Preserve Identity across distributed Server using Fedrated Identity Management System

Prof. Rahul R. Papalkar, Prof. Pravin R. Nerkar, Prof. N.S. Band, Prof. N.M Shivratriwar

Abstract— Using Single Sign On (SSO) user authenticate only one time & access several secure services & resources without reauthentication. Accessing several resources from distributed server is a complex job, simple Identity management does't preserve user identity across a distributed server, In this paper we mention the novel technique to preserve Identity across distributeted server using Fedrated Identity Management System. In this paper the proposed design allows user to use single set of credentials, even a user maintains with different kinds of cloud environments. We propose a solution with defacto standards of open authorization in which there is a trust party auditor which maintains all the credentials and cloud provider can uniquely distinguish one user from other. We also maintain secure channel for user in order to ensure the confidentiality.

Index Terms— Authentication, authorization, single sign on, Fedrated identity management, identity management, privacy, security.

1 Introduction

Cloud computing is not single technology is the combination of grid & cluster computing.Cloud means a distributed system.Cloud computing is popular due to its feature like high scalability and elasticity and also offers pay for use options for cloud users so that, user can pay based on their usage.

The National Institute for Standards and Technology (NIST) classifies cloud computing into three different service delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [1]. IaaS provides virtual computing resources such as virtual machines, networks and data storage. PaaS offers programming environments where customer can develop run and manage web application. Like .net framework using this framework developer can develop application without installing entire framework in client system. SaaS provide services through browser,user can acces software through internet from cloud service provider.

The today's need is to use Cloud computing in all areas where application can easily deploy on cloud and provides software as a service to users. The transfer of such applications to the cloud has a couple of advantages, e.g. less maintenance efforts or lower costs. But cloud service need to provide some level of security to such application. However, such security requirements are identification and authentication.

In web application security achived by two level one is high level & low level. In High level they achive securty using protocol like https,& in low level ie Page level security achive using simple mechanism called as username & password, but this most week technique to secure application, in simple authentication scheme multiple time authentication happend, this is very hectic while accesing resourses from distributed server . This problem get solve first using single sign on technique , then most popular fedrated user identity management system.

Developers should expect CSPs to offer a set of security features, including user authentication, single sign-on (SSO) using federation, authorization (privilege management), and SSL or TLS support, made available via the API. Currently, there is no PaaS security management standard: CSPs have unique security models, and security features will vary from provider to provider.

Identity federation is an emerging industry best practice for dealing with the heterogeneous, dynamic, loosely coupled trust relationships that characterize an organization's external and internal supply chains and collaboration model. Federation enables the interaction of systems and applications separated by an organization's trust boundary, e.g., a sales person interacting with Salesforce.com from a corporate network. Since federation coupled with good IAM practice can enable strong authentication by way of delegation, web single sign-on, and entitlement management via centralized access control services, it will play a central role in accelerating cloud computing adoption within organizations.

For achieving single sign on in cross cloud environment, the concept of federated identity management where credential of all the users manages to their respective cloud which avoids remembering and entering different credential for different application. The proposed approach also provides federated Identity management [3] which uniquely identifies the user in cross cloud environment. It manages the identity of all the users associated with different cloud in third party auditor which provides centralized authentication, where IID's of the entire user getting stored and managed.

2 Motivation

Detailed The user sign up for accesing cloud services by submitting their credential in cloud environment. Apart from providing the service, every service provider provides user management called identity provider to manage the user credential. Instead of maintaining all the user credential and authentication mechanism by service provider, the same can be possible to maintain in trust party auditor , so the user don't have to maintain different account for for accessing multiple application. User can directly logon to the services of different cloud providers by using a single set of credentials from a trusted third party vendor[3]. There are different protocols available to achieve single sign on namely SAML, open authentication mechanism like OpenId, Oauth etc. Sale and

OpenID are the standard protocols for single sign on authentication and proposed system uses the concept of OpenId provides authorization and authentication.

2.1 Objectives

1. The proposed system can be applicable to different cloud service provider , government firms in private domain.
2 It uses the concept of OpenID for generation of IIDs to securely accessing application from different domain.
3 For improving secure authentication, the concept of IP filtering and one time password are used.
4 For implementing Single sign on for different cloud application, the concept of Intercloud ID (IIDs) can be introduce which helps to improve trustworthy relation between different cloud application.
5 The proposed system can secure from some type of attacks like Denial of service, Identity theft etc.

6. Data files are also securely transfer from one cloud to another using AES encryption.
7 The end users, who are associated with different cloud, can also perform secure communication using AES 128 bit encryption.

3 Single Sign-On (SSO)

As Generally cloud service provider offers one or more SaaS applications for the user comfort. The provider maintains user data in management database for further identification and authentication. If cloud service provider offers multiple SaaS application then separate user management need to be run for each application. Therefore, when user want to access n application from same or different cloud service provider then user must go through n times authentication. These continuous authentication processes may lower the user’s reliability. To overcome this drawback, the concept of single sign-on (SSO) can be used. SSO allows the user to access one or more application by authenticating only once which avoids frequent reauthentication[2]
so the user usability can increase. In SSO, user has to provide unique or single set of credential for accessing n application, so once the user is authenticated at one cloud service provider then they automatically identified in other cloud service provider. The SSO system provides various advantages, first user just need to remember single set of credential which avoids burden on user. Second authentication time and cost can be save. Third only single user management need to run at cloud service provider side which improves security and avoids maintenance of multiple databases. SSO system also have some drawbacks like If someone steals your credential then complete SSO system is available to the attacker and If the user management fails then user can not able to access single application. The whole system is disturbed.

TABLE 1
Comparison of Protocols used to achieve SSO in Cross-Cloud Environment

Parameters	SAML	WS-Federation	OpenID	OAuth	Shibboleth
Authentication	SAML does not specify the method of authentication, it can be username/password or multi-factor authentication	Used security token services (STS) for authentication.	Used user Login credential as authentication mechanism	Used limited access OAuth Token i.e. valet key as authentication mechanism	Used user organization Login credential as authentication mechanism and send minimum details to service providers
Develeoped by	OASIS	BEA Systems, BMC Software, CA, IBM, Microsoft, Verisign	OpenID foundation	IETF OAuth WG	Open source software and release under Apache software License
Method of Exchange	XML based	XML based	URL-based OpenID identifier	API interface	Manage the list of providers and common rules between the providers
Applicable to	Web SSO, Attribute-based authorization, Securing web services	Microsoft Window Azure cloud platform	Google	Facebook, LinkedTn, or Twitter	Used in Universities and public service organization

Identity Management
Authentication, maintenance, discovery, information exchange, administration, management and policy enforcement used to ensure identity information these are the functions & role of identity management which improves security. An IMS provides set of rules for managing an individual user identities in a digital environment[10] .

The main functions of an of identity management system is as follows:
1. **Provisioning:-** the identity management system must ad-

dresses the provisioning and de-provisioning of user identities within an organization. There are various types of user are managed in organization. Based on their respective roles or designation the user accounts must provide (Example the role can be end user, IT administrator, supervisor, application administrator, developer etc.)[4].
2. **Authentication:-** with the help of authentication service the user can authenticated by identity management system by entering some credential like login id, password, token, biometric etc. once the user is authenticated the respective service is openly available to user.
3. **Authorization:-** The main goal of identity management system is to provide security to users and this can be achieved through authorization technique. Authorization allows the user to access the services based on some access level.
4. **Federation:-** federation allows the group of organizations or service provider establishes a circle of trust between them, and allows to share user identities with each other[4].

3.1 Federated Identity Management [2]

In the Internet users obtain access to the resources belonging to the different service providers by using different accounts. Passwords and user names generated in these accounts are different from each other. For this reason, the vast majority of the network users, try to use the same password in each possible place. This leads to serious security risks. The repeated authentication of the users causes the troubles among them and beside that it also strongly increases the series of the administrative expenses. Nowadays the majority of the world global organizations in order to struggle with passwords try to use SSO (Single Sign On) technologies as these technologies allow to replace the number of network passwords with a single password.

Identity Federation:- one of the identity management concepts [11], that share and distribute attributes and identity information across different administrative domains according to certain established policies.

Following three actors is forms identity federation model (Figure 1)[2]:
1. **Service Provider(SPs):-** Actors which consumes users identity data. They rely on the user authentication made by a third party. SP are also called Relaying Parties(RP)[2].
2. **Identity Providers(IdPs):**- Actors that assert information about a subject. IdP are also called asserting partoes(AP). IdPs focuses on the authentication of the users as well as on the management of identity information, which can be shared with various SP[2].
3. **Users:**- Actors which interact (ususlly vis the user agent, e.g. web browser) with SPs. They are the subject of the assertions[2].

As shown in the fig 1, the share of the identity information between the two providers (IDp1and IdP2) allows a user to login only once and gain a seamless access to services and applications offered in different domains. Identity federation can be accomplished by means of SAML, OpenID oauth or WS-Federation.

The below model is suitable for only static trust relationship.

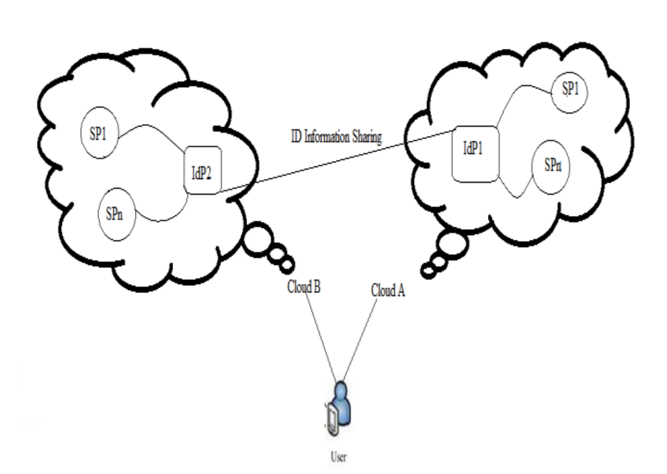

Fig. 1. Identity Federation Process.

3.2 Identity Providers and their Standards

The Table 2 describes the identity federation acceptance by various major cloud based application. The service providers are Google, Facebook, Twitter, Amazon web services(AWS). These providers standard protocol like SAML, Oauth and OpenID etc.

TABLE 2
IDENTITY PROVIDE BY DISTICT PROVIDER AS DIFFERENT STANDARD

	SAML	OPENID	OAUTH
FACEBOOK	NO	NO	YES
GOOGLE	NO	YES	YES
AWS	NO	NO	NO
TWITTER	NO	NO	YES

Proposed work

- To understand the fundamental concept like SSO, identity management etc.
- To understand the challenges and possible attacks. Understanding cross cloud architecture.
- Designing and implementing the cross-cloud federated identity management system.

4 CONCLUSION

IJSER In cloud computing it is typical task to preserve the identity across the distributed network, in our article we proposed the solution for that problem using Fedrated identity management.. Preserving privacy is also the main issue, by implementing the concept of identity management we will also preserve the privcy across the distributed server of distict service provider.

REFERENCES

[1] Fatemi Moghaddam, F.; Karimi, O.; Hajivali, M., "Applying a single sign-on algorithm based on cloud computing concepts for SaaS applications," Communications (MICC), 2013 IEEE Malaysia International Conference on , vol., no., pp.335,339, 26-28 Nov. 2013 doi: 10.1109/MICC.2013.6805850

[2] AzerbaijanBalasubramaniam, S.; Lewis, G.A.; Morris, E.; Simanta, S.; Smith, D.B., "Identity management and its impact on federation in a system-of-systems context," Systems Conference, 2009 3rd Annual IEEE , vol., no., pp.179,182, 23-26 March 2009 doi: 10.1109/SYSTEMS.2009.4815794.

[3] Revar, A.G.; Bhavsar, M.D., "Securing user authentication using single sign-on in Cloud Computing," Engineering (NUiCONE), 2011 Nirma University International Conference on , vol., no., pp.1,4, 8-10 Dec. 2011 doi: 10.1109/NUiConE.2011.6153227.

[4] Identity management based security architecture of cloud computing on multi-agent systems by R.M Lguliev Institute of Information Technology ANAS Baku, Azerbaijan, F.C. Abdullayeva Institute of Information Technology ANAS Baku,

[5] Khan, R.H.; Ylitalo, J.; Ahmed, A.S., "OpenID authentication as a service in OpenStack," Information Assurance and Security (IAS), 2011 7th International Conference on ,vol., no., pp.372, 377 ,5-8Dec. 2011 doi: 10.1109/ISIAS.2011.6122782.

[6] Cross-domain Identity Management System for Cloud Environment by: Nazia akhtar Aisha sajid,M Shoaib Farooqui.

[7] Secure Cross-Cloud Single Sign-On (SSO) using eIDs by Bernd wattendorfer, Arne Tauber E-Government Innovation Center (EGIZ) Graz University of Technology Graz, Austria.

[8] Single Sign On For Cloud by Pratap Murukutla National Institute of Technology,Karnataka, K.C. Shet National Institute of Technology,Karnataka.