ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Access Control in Cloud Using XML File

[I]Archana Salaria, [II]Harshpreet Singh Ahluwalia
[I,II]Lovely Professional University, Jalandhar

Abstract
Cloud computing is a new technology that provides the on request services and extremely scalable resources at reasonably priced rate. Identity management also plays a vital role in cloud security and privacy. Proper identity management is the first step toward accessing the services from cloud. Access control also plays an important role in identity management. Access control is mainly limitation of access to a resource. In this paper, we proposed a plan to speed and secure the access of user by using XML file.

Keywords
Cloud computing, identity management, Access control

I. Introduction

Cloud computing is a novel paradigm that has been devised to resolve IT management concerns and supply commercial necessities. The make use of hardware and software to deliver a network is called cloud computing. By using cloud, User can use applications and access the files from any device but that device has the right to use of the internet. In cloud, data is stored on many physical and virtual servers whereas in traditional computing data is stored on the Pc's, local hard drives. Cloud caters the on Demand services and extremely scalable resources at inexpensive rate.

1. Cloud Categories

There are mainly three categories of cloud.

Public cloud

A public cloud is comprised of resources such as storage, files, applications, and services that are provisioned for public use via the internet. Public cloud service provider is owned, operated and managed the public cloud.

Private cloud

A private cloud consists of storage, files, applications, and services that are dedicated for specific organizations. The cloud provider or companies themselves built the private cloud.

Hybrid cloud

The hybrid cloud typical mix of public and private clouds.

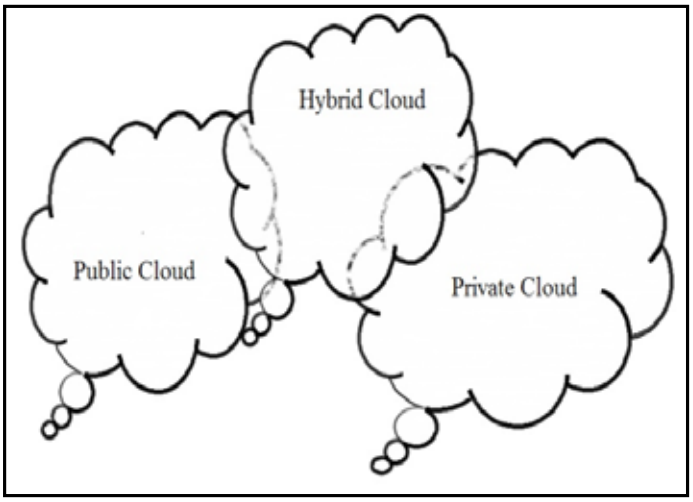

Fig.1 : Types of cloud

2. Cloud Computing Characteristics

Availability

There are multiple copies of data, physical resources are present on cloud platform. If any physical resource is going out of order then without the knowledge of user, the application moves on other physical resource.

On demand Service

Whenever a consumer wants to use the cloud services at any time and from any place, he/she automatically acquire computing resources such as storage, or software use, CPU without human interactions.

Rapid Elasticity

The nature of computing resources is dynamic and elastic. The user may scale up to use the resources according to the need and scaled down to release whenever finished.

Pay as you go

Cloud services are just like electricity or water, pay per usage metrics. The more utilization of resources, higher the bill.

Broad Network Access

Computing resources are access by various platforms such as laptops, tablets and mobile phones that are available on the network.

Multitenant

Multitenant is mainly a software architecture that refers to the distribution of same software or application or database instance to many different users for decreasing the cost.

3. Identity Management

Identity management (IDM) describes the management of individual principals, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost , downtime and repetitive tasks.[1] There is mainly four A's in identity management: Authentication, Authorization, Audit Logging, Account Management that give the full description of identity management what is it.

Authentication

Authentication is the act of verify Who is the user . Whether the user has unique identity (such as username or password) or not.

Authorization
Authorization tells us what user is allowed to do. It is the act of giving rights to resources to do or have something.

Audit Logging
Audit logging is to record of where the user has been.

Account Management
Account management refers that what can the user access.

4. Parties Use IDM

Service Provider
Access of services provided by service provider to the identities that have the right essential identities. It is mainly third party that maintains and controls about or on behalf of consumer.

Identity provider
Digital identities provided by the Identity provider. For example PAN card or SSN to citizens by Government.

Identity verifier
Identity verifier verifying the requests claims about an identity that is sending by the service providers.

Entity
Entities are the ones that survive by it or about who claims are made.

II. Literature Survey
Sanchez Guerrero, et.al, [2012]: A new generation of technology i.e. Cloud computing, in several area, it includes distributed computing, service oriented architecture and uses services. In the complex ecosystem, there is arisen of security and identity management challenges. In cloud computing, user in one cloud can access the application of another cloud. So there is a need of trust relationship between the different cloud domains. Thus due to rapid changing relationship, it is necessary to propagate trust for manage privacy and access control. This paper presents the trust aware Identity management architecture based on privacy & reputation extension with SAMLv2 standard media. In this paper they have, developed their own IDM infrastructure by using C library called Lasso. These libraries use Apache2 and OpenSSL. Apache2 as a web server and OpenSSL as underlying cryptography library [2].

Fu, Zombo, et al, [2010]: In cloud computing, resources are shared by many Organizations. Applications need authenticates many consumers of different organizations. For privacy preservation, Application independent identity management presents. This paper gives the introduction of some preliminary concepts and definitions related to digital identity in federation. This paper proposes new IDM model which provides a better way of preserving privacy than the current paradigm and adopts complicated and uncertainly trust relationship. This Model has some advantages in security and usability. This model provides flexible access control as well as powerful privacy preservation that decreases the risk of leakage of identity information especially when cross domain transaction is executed or implemented [3].

Ranchal, Rohit, et al, [2010]: A cloud computing service allows the users to use the internet based services by paying rental to IT-services according to usage. It recommends the absorption of resources but also cause risks for data privacy. The heterogeneity of "consumers" represents a danger of many, collaborative threats. But as new technology cloud computing grows, the entities have several account associated with different SP's or one SP there is sharing of personally identifiable information (PII) of the same entity across services along with associated attributes. Identity management is solution to cloud privacy and security. In identifying the entities to service providers, existing solutions use Trusted Third Party. Their solutions on untrusted hosts are not useful. This paper mainly proposes an approach for Identity Management which is independent from Trusted Third party. This approach has the capability to use the identity data on untrusted host. Active bundle plays an important role in this approach. Active bundle act as the Middleware that include PII, Privacy policies, a set of protection mechanism to protect itself and a virtual machine that implement the policies. In this approach Active bundle interacts to cloud computing to authenticate on behalf of users using user's policies. Without disclosing unencrypted data, this approach has facility to authenticate [4].

Celesti, Antonio, et al, [2010]: In IT world Cloud Computing is a new paradigm. Along the cloud computing, several challenges are being lifted including security, privacy and federation. This paper presents the new concept of cloud computing and security .This paper aims to focuses on heterogeneous and federated scenarios of cloud computing scenarios. This paper firstly presents the IDM using IDP/SP model that using a global approach to solve the SSO authentication problem and integrating many technology. This model includes four
logical components that are End user, User Agent, Service provider and Identity provider. After giving the overview of IDM/SP model, this paper presents Inter cloud IDM infrastructure which is solution of Intercloud IDM and implements by using SAML.[5]

C Guo, et al, [2008]: With the integration of Identity management in Enterprise resource planning system, the ERP system becomes significant and complicated. This paper firstly proposes the main problems that exist in traditional ERP system of identity management such as 1) Traditional identity management system is time consuming and costly. 2) The time consuming and costly identity management of ERP system require cursory protection. After proposing the main problems, this paper overviews the benefits of applying federated identity management to ERP system.[6]

III. Proposed Work
In Cloud Identity management there is mainly sharing of data. So there is more need to secure the data and access control. Here our main anxiety is to improve the speed of access and secure the data of users.

For that user's credentials and their rights save on XML file instead of using Third party.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

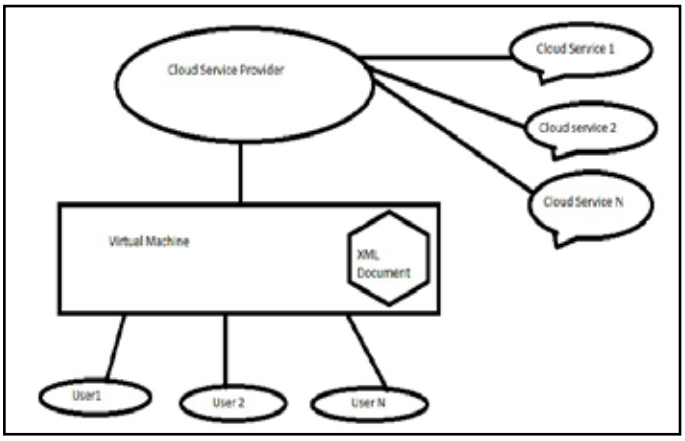

Fig. 2: Cloud Access control using XML

XML coding for configuring and mapping a servlet code in the xml file:

```
<web-app>
<servlet>
  <servlet-name>add</servlet-name>
  <servlet-class>com.controller.add</servlet-class>
  </servlet>
<servlet>
  <servlet-name>delete</servlet-name>
 <servlet-class>com.controller.delete</servlet-class>
  </servlet>
<servlet-mapping>
  <servlet-name>delete</servlet-name>
  <url-pattern>/delete</url-pattern>
  </servlet-mapping>
<servlet-mapping>
  <servlet-name>add</servlet-name>
  <url-pattern>/add</url-pattern>
  </servlet-mapping>
  </web-app>
```

In this, firstly there is configuring of servlet by using <servlet> element. Here provide the servlet name and write the servlet class name.
Secondly, mapping of the servlet to URL pattern in the <servlet-mapping> element.

IV. Conclusion And Future Scope

As cloud identity management has main task manage the identities of the users and access control. Consequently there is need of proper security and speed so that user can access their data. So the proposed plan helps to speed the access of users. It also helps in secure the access of the users. But there are some constraints of XML file. It has hacked.
So in future there is need to develop a more secure XML file.

References

[1] *http://en.wikipedia.org/wiki/Identity_management*
[2] *Sanchez Guerrero, R., P. Arias Cabarcos, F. Almenares Mendoza, and Daniel Diaz-Sanchez. "Trust-aware federated IDM in consumer cloud computing." In Consumer Electronics (ICCE), 2012 IEEE International Conference on, pp. 53-54. IEEE, 2012.*
[3] *Fu, Zombo, Jianxin Wang, Lin Yang, and Yuan Cao. "Application independent identity management." In 2010 IEEE International Conference on Information Theory and Information Security, pp. 625-628. 2010.*
[4] *Ranchal, Rohit, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, Anya Kim, Myong Kang, and Mark Linderman. "Protection of identity information in cloud computing without trusted third party." In Reliable Distributed Systems, 2010 29th IEEE Symposium on, pp. 368-372. IEEE, 2010.*
[5] *Celesti, Antonio, Francesco Tusa, Massimo Villari, and Antonio Puliafito. "Security and cloud computing: Intercloud identity management infrastructure." In Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on, pp. 263-265. IEEE, 2010.*
[6] *Guo, Chunfang, and Ying Wang. "Application of federated identity management in ERP system." In Service Operations and Logistics, and Informatics, 2008. IEEE/SOLI 2008. IEEE International Conference on, vol. 2, pp. 1971-1974. IEEE, 2008.*