Study of Authentication and Authorization in Cloud Computing

Dr. Nilesh Mahajan
Research Guide
Prof. BharatiVidyapeeth University
IMED Pune

Mrs. Devyani Patil
Research Student
Asst. Prof. Arihant College Camp, Pune

Abstract **–**Cloud Computing is aconvenient model for on-demand network. Cloud Computing (CC) refers to applications & services which we can run on a distributed network. This Network use hosted services and virtualized resources delivered over the internet. Cloud computing is characterized into two main categories**(a) Virtualization**– As the network has no limit resources are virtual and limitless.**(b)Abstraction**–All details of physical systems which run the software are abstracted from users.There are three categories of Cloud Computing: (a) Infrastructure-as-a-Service (IaaS), (b) Platform-as-a-Service (PaaS) and (c) Software-as-a-Service (SaaS). The data we are storing on CC must be safe and secure then only users will trust on this environment. Access Controls for file and directory, Flex list Models, SLAs etc are some of the facilities available for this. But still there are some drawbacks in security. When users access data from CC, Authorization and Authentication are very important. We call this as first stage of Security. This paper focuses on Authentications and Authorizations in CC.

Keywords *– Cloud Computing (CC), Authentication, Authorization, Security Levels*

*****

Introduction –

Authentication is the process of to establish confidence in users identities. Authentication assurance levels should be appropriate and accurate for the sensitivity of the any application, information assets accessed and the risk involved.[1][3] All growing cloud providers support the SAML standard and use it to administer users and authenticate them before providing access of their data. Security Assertion Markup Language(SAML) is open standard data format used to distinguish between identity providers and service providers to exchange authentication and authorization.Any network access should is made secure by strong authentication.[3][7] In IT resources beingadministered via strong authentication for example viaUSB sticks on resources,a hardware-based authentication system using chip cards, via one-time passwords. For this user obtains a certificate which proving his identity signed by the Certification Authority (CA).[2]Cloud service providers help users easily to access their personal information which is available to various servicesacross the Internet. An identity management(IDM) mechanism is useful for authenticating users and services basedon their credentials andprofile.

Access Control in CC –

Access control is a very important security technique that can be used to regulate who can view and use resources in computing environment. Access control plays an important defense for data privacy in PASS category of CC. For strong access control PASS chooses a mandatory access control model which grants access grant delegation.[5] Whenever such type of access control want to implement in CC a good security labeling is very important. This security label consist of two parts 1) Security Level 2) Categories. These categories are applicable for either data items or subjects. When access control is assigned for data items the security level indicates the data security sensitivity and categories describes kinds of information of the data. When access control is assigned for subjects security level indicate subject's security clearance and the set of categories describes what kinds of data the subject has right to access. The United State's Department of Defense defined four security levels for their application: top secret, secret,confidential and unclassified.[4][10]

The trusted third party can be tried upon forsecurity :

1) Low and High **level confidentiality -**

Server and Client Authentication- A Certification authority is required to certify entities involved in interactions in cloud environment. It include certifying environment users, physical infrastructure servers, virtual servers, and networks devices. Digital signatures in combination with SSO and Ldap, implement the strongest available authentication process in distributed environments guaranteeing user mobility and flexibility.[6]

2) Creation of **Security Domains-**

For creation of security domains federation is a group of legal entities it share a set of agreed policies and rules to access online resources. It provides a structure and a legal framework which help to enable authentication and authorization across different organizations. This cloud environment is called as "Federated clouds". Federated Cloud is collection of single Cloudwhich can interoperate means exchange of data and computing resources through defined interfaces.[9]There is one basic principle for federation i.e. in Federation of Clouds each single Cloud environment remains independent and can interoperate with another Clouds in the federation.

3)Cryptographic Separation of Data-

Cryptographic Separation in which data is appear intangible to another unauthorized person. In which Confidentiality and integrity also privacy of data can be protected through encryption. By using the combination of asymmetric and symmetric cryptography we can offer the efficiency of symmetric cryptography while maintain the security of asymmetric cryptography.[10]

4)Certificate-Based **Authorization –**

Relation between resources and users is more ad hoc and dynamic in cloud environment. Users in this cloud environment are usually identified by their characteristics or attributes rather than predefined identities. For this purpose traditional identity-based access control models are not effective.In this case Certificates issued by a PKI facility can be used for enforcing access control in the Web environment, e.g. use of an extended X.509 certificate that carries role information about a user.[8] Such type of certificates are issued by a certification authority that acts as a trust center in the global Web environment.These certificates contain an attribute value pair and the principal to whom it applies. Attribute based access control, decide access priority which is based on the attributes of environment, requestors and resource. It provides the flexibility and scalability which is essential to large-scale distributed systems such as the cloud.

5) User Based Authentication :

In this common form of authentication user use his login id and password that one stored in system repository are validated under credentials.

6) Smart Card based authentications :

It is a second factor authentication which store cryptographic data.

7) Biometrics :

It is a strongest third party authentication. In this user have to providesomething as input like username, token, retina scan or thumbprint. It is useful only when data is top confidential e.g. Military or Defence.[11]

8) Grid Based Authentication :

It is a second factor authentication which is provided by entrust identity guard.

9) Knowledge Based Authentication :

This facility provides additional confidence in user's identity to challenge attacker that is unbreakable. In this providers can ask to user about appropriate information to confirm information about user that already known through registration process like cross verification.[12]

10) Machine Authentication :

In this effective method in which users can typically access their account from regular machines allowing for stronger authentication to be performed without any impact on users experience.[7]

11) One Time Password : (OTP)

It is a dynamically generated password which is valid for once only so if hacker hack this password he can't use it.OTP has two types :1) Synchronous – in which token device is synchronizes with authentication services by using time as core piece of authentication process. 02) Asynchronous - In asynchronous token device used as challenge response scheme to authenticate user. [13]

12) Global Authorization :

Asnamesuggested all security rules and policies defined in this method are globally declared. This method is classified into local and global authentication. E.g. Global – Organizational Membership, Local-Banned Users.

Research Work :

A lot of research work is going on in this term of Authentication and Authorization especially for cloud computing. In this Context aware platform stores each user's personal information profile provides suitable services to user so that this environment is user friendly for users. This context aware model authenticate user with its access priority and user can use cloud computing services. Some work related this I am mentioning her like, Esou Wu, Lizhao Liu, Jian Liu and others proposed a grid distributed parallel authentication model based on trusted computing. By using multiple techniques like SSL,TLS protocols, stream cipher heuristic code generator models of authentication and authorization are designed. In biometric some other facilities are again added by many researchers like three tier architecture. Other than this multiple frameworks are designed by multiple researchers in this field.

Conclusion :

For the large distributed system like cloud Authentication and Authorization is a very important term. This term is helpful for all security issues for both to user as well as cloud providers which solve multiple issues. Research regarding this security issues is still in progress which will find new methods in this issue. So this paper will give you many ideas about different methods and frameworks designed by many researchers.

References :

[1] Abdelmajid Hassan Mansour Emam,"Additional Authentication and Authorization using Registered Email-ID for Cloud Computing" (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013

[2] S.S. Wang#1, M.L. Chiang#2*, K.Q. Yan#3*, S.C. Wang#4*, S.H. Tsai#5"The New Territory of Group Key Authentication in an Insecure Cloud Computing Environment",International Journal of Advanced Information Technologies (IJAIT), Vol. 5, No. 2

[3] Jyh-haw Yeh,Dept. of Computer Science, Boise State University Boise, Idaho 83725, "A PASS Scheme in Cloud Computing – Protecting Data Privacy by Authentication and Secret Sharing",USA

[4] PrachiSoni, (Asst. Prof.) MonaliSahoo, Computer Science & Engineering Takshshila Institute of Engg& Tech., Jabalpur (M.P.) ,"Multi-factor Authentication Security Framework in Cloud Computing"R.G.T.U Bhopal (M.P.) India, Volume 5, Issue 1, January 2015

[5] Ariel Stolerman Drexel University,Philadelphia, PA stolerman@cs.drexel.edu, Alex Fridman Drexel University Philadelphia, PAaf59@cs.drexel.edu, RachelGreenstadt Drexel University Philadelphia, PA greenie@cs.drexel.edu, Patrick Brennan Juola& Associates Pittsburgh, PApbrennan@juolaassoc.com
Patrick JuolaJuola& Associates Pittsburgh, PApjuola@juolaassoc.com,"Active Linguistic

[6] Authentication Revisited: Real-Time Stylometric Evaluation towards Multi-Modal Decision Fusion"
Jaejung Kim* and Seng-phil Hong, " A Consolidated Authentication Model in Cloud Computing Environments"International Journal of Multimedia and Ubiquitous Engineering Vol. 7, No. 3, July, 2012

[7] Man-Jae Kim, HoonJeong, Eui-In Choi, Department of Computer Engineering, Hannam University, Daejeon, Republic of Korea{mjkim, hjeong,

eichoi}@dblab.hannam.ac.kr,“Knowledge Base Configuration for User Authentication in Cloud Computing”

[8] Xiaohui Li1,3, Jingsha He1,2 and Ting Zhang1 “A Service-oriented Identity Authentication Privacy Protection Method in Cloud Computing”, International Journal of Grid and Distributed Computing Vol. 6, No. 1, February, 2013

[9] S.S. Wang#1, M.L. Chiang#2*, K.Q. Yan#3*, S.C. Wang#4*, S.H. Tsai ,“The New Territory of Group Key Authentication in an Insecure Cloud Computing Environment” International Journal of Advanced Information Technologies (IJAIT), Vol. 5, No. 2

[10] S.Ziyad1 and S.Rehman2Department of Information System Salman bin Abdul Aziz University, KSA,
“Critical Review of Authentication Mechanisms in Cloud Computing” IJCSI International Journal of
Computer Science Issues, Vol. 11, Issue 3, No 1, May 2014 ISSN (Print): 1694-0814 | ISSN (Online):
1694-0784 www.IJCSI.org 145

[11] http://www.engpaper.net/authentication-in-cloud-computing.htm

[12] http://blog.gogrid.com/2013/04/19/cloud-is-key-to-unlocking-security-opportunities/

[13] http://www.net-security.org/secworld.php?id=9442