges in protecting their data and other business credentials in the cloud environment. Managing the identities and restricting the access to various important resources becomes an important aspect of Identity as a service (IDaaS) in cloud environment[1]. As most of the enterprises and organizations are migrating towards the deployment and use of various cloud service providers (CSPs) and cloud architectures for effective utilization of their resources, the security features of IDaaS plays crucial role in establishing integrity of the enterprise. Especially, features like Single sign-on (SSO) is one of the important security aspects of IDaaS that provides better user experience by entering the user’s authentication credentials only once and hence permitting the users to access multiple resources of an enterprise in a secured way[2]. Single sign-on (SSO) is an application based on Security Assertion Markup Language (SAML). SAML is an XML based open standard developed by OASIS security Services technical committee. It asserts the identity of users to another system, without involving any other third party.

This is because of the lack of trust mechanisms and proper concrete agreements between the enterprises and various Cloud Service Providers (CSPs). A lot of research is still going on to counter these security challenges in cloud environment. Dealing with the identity of their employees and other users and ensuring the integrity of their data is always important for a business enterprise to keep their data and other credentials confidential and secret from their competitors. In this context, user authentication and authorization is crucial and access management also becomes critical. These days many companies and organizations are now focusing on the deployment of various technologies and tools for effective handling of these issues. OAuth and SAML standard technologies that facilitate the effective implementation of features like Authorization, Authentication and Single Sign-on (SSO).

Managing IDaaS services in federated cloud set up introduces many challenges these days. One way to improve the security and hence to manage IDaaS in better way is to multifactor authentication of the users by multiple IdPs[3]. This technique ensures the increased levels of security by prompting the users to enter his identity credentials number of times in multiple ways. Adapting the technologies like SAML or OAuth along with identity credentials like Quick Response (QR) code improves the security a lot.

The rest of this paper is organized as follows: Section 2 deals about the flow in SAML based SSO, section 3 about the brief literature survey and
related work, section 4 about multiple Identity Service Provider based Multi Factor Authentication, section 5 about proposed methodology and experimental setup, section 6 about the results and discussions and finally section 7 presents the conclusions and future work.

2. Flow in SAML based SSO

Figure 1 shows the flow of actions in an SAML based SSO. Initially the user requests the service from a service provider. The service provider requests the identity provider for the details of identity. Now SAML makes authentication assertion about the identity of the user. The authentication request will be sent to the user the response is sent back to the Identity Provider. SAML sends the authorization assertion to Service Provider. After receiving the assertions, then the Service Provider provides the service to the user.

3. Related Work and Literature Survey

Various commercial vendors already started working on the development of various tools and technologies to manage IAM and hence IDaaS services. Especially centrify developed its own licensed tool that integrates SAML technology [13]. Umme Habiba et al discussed about various identity management security issues and taxonomies at length [14]. Tri Hoang Vo at al presented the missing gap for moving enterprise applications in Inter-Cloud [15]. Securosis has presented a detailed study on various IAM cloud services [16]. David Nunez at al., has proposed a security model by integrating OpenID and proxy encryption scheme for better cloud based identity services [17]. Cloud Security Alliance discussed about various access management services in cloud [18]. Sean Deuby has mentioned in his article about the drawbacks of IDaaS. Tarek Kiblawi at al presented a closer look on the disruptive innovations in Cloud Computing and their impact on business and Technology [19].

Utpala Subodhani Premarathne at al has designed and implemented a frame work for effective mechanism for trust negotiations. They proposed completely new metrics based on the potential attacks and the vulnerabilities. They have also demonstrated these metrics using historical data sets [20]. Dominick Bayer at al presented various authorization and authentication mechanisms and identity services based on identity [25]. OpenID technique also permits to implement Single Sign-On (SSO) service, without asking the user’s password credentials again and again [26]. Bharath Bhargava at al reviewed about the privacy techniques in Cloud Setup [27].

4. Multiple Identity Service Provider based Multi Factor Authentication

In single cloud Identity provider based identity management i.e. Isolated and Centralized Identity management, the user credential attributes are stored at single Identity server and if the attacker gain access to it, then the users who have registered with that particular Identity Provider are at risk. So it is to better to go for Federated Identity Management Systems where user identity data or attributes are stored at multiple identity providers (IdPs) and even if the attacker gain access to one of the server, he cannot access others because there are multiple IdPs which are distributed at different locations and as the user identity information is not completely present at single Identity Provider. It is very much difficult for the attacker to crack the credentials in this case and this is the added security in Federated Identity Management Systems.

So in Federated Identity Management ,using multifactor authentication where at one of the Identity Provider (Idp1) ,using alpha numeric password based authentication factor and at the second Identity Provider (IdP2) we are using Quick Response (QR) code as the authentication factor[3]. And for the communication between the Service Provider and the Identity Providers we are using Security Assertion Mark-up Language (SAML) assertions.

5. Proposed Methodology and Experimental Setup

The working process can be understood as, first the User or Cloud Service Consumer registers with the Identity Providers (IdPs).When the user wants
to access a particular service from the Cloud Service Providers (CSPs). The user is presented with an interface at the Cloud Service Providers home page to select the trusted Identity Provider he is registered with and when the user selects the Identity provider he will be provided with an interface of IdentityProvider1 (IdP1) with username and password where the user enters his credentials which are verified by the IdentityProvider1 and if he is valid user then he/she is redirected to a second Identity Provider(IdP2) interface which generates a QR code and the user needs to scan it with the registered mobile which is used during registration process and if it is success, then the Identity Providers(IdPs) send SAML response to the Cloud Service Provider and based on the SAML Response assertions(attributes) which contain authorization information, the Cloud Service Provider provide Only the authorized services which the user is authorized to access.

In this model even if the attacker gains access to first Identity Provider where alphanumeric password based authentication technique is used, he cannot gain access to the second Identity Provider where QR code based authentication technique is used and for every new session a fresh QR code is generated and it requires to be scanned by the users registered mobile device and it is an added security as we have used multifactor authentication using different factors at different Identity Providers and the communication between the Cloud Service Provider and the Identity Providers occurs in the form of SAML assertions.Figure.1 depicts the concept of multiple identity service provider based multifactor authentication

---

**Figure.1.** A view of Federated Identity Management with User, Cloud Service Provider and two Identity Providers

The sequence of actions is shown in the figure 2 below.

**Figure.2.** Sequence of actions in the proposed Federated Identity Management Model

6. Results and Discussions

Figure.3 shows the home page of a Cloud Service Provider(CSP).

**Figure.3.** Cloud Service Provider(CSP) Home Page

Figure.4 shows the screen shot of log-in option of CSP.

**Figure.4.** The User Clicks on Login option

When the user clicks on login option he will be redirected to Identity Provider selection interface. It was shown in figure.5 below.
Figure 5. User Redirection to IdP Interface
Now the user will select the first Identity Service Provider IdP1 as shown in figure 6 below.

Figure 6. User selection of IdP1
When the user selects IdP1 he will be provided with a signIn page where he need to provide valid credentials and after successful verification by the IdP1, redirection goes to IdP2 as shown in figure 7.

Figure 7. log-in Page of IdP1 Interface.
After successful authentication by IdP1, IdP2 generates a Quick Response code which needs to be scanned by the mobile of consumer or user which is used during registration process. And after successful authentication by IdP2, the user is provided with requested services/application by the Cloud Service Provider based on the SAML authorization response send to the provider, as shown in figure 8 below.

Figure 8. Interface prompting for QR Code
After successful authentication by the Idp2 the Idp2 will send SAML authorization response to cloud service provider and based on that response the cloud service provider will provide the authorized services/applications to user as seen in above Interface as shown in figure 9 below.

Figure 9. CSP allows to access the Applications

7. Conclusions
These days most of the Cloud Service Providers are going for Federated Identity Management Systems instead of maintaining user identities on their own thereby CSPs need not bother of managing and providing security to user identities. In this paper, the issues related to security of user Identities, and proposed a secure federated identity management using SAML and Multi factor authentication using QR code and showed the implementation results. In this case even if the first IdP is compromised by the attacker, it is very difficult to gain access to second IdP as we have used QR code as the second authentication factor and it needs to be scanned by the user mobile which is used during registration. Therefore this level of authentication definitely increases the security as the number of factors in the authentication process increases. As part of future work this model can be enhanced to have more number of Identity Providers (IdPs) where different authentication factors for different Identity providers.

References


