Advances in Computer Science and Information Technology (ACSIT)
Print ISSN : 2393-9907; Online ISSN : 2393-9915; Volume 2, Number 7; April – June, 2015 pp 58 – 63
Krishi Sanskriti Publications
http://www.krishisanskriti.org/ACSIT.html

Secure interoperable identity in the cloud: Issues and Techniques

Pankaj Deep Kaur[1], Tania Chaudhary[2]

[1]CSE Department
GNDU RC Jalandhar, Punjab, India
[1]pankajdeepkaur@gmail.com
[2]MTECH CSE(2nd sem)
GNDU RC Jalandhar, Punjab, India
[2]chaudharytania57@gmail.com

Abstract: *The migration of desktop application to cloud computing platform has raised concerns about the privacy of sensitive data belonging to users . Cloud users suffers from identity theft, duplicate identity and interoperable identity issues among different clouds. Various standards and techniques have been developed to secure the identity of cloud consumer. In this paper various interoperability issues regarding cloud, open standards for cloud identity management and various identity management techniques are discussed.*

Keywords- IDM, SAML, XAML, SPML, SLA, SSO, STS, SMS, API, PRIME, ZKP

1. INTRODUCTION

Cloud computing is a technique that provides convenient on demand service to its users from shared pool of resources.The cloud model promotes availability and is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), three service models (IaaS, PaaS, SaaS), and four deployment models (Private, Community, Public, Hybrid). For efficient cloud services we need interoperability between clouds which means ability to comfortably move workloads and data from one cloud provider to another or between private and public cloud.

Vendor Lock-in is the main barrier behind interoperability between clouds.Vendor Lock-in mechanism refers to the situation in which if an organization or consumer has selected a cloud provider, either it cannot select another provider or it can select another provider at a very high cost. The main requirement for interoperability is to maintain identity of the organization or user of cloud and make it securely interoperable, means if an user has maintained identity with one cloud provider it can use this identity to fetch resources from other another cloud provider.

While usinginteroperable identity service consumer provide some sensitive and confidential data in order to have access to online services.

Identity management services in cloud computing environments are mainly responsible for authenticating users and supporting access control to services based on user attributes, such services should preserve the users' privacy while supporting interoperability across multiple domains and simplifying management of identity validation, as they evolve to Intercloudmouldings, identity management systems should not only be capable of identifying users but also resources that originate from different clouds.

2. IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity and access management in cloud deals with a secure unique identity of cloud consumer with the help of which it can interoperate between clouds and access cloud resources. Handing sensitive data to cloud service provider (SP) is a serious concern because cloud computing can increase the risks of security breaches. Knowing who has user's personal data, how they are being accessed, and the ability to maintain control over them prevents privacy breaches and can minimize the risk of identity theft and fraud. IAM(Identity and Access Management) is the key to cloud privacy and security.
Federated Identity

To have secure identity and access management we use Federated Digital identity, Federated here means identity is managed by single entity, it is a centralized approach where some internal autonomy is maintained.[2] **Federated Identity** is a way through which an organization can manage consumers electronic identity and attributes across multiple domains.In the cloud computing environment, federation of identity plays a key role in enabling allied organizations to authenticate, provide single or reduced signon, centralized

authentication, and exchange identity attributes across multiple cloud computing domains.

3. OPEN STANDARDS FOR MANAGING DIGITAL IDENTITIES ON CLOUD

A. Security Assertion Markup Language (SAML)- It provides an XML based message exchange open standard protocol that specifies the rules for exchanging security assertions among multiple organizations and applications. Three security assertions are defined under it i.e. authorization, authentication and attributes.SAML[3][4] allows the receiving entity to validate the request before sending a response. This validation is done through 'claim set' (that includes User name, User role, Purpose of use, User organization, Authorization details, Digital signature, Issuer).

B.eXtensible Access Control Markup Language (XAML)- It[5]provides a means for organizations to implement a common authorization method across federated clouds.

Consists of four policy components: PEP, PIP, PDP, and PAP

- Policy Enforcement Point (PEP) – enforces policy decisions and admission control in response to a request for information and/or resource.
- Policy Information Point (PIP) – supplies data that's used for evaluating an authorization policy.
- Policy Decision Point (PDP) – makes decision for entity to gain access to resource and/or information.
- Policy Administration Point (PAP) – creates a policy or a set of policies.

C. Service Provisioning Markup Language (SPML)- It[6]provides an open standards approach for managing user accounts. Allows organizations with enterprise level platforms (e.g., web portals, application servers, and service centers generate provisioning requests) to generate requests across organizations.

Standard	SAML(Security Assertion Markup Language)	XAML(eXtensible Access Control Markup Language)	SPML(Service Provisioning Markup Language)
Features	It is used for exchanging authorization data.	It is used for creating GUI . It is used to implement common authorization method among cloud.	It is used for exchanging users, resources and service provisioning information.
Single Sign-On	It provides single sign-on facility.	It provides single sign-on facility.	It do not provide single sign-on facility. It is used for integration and interoperation of service provisioning requests.
Authorization	Authorization is done through claim set.	Authorization is done through policy enforcement.	In relation to SAML and XAML it provides provisioning/de-provisioning processes from the identity provider to its target service providers.

Table1: Comparative analysis of open standards for cloud identity management

4. TECHNOLOGIES USED FOR MANAGING DIGITAL IDENTITIES ON CLOUD

A. Single Sign-On (SSO) / Reduced Sign-On (RSO) – It[7]enables an organization to implement federated identity between multiple domains. Main motive of this technique is maintain a single identity of a consumer and interoperate it among multiple domains. Allows a user to authenticate to a single system, while the SSO system manages the user's access to other systems.
Common SSO implementations of this technique are:

*Kerberos Ticket-Granting Ticket (TGT)
*Smart Card Based (e.g., Government CAC card)

B. Secure Token Service (STS)- Itis a key aspect in implementing a securefederated cloud environment.STS[7] provides a softwarebased identity providercapability that is responsiblefor issuing security tokens in a claims-based identity system.

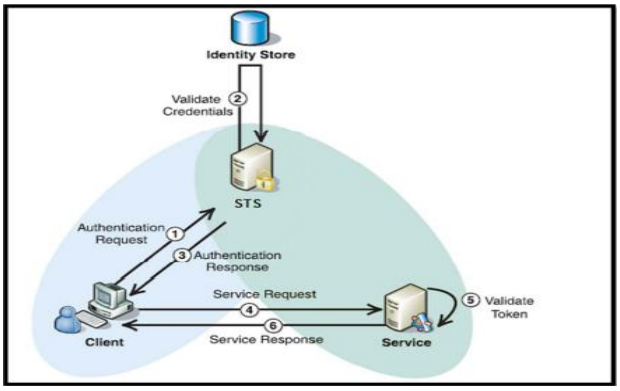

Figure1: Security Token Service Model[7]

C. Secure Mediation Service (SMS)– Itprovides the conduct for subjects[7] (users, systems , services) to request and receive resources and services across cloud computing domains, by providing information to authenticate and authorized subjects, so that consumers can securely access them online.

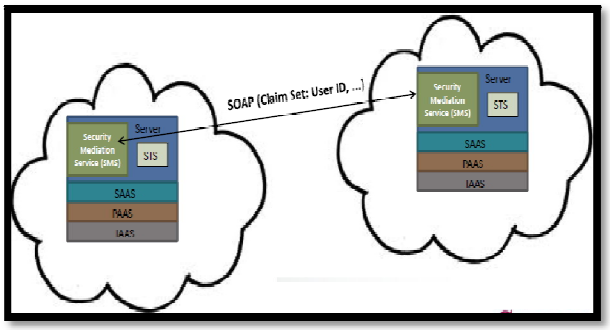

Figure2: Secure Mediation Service Model[7]

D. Application Programming Interface (API) Key – It[7]provides an additional layer of security for resources or service exchanges. It's key functions serves as a: unique identifier, Security token for authentication and set of access rights on the API associated withit.

5. IDENTITY MANAGEMENT SOLUTIONS BASED ON THESE TECHNIQUES AND STANDARDS

Identity and access management is an integrated approach in which four entities are involved

1) Identity provider (IdP). It issues digital identities.
2) Service provider (SP). It provides services to user/entities that have required identities.
3) User/Entity. Have to claim who they are prior of accessing services in the cloud.
4) Identity management. A third trusted party used to manage digital identities.

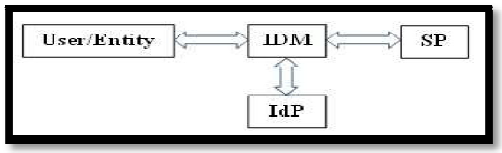

Figure3: Identity Management System[8]

A. OpenID

OpenID[8][9] is a technique used for user authentication without requiring separate ad hoc systems and helping in federation of user's identities. With OpenID a consumer uses single username and password to access multiple web sites. The user authorize to an OpenID server to get theirOpenID and use the token to authenticate to web sites. A user of OpenID does not need to provide a service provider with his predicate or other sensitive information.OpenID is a decentralized authorization protocol. No central authority must acclaim or acceptOpenID Providers. The consumer is free to choose an OpenIDProvider(OIdP), and can secure their attributes if they shiftOpenID Providers. OpenID is highly susceptible to security breaches. A consumer who visits an malicious site, sends the fake service provider hisURL. The provider consults the URL's content to fetch the location of his OP (OpenID provider). Instead of redirecting the user to the valid OP, it redirects him to the malicious site. The Evil Scooper contacts the valid OP and pulls down an exact replica of its login information (it can simply actas "man in the middle"). Convinced he is talking to his OP, the user posts his attributes (username and password) which can now be used by the malicious scooperto get tokens from the legal OP. These tokens can then be used to gain access to any legal Service Provider.

B. PRIME (Privacy and Identity Management for Europe)

PRIME[8][9], is a distinct application — the PRIME Console — that handles user's private data PRIME's approach uses "private credentials" which enable proving one's authorization (e.g., to be over 18 years old) without disclosing details that may recognise the individual. These private credentials are derived from certificates issued on different pseudonyms of the same person. Multiple private credentials can be generated from a single certificate that are neither associated to each other nor to the issuance interaction in which the master certificate was obtained. Private credentials provide accountability while protecting the anonymity of the user as long as there is no misuse – in this case the user's anonymity can be revoked. A major challenge for a large scale adoption of PRIME technology is that it requires both individuals and service providers to implement the PRIME middleware, on both sides. Another prerequisite for large scale adoption of PRIME is interoperability.

C. CardSpace

When a CardSpace-enabled application or website wishes to authenticate a user, it requests a particular set of claims from

the user. The user selects an InfoCard to use among the ones visually presented to him, and the CardSpace[8][9] software contacts an IdP to obtain a digitally signed XML security token that contains the requested information, which is communicated to the requesting application. A user might rely on an application that supports CardSpace, such as a Web Crawler, to access any of several relying parties. It might also be able to select from a group of identity providers as the source of the digital identity presenting those relying parties. Whatever choice is made by the user, the basic exchange among these parties has three steps:

First, the application gets the security token requirements of the relying party (RP) that the user wishes to access. This information is contained in the RP's policy, and it includes things such as what security token formats the relying party will accept, and exactly what claims those tokens must contain.

Second, once it has the details of the security token this RP requires that the application passes this information to CardSpace, asking it to request a token from an appropriate IdP.

And third, once this security token has been received, CardSpace gives it to the application, which passes it on to the RP. RP can then use this token to authenticate the user or for some other purpose.

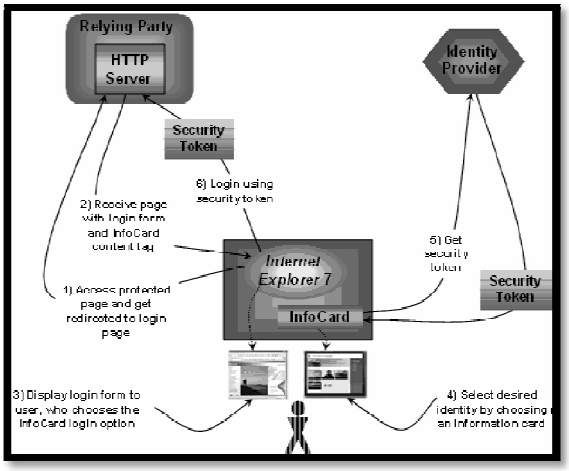

Figure4 Card Space Model[9]

These solutions suffer from some limitations. The consumers do not pay much attention when they are asked to accept a digital certificate, either because they do not understand the importance of the approval decision or because they know that they must accept the certificate in order to get access to a particular website. RPs without any confirmation certificate can be used in the CardSpace framework (given user consent), and this leads to a serious risk of a security breaches.

Another limitation isReliance on a Single Layer of Authorization: The security of the CardSpace identity meta system depends upon the authorization of the user by the IdP. In a case where a single IdP and multiple RPs are involved in a single working environment, which we expect to be a typical scenario, the security of the identity metasystem within that working environment will rely on a single layer of authorization.. In the majority of cases, a simple username/password authorization technique will be used. If a working session is hijacked or the password is cracked, the security of the entire system will be compromised.

C. Horizon

Horizon is VMWare's Identity and Access Management (IAM) product. Provides organizational management access via web applications. Leverages an organization's existingdirectory services by pulling userauthentication into the cloud. Metadata is used to associate auser's identity with the cloudmanagement product.

D. Keystone

Keystone is Openstack IAM product.Token generation is used to authorize users. Provides authentication and authorization services for all OpenStack components.Provides a catalog of available services.Provides a means for thesoftware to integrate with an existing backend directory service such as LightweightDirectory Access Protocol (LDAP).

E. Elastic Compute Cloud (EC2)

It creates trust challenges fororganizations seeking to employ aninteroperable IAM solution.Provides support for identity and access management that implements usersecurity credentials, managespermission assignments, and allows organizations to set up IAM functionality via APIs.

To remove the limitations three approaches are used

- *Zero Knowledge Proofing*: The ZKP[9] approach allows the user to prove his allegation without disclosing his credentials. A solution using a ZKP works in the following way: a service provider requires a user to be over 18. The consumer need to pacify the relying party's technical agreement but tell the party nothing or as light as possible. The consumer need not to disclose his date of birth, instead he somehow needs to prove that he's over 18. This proves something without disclosing all.

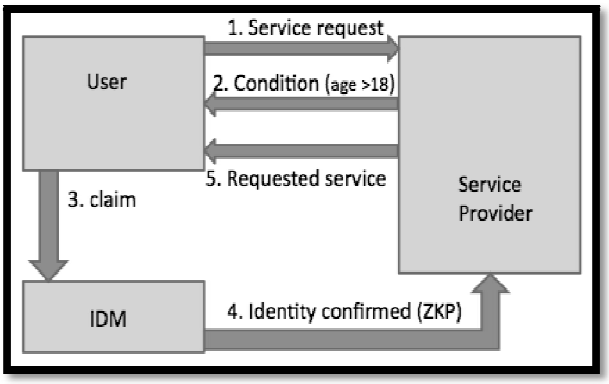

Figure5: ZKP Implementation[9]

- *Selective Disclosure Approach*: In the Selective Disclosure[9] protocol exchange of data is performed such that the consumer reveals certified data in a data minimizing approach (little/selective revelation of personal identification information(PII)). This approach uses predicates over traits in addition to simple pairs, e.g., one may state that their age is less than or equal to stated fixed value. Predicates over data are part of a logical formula that makes more general assertion about identity associated with a party. A set of predicates for making data minimizing assertions, such as =, ≠, <, ≤,>, ≥, can be embedded in the SAML Tokens.
- *Anonymous Credential*: This scheme allows consumer to derive from a single master secret key multiple cryptographic pseudonyms[9]. Then, it authenticates himself by proving that he knows the master secret key underlying a cryptographic pseudonym i.e. (Derived pseudonym predicate). The predicate *NymDer*(*nym,A*) is true if and only if A encodes the master secret key from which the cryptographic pseudonym *nym*was derived. The central idea is that all the user's credentials are underlain by the same master secret *msk*, so that by sharing *msk*with others, the user is sharing her whole identity, rather than just her pseudonym *nym*and the associated access to this service. However, the pseudonyms are not linkable to the user and keep the user anonymous in a sense. The pseudonym mechanism can be integrated in the SAML Tokens.

6. COMPARATIVE ANALYSIS OF COMMERCIALLY AVAILABLE IAM SOLUTIONS

VENDOR	PRODUCT	Standards and techniques used for SECURITY	Standards and Techniques used for INTEROPERABILITY
VMWare	Horizon	*Provides additional user authentication support by employing Open Authentication (Oauth *Provides mechanism for implementing policy enforcement *SAML is used for user authentication	* Supports SAML * Provides limited support for other cloud computing softwareproducts.
OpenStack	Keystone	*Keystone employs security by using a secure token exchange that includes public and private keys.	* Supports SAML *Provides an open source option for organizations that chose to add to the existing IAM product or develop an independent IAM Solution.
Amazon	Elastic Compute Cloud (EC2)	*Organizations that choose to build their Own PAAS must have security aware software developers. *Addresses security with its multiple user authentication methods for security: AWS access key, public private keys, and multifactor authentication	*Supports SAML *Limited transparency, thus limiting trust between organizations
Microsoft	Windows Card Space	*Windows CardSpace employs security by using a sercure token exchange . *High assurance certificate X.509 is used for authentication	*Supports SAML *Limited Transparency, but supports trust between organization by implementing ZKP
	Perfcloud	* Provides a mechanism for implementing policy enforcement *Key is protected with Encryption *High assurance certificate is used	*Use POIS(Policy and OCSP based interoperability system) *It provides Role Mapping among various clouds

Table2 Comparative analysis of different commercially available IAM solutions

7. CONCLUSION AND FUTURE WORK

One of the main security issues in cloud computing is identity federation. There are many cloud solutions available but they lack identity management. In this survey we have gone through some open standards, techniques and solutions. Among open standards SAML is very powerful tool in federated identity. SAML can establish trust relationship between entities with different security mechanisms. SAML is different from other security systems due to its approach of expressing assertions about a subject that other applications within a network can trust. There are many commercially available Identity management solutions we have discussed here which mainly based on SAML as it provides Single Sign-On facility. Although we have discussed many solutions here which resolved interoperable identity problem but they still lack security at some level as user credentials are revealed at access time which is a serious threat, to avoid this we need some approach through which user can interoperate between clouds and internal autonomy is maintained. To implement this there is a solution which is still under development it is Identity As A Service layer which need to be embed in cloud structure so that user credentials during access are not revealed.

REFERENCES

[1] Peter Mell and Tim Grance, "The nist definition of cloud computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/cloud-def-v15.doc, 2009.

[2] Tivoli Federated Identity Manager, IBM, http://www01.ibm.com/software/tivoli/products/federated-identity-mgr/

[3] "Security Assertion Markup Language (SAML) V2.0 Technical Overview", OASIS, http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-techoverview-2.0-cd-02.html, Mar. 2008

[4] "WS-Security Profile of the OASIS Security Assertion Markup Language (SAML)", OASIS, https://www.oasisopen.org/committees/security/docs/draftsstc-ws-sec-profile-04.pdf, Sep. 2002.

[5] "eXtensible Access Control Markup Language (XACML)", OASIS, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf,Feb. 2005.

[6] Service Provisioning Markup Language (SPML) Version 1.0, OASIS, https://www.oasisopen.org/committees/download.php/4137/os-pstc-spml-core-1.0.pdf, Oct. 2003.

[7] Michelle carter,"Secure Identity In Cloud" https://gsaw.org/wpcontent/uploads/2013/06/2013s11b_carter.pdf,Mar.2013

[8] ArdiBenusi, "An Identity Management Survey On Cloud Computing" http://dx.doi.org/10.12988/ijco.2014.458

[9] Bharat Bhargava, Noopur Singh and Asher Sinclair, "Privacy in Cloud" https://www.cs.purdue.edu/homes/bb/PrivacyinCloud.pdf