TRUST BASED IDENTITY FEDERATION IN CLOUD

Aradhana
Assistant Professor
Post Graduate Department of Computer Science and Applications
Guru Gobind Singh College for Women, Sector 26, Chandigarh, India

Abstract: In a federated environment like Cloud Computing security remains major concern for cloud users as their sensitive data is handled by a third party. Identity management plays major role in Cloud security. This paper aims to provide means of understanding new dimensions of identity management in cloud security and necessity of building dynamic trust relationships for efficient federated identity management.

IndexTerms - **Cloud Computing, Identity Management, Trust**.

I. INTRODUCTION

Cloud computing is a distributed computation model over a large pool of shared and virtualized computing resources, such as storage, processing power, applications and services. It provides a number of benefits, including reduced IT costs, flexibility, increased collaboration, etc. [1]. It gets its name as a metaphor for internet. In this pool of resources are made available to the users through internet and they are billed accordingly just like electricity and they need not to worry about installations and maintenance issues. Cloud Computing comes in various flavors in which 'X' is offered as a service. The term services in cloud computing is the concept of being able to use reusable, fine grained components across a vendor's network. Depending on the type of resources provided by the Cloud, distinct layers can be defined (see Fig.1). The bottom-most layer provides basic infrastructure components such as CPUs, memory, and storage, and is henceforth often denoted as Infrastructure-as a- Service (IaaS). Amazon's Elastic Compute Cloud (EC2) is a prominent example for an IaaS offer. On top of IaaS, more platform-oriented services allow the usage of hosting environments tailored to a specific need. Google App Engine is an example for a Web platform as a service (PaaS) which enables to deploy and dynamically scalable Python and Java based Web applications. Finally, the top-most layer provides it users with ready to use applications also known as Software- as-a-Service (SaaS) [2].

Three types of cloud can be there-*Private cloud* that is hosted maintained and privately by the organisation and more customized, *Public cloud* that is managed by third party and access is by subscription and *Hybrid cloud* is mixture of private and public cloud and meets benefits of both.

Cloud Computing offers various benefits like multi tenancy, scalability, high abstraction etc but despite these benefits its adoption is being hindered due to security issues. Users' fear of leakage of commercially sensitive data and loss of data privacy may be justified. For example in 2016 users' sensitive data and identity credentials held by Verizon was stolen by cybercriminals.

Identity management assumes an upper hand in cloud security. Cloud scenarios require just in time provisioning (i.e. timely boarding and off-boarding of users) which indicates federation of identities without sharing prior data, based on some trust model. On internet it is likely that a user ends up with multiple accounts with different access permissions on different service providers. These fragmented logins present challenge to users and service providers in terms of synchronization of shared identities etc. Currently it is based on policy files framed by the local authority, depending on various factors like the domain trust information automatically fed in by the trust authorities. There is a strong need of trust relation setup between service providers of the federated world [3].

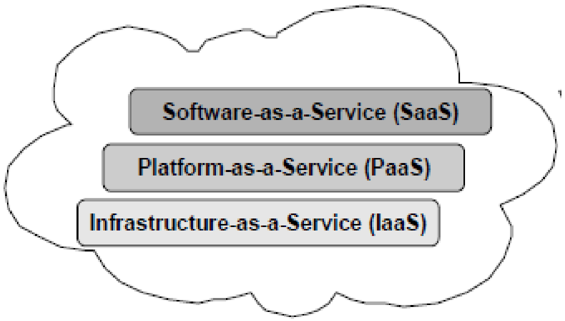
Software-as-a-Service (SaaS)
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service (IaaS)

Figure 1 Cloud Layers [2]

II. NOTION OF TRUST

Trust is a key concept for providing seamless interaction between different trust domains and improved user experience. Fig. 2 shows conceptual view of trust.

2.1 Definition of Trust

Trust is a directional relationship between two parties that can be called trustor and trustee. One must assume the trustor to be a "thinking entity" in some form, meaning that it has the ability to make assessments and decisions based on received information and past experience. The trustee can be anything from a person, organisation or physical entity, to abstract notions such as information or cryptographic key [4]. Here we consider 'principal' as entity which can be a Service Provider (SP), Identity Provider (IP) or any user.

2.2 Types of trust

Trust can be either static or dynamic [5]:

- *Static trust*- This is simple trust based on agreements signed between two principals.
- *Dynamic trust*- Dynamic trust is calculated by principal's own experience or peers' experience with the trustee.

2.3 Facets of trust

There are different faces of trust that can be considered while taking decision [6].

- *Simple trust*- Simple trust can be built between two principals who have direct trust agreements with each other.
- *Trust from past experience*- Interaction between two principals can be audited for future decision before next interaction.
- *Trust by reputation*- Information about a principal can be gained through feedback about it from the peers.
- *Trust by belief*- When the principal is totally unknown and has no earlier interaction with the peers.

III. IDENTITY FEDERATION FRAMEWORKS : STATE-OF-THE-ART

Identity federation can be achieved by means of various technologies. One of them is Security Assertion Markup Language (SAML) [7] an XML-based specification for exchanging security information. SAML defines a trust mechanism for Single Sign On in which interaction takes place only if there is predefined existing relationship between the relying party and asserting party. The trust mechanism in SAML is based on Public Key Infrastructure.

OpenID [8] is another way to achieve identity federation. It is centric around user, open and decentralized framework. It makes single sign on very easy to be achieved as user can have multiple logins and there is no requirement of predefined trust. It is mainly authentication protocol mainly achieved through attribute exchange.

Liberty bases Identity Federation on the concept of "Circle of Trust" (CoT), which means entities must establish business and trust agreements in order to enable future interactions. Thus, CoTs defined by LA specify different kinds of trust relationships that can exist between two entities depending on the context. If the context is authentication; we can have direct or indirect trust relationships. On the other hand, a business relationship can be: *pairwise*, when directly links the two entities; *brokered*, when an intermediary (*"broker"*) is required; or *community*, when no relationship of any kind exists. So Liberty entities have a TAL or Trust Anchor List with the trustworthy entities for authentication purposes, and also have a BAL or Business Agreement List, containing those parties which are related to the entity via a business agreement [9].

In WS-Federation [10], an administrator or other trusted authority may designate that all tokens of a certain type are trusted (e.g. all X.509 tokens from a specific CA).The security token service maintains this as a trust axiom and can communicate this to trust engines to make their own trust decisions.

Table1 shows above mentioned technologies implement static trust models where as cloud scenarios require trust models for dynamic environment also none of them cosider what will happen if the principal is totally unknown.

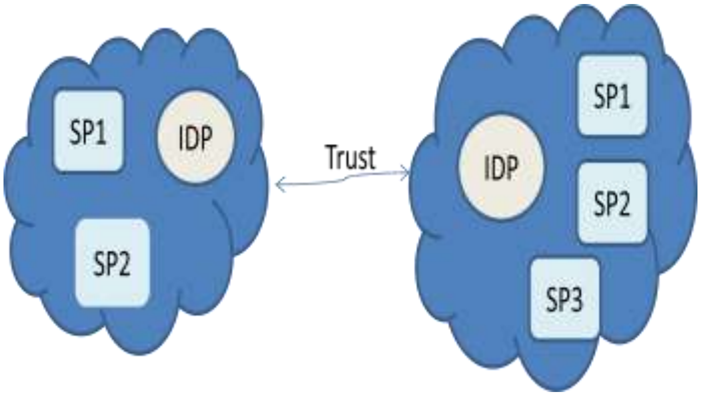

Figure 2 Conceptual view of trust

Table1 Comparison of Current Identity Frameworks

Identity Framework	**Domain**	**Open Source**	**Advantages**	**Limitaions**	**Provider/Project**	**Common Limitaion**
SAML	Exchanging authentication and authorization. Supports Single Sign On	Yes	Based on open industry standards, it is simple and ensures integrity and privacy.	Uses trust model which is hard to deploy and maintain.	SugarCRM, Knowledge Tree	None of them include efficient trust models for Dynamic Trust establishment
OpenID	Single Sign On	Yes	Open, flexible and free framework.	Too much flexible anddoes not have any trust model and uses symmetric insecure encyption.	VeriSign, Orange, Live Journal	
Liberty Alliance Initiative	Authentication and Single Sign On	Yes	Supports SSO and has strong authentication capability.	Trust lists are maintained manually.	Openliberty.org, Concordia	
WS-Federation	Single Sign On, Single logout, interoperability and secures protected resources	Yes	Based on established standards and is extensible.	Complex and has constraints in deployment.	OpenSSO Enterprise	

IV. DYNAMIC TRUST ESTABLISHMENT

For seamless interaction between two different trust domains dynamic trust establishment is required. This increases user experience and reduces complexity for both user and service provider while maintaining privacy. Trust can be established dynamically by using SAML extenstions or through the use of XACML policies.

4.1 SAM extension for Dynamic federation

SAML is the most flexible standard to add extensions in order to achieve dynamic federation in a generic way. In addition, SAML is the mostly deployed federation solution and has been adopted by many well known providers (e.g. Google Apps). It defines an XML based framework to allow the exchange of security assertions between entities.

Furthermore, while all the solutions are mainly concerned with web scenarios and the SSO use case, SAML offers abstraction enough to be applied to a wider range of situations. So by including modifications in the abstract level we can assure its later application in more specific use cases. Also, SAML is the only standard nowadays and LA is based in its specifications, so it was more logical to introduce modifications in SAML that could be later adopted by other technologies based on it. Enhancement to SAML could fulfill trust establishment requirements such as minimizing dependence on central servers, modeling trust evolution over time and allowing seamless interaction between the main actors involved in identity management scenarios.

A new component the Trust Engine is added which will be in charge of processing every trust-related data to decide if an entity is trustworthy or not. The trust information can be obtained from external or internal source. The Trust Engine will allow entities to maintain a dynamic store instead of a static list with trust data, that we call Dynamic Trust List or DTL [8].

4.2 *Through the use of XACML policies*

eXtensible Access Control Markup Language (XACML) policies can be used for controlling the flow of user's personal information. In this an algorithm is designed which computes trust values according to past experiences i.e. if there is any direct or indirect relationship between the two parties. These computed values are stored within trust relationship sub objects. The computed trust level values serve as parameters for ARP's threshold to determine whether the user data should be released or not. Fig. 3 how trust can be calculated using this algorithm.

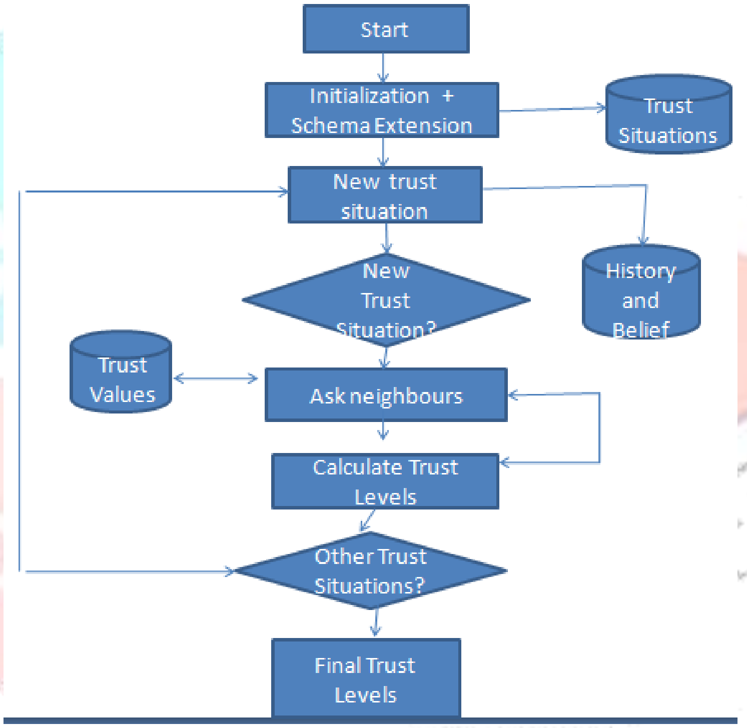

Figure 3 Trust Flowchart

The principals are represented as nodes into a trust graph, where the weight of the connections between the nodes is estimated according to an algorithm that is based on a collection of attributes. These attribute are created, along with the identity of the principal, during a process of the interaction, as they tend to identify the other party as well as the level of trust in order to estimate carefully how it is likely to behave in a given situation [11]. Table 2 shows comparision of the above techniques and their limitation.

V. CONCLUSION

Cloud Computing has emerged as successful utility based paradigm. It provides a flexible way of meeting resource sharing needs in a cost effective manner and is extensively used in distributed environment with other technologies but security issues in cloud identity management require special attention because customers are not sure how there data will be handled by third party.Trust manageemnt can play an important role giving confidence to the user to move to the cloud with minimalistic privacy and security concerns. In this paper we have analysed different facets of trust, current frameworks for identity federation and need of trust in dynamic environment.

The most obvious finding from this study is that, to meet the demands of cloud and for smooth interaction between different trust domains dynamic trust model is required.

VI. SCOPE

The benefits of Cloud Computing can be leveraged to its stakeholders by developing dynamic trust models by taking into account many other factors such as gathering feedback about the service provider, sharing statistics of affected users and evaluating trust worthiness of the actors of the Cloud Scenarios.

Table 2: Comparison of current dynamic trust establishment approaches

Dynamic Trust Establishment Approach	**Main objective**	**Common Limitations**
Service specific XACML policies	to maintain a repository where trust relationships are stored and accessed to find path between principals	• They do not know what trust value should be assigned to a completely unknown entity. • Dimensions of trust, such as risk management, are not considered in the presented approaches.
SAML extension for Dynamic Federation	permits to take richer decisions based on different trust dimensions	

REFERENCES

[1]Qin, Z., Sun, J., Wahaballa, A., W, Zheng., H, Xiong and Z, Qin.2017. A Secure and Privacy-Preserving Mobile Wallet with Outsourced Verification in Cloud Computing.Computer Standard and Interfaces, 57(1):55-60.

[2]Jensen, M., Schwenk, J., O, Gruschka, N. and Iacono, L. L. 2009. On Technical Security Issues in Cloud Computing. In *IEEE International Conference on Cloud Computing (CLOUD-II 2009)*, Bangalore, India, September 2009, 109-116.

[3] Gopalakrishnan, A. Cloud Computing Identity Management. SET Labs Briefings, vol. 7. Online at: http://www.infosys.com/research

[4] Josang, A. The right type of trust for distributed systems.1996. In C. Meadows, editor, *Proc. of the 1996 New Security Paradigms Workshop*. ACM.

[5] Boursas, L. and Danciu, V. 2008.Dynamic inter-organizational cooperation setup in circle-of-trust environments". In the Proceedings of the 20th IEEE/IFIP Network Operations and Management Symposium NOMS08, Salvadore, Brazil.

[6] Boursas, L. Trust-Based Access Control in Federated Environments. 2009. PhD thesis, Technische Universit¨at M¨unchen, Munich, Germany.

[7] Eghbal, G., A.M. Jamalul-Lail, Z. Mazdak and P.Abolghasem. 2012. A survey on security issues of federated identity in the cloud computing. Proceedings of the IEEE 4th International Conference on Cloud Computing Technology and Science.

[8] Security Assertion Markup Language (SAML) V2.0, Oasis, 2007; http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0- os.pdf. 2014.

[9] Victoria, S., Hogan and Hartson. 2005. Liberty Alliance Contractual Framework Outline for Circles of Trust Liberty Alliance Specification.

[10] Lockhart, H. Web Services Federation Language (WS-Federation).2006. version 1.1.

[11] Boursas , L. and Reiser, H. Propagating Trust and Privacy Aspects in Federated Identity Management Scenarios.2007. In *Proceedings of the 14th Annual Workshop of HP Software University Association*, Leibniz Supercomputing Centre, Munich, Germany.