Volume 5, Issue 4, 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Comparison of Different Authentication Protocols Used for Federated Identity Management in Cloud

Meenakshi Bhat, Prof. Anuradha Panjeta
CSE & Kurukshetra University
Haryana, India

Abstract— In the past few years cloud computing has emerged as a boon for IT industry. Cloud computing is a playing field leveller; it gives small businesses access to technologies that previously were out of their reach and lets small businesses compete with both small businesses and big ones. And to make the deal even better, cloud computing can save small business money, too. There are still many organizations who have not adopted this concept because of security reasons which means authentication becomes important in cloud. In this paper we have discussed few authentication protocols used for federated identity management in cloud and also tried to layout their differences

Keywords— Authentication, Identity federation, SAML, Open ID, OAuth, Single- Sign-On (SSO).

I. INTRODUCTION

Cloud computing is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.With cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, notebooks, handhelds and other devices. The most common analogy to explain cloud computing is that of public utilities such as electricity, gas, and water. Just as centralized and standardized utilities free individuals from the difficulties of generating electricity or pumping water, cloud computing frees users from certain hardware and software installation and maintenance tasks through the use of simpler hardware that accesses a vast network of computing resources (processors, hard drives, etc.). The sharing of resources reduces the cost to individuals. Users face difficult business problems every day. Cloud computing adopts concepts from Service-oriented Architecture (SOA) that can help the user break these problems into services that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way.Cloud computing also leverages concepts from utility computing in order to provide metrics for the services used. Such metrics are at the core of the public cloud pay-per-use models. Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques[1].The National Institute of Standards and Technology‘s [2] definition of cloud computing identifies "five essential characteristics":

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service . Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. Despite of all these facts organizations have failed to fully adopt this concept because of security concerns. Authentication and identity management one of security and privacy issues in cloud computing have become increasingly an area of concern for organizations.

In this paper our focus is on authentication in cloud. The rest of the paper is organized as follows: section2 and section3explains cloud deployment models and service models.Section4 explains the process of authentication and identity federation in cloud,section5 defines the challenges faced in federated identity management. Then we have authentication protocols explained in section6 with their comparison in section7.Section 8 discusses the problems faced in real world regarding SSO.Section9 concludes the paper and finally some references have been given.

II. Authentication and Federated Identity

A. Authentication:

Authentication is the process for confirming the identity of the user. The typical authentication process allows the system to identify the user (typically via a username), and then validate their identity through user-provided evidence such as a password. There are stronger methods of authenticating the user[9], including certificates, one-time passwords, and device fingerprinting. These can be combined to provide a stronger combination of authentication factors which leads to multifactor authentication in cloud where a user has to provide multiple pieces of evidence to prove their identity.GazzangzTrustee offers a unique multi-factor solution[10] built for cloud environments.Rather than requiring a biometric characteristic or a physical card or token,it uses designated people or processes as a second factor.GazzangzTrustee is a key and certificate manager that stores and manages cryptographic keys ,certificates,configuration files,tokens and any other opaque objects an enterprise maintains to secure its most sensitive data. The user should be able to authenticate themselves using standard authentication protocols or identity providers, such as SAML, OpenID, OAuth. A user can use the services of different cloud service providers,but before that he needs to build a trust with the cloud service provider. For this he has to authenticate himself on every cloud by providing different login details. Organizations needed a way to unify authentication systems in the enterprise for easier management and better security. Single sign-on was widely adopted and provided a solution for keeping one repository of usernames and passwords that could be used transparently across several applications. The problem?How to bring together user login information across many applications and platforms to simplify sign-on and increase security.The solution? Federated identities .

B. Federated Identity:

Federated identity[11] means linking and using the electronic identities a user has across several identity management systems. In simpler terms, an application does not necessarily need to obtain and store users' credentials in order to authenticate them. Instead, the application can use an identity management system that is already storing a user's electronic identity to authenticate the user—given, of course, that the application trusts that identity management system. For example, Facebook Connect is a federated identity management system. Another example, this time in the public arena, is the UK Government Department for Work and Pensions allowing UK residents to sign-up and sign-into its website to manage benefit claims using their login information from one of eight providers, all private companies, including Experian and PayPal.

In information technology,federated identity means:

1. Single authenticated user identity that is accepted as valid across a wide variety of identity management systems.
2. A user's authentication process across multiple IT systems or even organizations.

As far as our case is concerned users of different cloud service providers can use a federated identification for identity establishment in cloud computing. It makes easier to centralize the authentication and authorization functions in the enterprise to avoid a situation where every application has to manage a set of credentials for every user.The diagram for federated identity management is shown in Fig. (1) below.

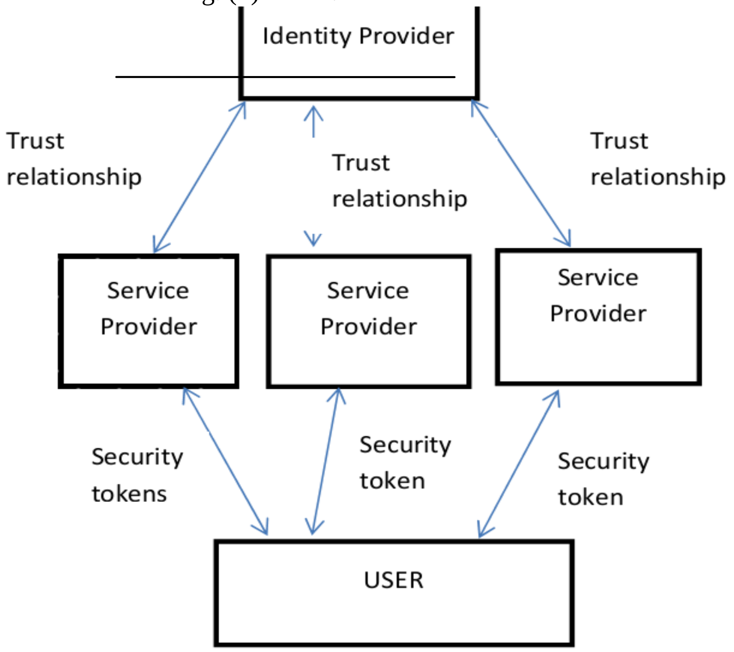

Fig 1: Federated Identity Management

III. Identity Management

Federated identity management faces various challenges which are categorized into technological, economical and legal challenges[12].

1. Identity management is highly dependent on technology. These might include technologies used to create secure data tokens, encryption technologies and various data security technologies. These technologies should be utilized properly to achieve the intended result. Thus one key challenge to the participants in the identity management is the risk involved if the technology designed does not achieve the desired results or do not function properly.[12]
2. Identity management depends on different processes and procedures which merely include series of steps performed by a person such as identity proofing an individual subject which might include which documents to be checked to verify that person online. Again there is a challenge involved that whether mere identity proofing is enough to establish a secure and trustworthy relationship with the user. [12]
3. Another challenge involved in identity management is regarding the performance. Although the processes and technology may work properly but they are of little or no value if they are not properly implemented or understood by a person responsible for using them. Thus one key challenge to the participants is the risk involved if the person does not act according to his role on whose performance the system depends. [13]
4. One more challenge in federated identity management is related to privacy. Identity management involves collecting data by identity provider and disclosure of information to relying party.There is routine transfer of information between organizations as well as between individuals and organizations and it may cross the organizational boundaries. The personal data collected as part of the identity proofing may be misused by the parties who have access to it or it may be improperly disclosed.[12]
5. Another challenge to federated identity management is the liability risk. Identity Management may suffer from faulty Identification, faulty authentication, inadequate security or misuse of personal data, or failure to follow appropriate procedures. Thus the concern is who will be held liable for the risk associated with these problems. So the challenge here is that every participant may be held legally responsible for the problems or damages due to the above reasons and need to address these issues.[14]
6. In identity management if one participant fails the other must have the ability to identify the reason behind failure, remedy such failures and compensate for any losses suffered. So it focuses on enforceability risk which refers both to the ability to detect that problem, as well as the ability to require the participant to remedy its performance or withdraw from the system.[15]
7. In identity management both the identity provider and the relying party must comply on certain applicable laws in order to know the manner in which information is collected, used and stored by the identity provider. If any of the participant acts contrary to the requirements of those laws then there is compliance risk to the participant. [14]

IV. OPENID, SAML& OAUTH

A. OpenID:

OpenID[16] is an open standard that allows users to be authenticated by certain co-operating sites known as identity providers (or Relying Parties) using a third party service, eliminating the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. Users may create accounts with their preferred OpenID identity providers, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication. OpenID is an open standard sponsored by Facebook, Microsoft, Google, PayPal, Ping Identity, Symantec, and Yahoo.

B. SAML:

SAML, developed by the Security Services Technical Committee of "Organization for the Advancement of Structured Information Standards" (OASIS)[19], is an XML-based framework for exchanging user authentication, entitlement, and attribute information. SAML is a derivative of XML. The purpose of SAML[17] is to enable Single Sign-On for web applications across various domains.The SAML specification defines three roles:The principal, which is typically the user looking to verify his or her identity.The identity provider (idP), which is the entity that is capable of verifying the identity of the end user.The service provider (SP), which is the entity looking to use the identity provider to verify the identity of the end user.SAML will be supported for organization users. An organization administrator can configure the SAML URL and the public key. A user from the organization should login with his/her domain say "https:// .business.zoho.com". The user will be redirected to the IDP provided for SAML with the SAML request for authentication. The IDP will authenticate and send us the SAML response. If the response is success, a ticket will be generated for him and will be set in the cookie.

C. OAuth

OAuth is an emerging authentication [20]standard that allows consumers to share their private resources (e.g., photos, videos, contact lists, bank accounts) stored on one cloud service provider(csp) with another cloud service provider without having to disclose the authentication information.It is supported[21] via an API by service providers including GOOGLE, TWITTER, FACEBOOK, and PLAXO. OAuth is different than OpenID and SAML in being exclusively for authorization purposes and not for authentication purposes.The OAuth[27] specifications define the following roles:The client (OAuth Consumer), which is the entity that is looking to consume the resource after getting authorization from the client.

TABLE I COMPARISON AMONG OPENID, SAML&OAUTH METHODS[24]:

Method	**Authentication [29]**	**Discovery**	**SP/IdP Initiated[23]**	**Protocols used [22]**	**Scope**	**Identifiers[23]**	**Degree of security [28]**
OpenID	With OpenID, the process starts with the application asking the user for their identity typically an openidurl.	It does not require hard coding the provider we want to use ahead of time.Usingdiscovery,the user can choose any third-party provider they want to authenticate.	It is always SP initiated.	XRDS, HTTP	It is used to facilitate SSO for consumer apps. and services.	Default assumption is that users are identified by a personal URL.	Less secure
SAML	Its authentication process is based on explicit trust between your site and the identity provider.	SAML provider usually has to be coded in advance and we federate our appn. with only selected IdP.	It can be SP or IdP initiated.	SAML, XML,HTTP,SOAP	Typically used in Enterprise SSO scenarios.	Allows for a variety of identifier types, from pseudonyms to one-time anonymous.	Highly secure
OAuth	In this case the application directly requests a limited access OAuth token to access the API's on user's behalf.	It does not support discovery,so it requires pre-selecting and hard-coding the providers we decide to use.	It is also SP initiated but OAuth 2.0 is expected to be IdP initiated.	JSON,HTTP	It has been designed for use with apps. on the internet,primarily for delegated authorization of internet resources.	The service is identified rather than the user. An opaque one-time identifier is used to map between user accounts on each side.	Inherently insecure

IV. CONCLUSION

With the evolution of new technologies like cloud computing authentication has become a crucial factor in identity management .In this paper we have presented various protocols that are being used for federated identity management. The comparison of these protocols is also presented in this paper based on various parameters like scope, authentication etc. The paper also reveals the various challenges that are being faced in federated identity management. The future work includes proposing a model that will overcome these challenges in order to widen its adoption across different organizations.

REFERENCES

[1] HAMDAQA, Mohammad (2012). Cloud Computing Uncovered: A Research Landscape. Elsevier Press. pp. 41 85. ISBN 0-12-396535-7 .

[2] "The NIST Definition of Cloud Computing". National Institute of Standards and Technology.Retrieved 24 July 2011.

[3] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy." KM World , pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[4] "Defining 'Cloud Services' and "Cloud Computing"". IDC. 2008-09-23.Retrieved 2010-08-22.

[5] http://blogs.gartner.com/thomas_bittman/2012/09/24/mind-the-gap-here-comes-hybrid-cloud/

[6] Voorsluys, William; Broberg, James; Buyya, Rajkumar (February 2011). "Introduction to Cloud Computing". In R. Buyya, J. Broberg, A.Goscinski. Cloud Computing: Principles and Paradigms. New York, USA: Wiley Press. pp. 1–44. ISBN 978-0-470-88799-8

[7] Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds [1]

[8] "HVD: the cloud's silver lining". Intrinsic Technology.Retrieved 30 August 2012.

[9] User Authentication in Cloud Computing.Hyokyung Chang, Euiin Choi. Springer

[10] Secure User Authentication in Cloud Computing Management Interface. Liliana F. B. Soares, Diogo A. B. Fernandes, Mário M. Freire and Pedro R. M. Inácio

[11] Trusted Federated Identity Solution Architecture Business Requirements.White Paper

[12] Economic Tussles in Federated Identity Management.Susan Landau Radcliffe Institute for Advanced Study Harvard University.Tyler Moore Center for Research on Computation & Society

[13] An Investigation of Challenges to Online Federated Identity Management Systems by AparajitaPandey and Dr.Jatinderkumar R. saini.International Journal of Engineering Innovation & Research Volume 1, Issue 2, ISSN : 2277 – 5668

[14] http://docs.oracle.com/cd/E15523_01/oim.1111/e13400/intro.htm

[15] Kuyoro S. O., Ibikunle F. &Awodele O. International Journal of Computer Networks (IJCN), Volume (3) : Issue . (5) : 2011 247 Cloud Computing Security Issues and Challenges

[16] http://en.wikipedia.org/wiki/OpenID

[17] https://adminconsole.wiki.zoho.com/accounts/SAML-Authentication.html

[18] http://stackoverflow.com/questions/7699200/what-is-the-difference-between-openid-and-saml

[19] http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

[20] http://architects.dzone.com/articles/saml-versus-oauth-which-one

[21] A Survey Paper on Social Sign-On Protocol OAuth Journal of Engineering, Computers & Applied Sciences (JEC&AS).

[22] http://www.softwaresecured.com/2013/07/16/federated-identities-openid-vs-saml-vs-oauth/

[23] http://www.eb2bcom.com/information/whitepapers/pingidentity/internet_scale_identity_systems.pdf

[24] Comparative analysis of various authentication techniques in cloud computing. International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 4, April 2013

[25] Why did Microsoft Passport fail, and how good is the CardSpace solution?Mohammed H. Almeshekah and Waleed A. Alrodhan.Information Security Group Royal Holloway, University of London.Egham, United Kingdom{m.h.almeshekah, w.a.alrodhan} @rhul.ac.uk.

[26] Risks of the Passport Single SignonProtocolDavid P. Kormann and Aviel D. Rubin AT&T Labs – Research {davek,rubin}@research.att.com.

[27] https://community.jivesoftware.com/docs/DOC-103154

[28] http://www.baypayforum.com/news-from-the-industry/entry/intro-to-openid-oauth-and-saml

[29] http://developers.axiomatics.com/blog/index/entry/authentication-vs-authorization-part-2-saml-and- oauth.htm