Data Security Using Authentication And Authorization In Cloud Computing

P.Joseph Charles[1], D. Roselin Jaya Priya[2]
[1]Assistant Professor, Dept of IT
[2]Dept of IT
[1, 2] St.Joseph's College, Trichy

Abstract- *Cloud computing is one of the general purpose technology. It is mainly used for distributed the data centres, resources and services that are pro-vided by the network or online. In cloud computing, compatibility means ability of computer system to run application program from different seller and to interact with other computers. That is bringing with many challenges of security and privacy. Most of the data store in cloud. Because it is safe and secure then only users will trust on their environment. Now days cloud computing is mainly used in both industrial field and academic field. As the field of cloud computing is growing the new techniques are developing. Security is the big problem for cloud computing clients especially access control. Such as massive traffic handling, service ability, security issues technology, application security. This paper briefly describes the cloud based secure and privacy enhanced authentication and authorization for cloud computing and security.*

I. INTRODUCTION

Cloud computing is a main extremely paced distributed technology has been developed very quickly in recent years.[1] The huge spread of internet resources on the web and fast growth of services providers enabled cloud computing system to become a large scaled IT services model for distributed network environment. Cloud computing is built on top of already existing internet technologies and is delivered as a self-services utility.

Data storage in a cloud computing is one of the most important concerns from a security point of view. Because multiple cloud customers from the same a similar organization can use the same resources or applications. Certain security risks should be evaluated and solved before private and sensitive data, application and system functionality are moved into the cloud.

Cloud service providers help users easily to access their personal information which is offered to various services across the internet. Authentication is the process to establish confidence in user's identities .Authentication assurance levels should be appropriate and accurate for the sensitivity of the any application, information resources accessed and the safety involved.

II. LITERATURE OF OVERVIEW

User Authentication and Authorization

Cloud computing provide the reliable data to the customers with high scalable and computing resources. Cloud computing have three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructural as a Service (IaaS), each service models intention a specific need of customers.[2]

- Software as a Service offer application that were provide by the cloud service providers and hosted by the cloud supplier.
- Platform as a Service offers hosting environment for developers to develop and publish their applications.
- Infrastructural as a Service offers visualised computing resources such as virtual desktop, virtual storage, etc.

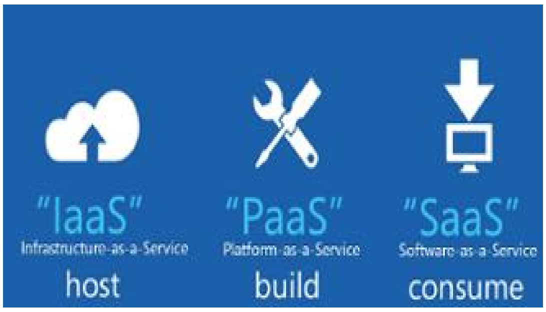

Figure 2.1 cloud service model

Various cloud services and cloud service providers are helpful for customers who seek specific computing resource; it creates some security challenges to the customers in search of different cloud services on the other hand.

As users communicate with the Cloud, identity becomes an important issue to maintain security, visibility and control. In this distributed environment, it is essential for applications to authenticate the user's identity, understand what that user is authorized to do, create or update an account and check their activities. Thus Authentication and authorization are essential components provide portability and extensibility outside activity limits.

Authentication Authentication is the process for confirming the identity of the user. Typically by having the user enter a valid username and valid password before accessing is granted. The process of authentication based on each user having a unique set of testing for gaining access. The AAA(Authentication, Authorization and accounting) server compare a users' authentication ID stored in a cloud. If ID match the user is granted access to the network .suppose the ID was not match authentication fails and network access is stopped.

Authorization Authorization follows the authentication step. This step determines what the user is allowed to do. The application which is being accessed handles the part of authorization. Authorization can be determined based on the user identity alone, but in most cases requires additional attributes about the user, such as role or title.

Sanjoli Singla, Jasmeet Singh proposed *Data security issues in the cloud*. Because of the essential nature of cloud computing and large amounts of complex data it carries, Therefore, data privacy and security are issues that need to be resolved as they are acting as a major problem in the acceptance of cloud computing services[3]

Cloud Computing Concerns in the figure

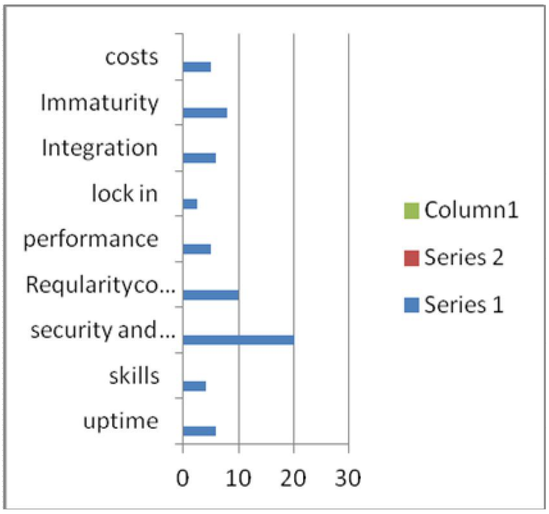

Figure 2.2 cloud computing concerns

There are two types of major security issues with cloud are:-

1. Privacy and Confidentiality

Once the clients outsource data to the cloud there must be some guarantee that data is accessible to only authorized users. The cloud user should be secure that data stored on the cloud will be secret.

2. Security and Data integrity

Data security can be provided using various encryption and decryption techniques. With providing the security of the data, cloud service provider should also implement mechanism to monitor reliability of the data at the cloud

The two different approaches used for ensuring security in cloud are as follows:-

1. **Extensible Authentication Protocol-CHAP:**

EAP(Extensible Authentication Protocol) will implement on Cloud environment for authentication purpose. It is used for the transport and usage of keying material and parameters generated by EAP methods.

2.Rijndael encryption Algorithm-

Rijndael as the standard symmetric key encryption algorithm to be used to encrypt sensitive information.

Mrs. S. M. Barhate1, Dr. M. P. Dhore2 PROPOSED Security issues in cloud computing

Cloud computing is not much secure by nature. Cloud security is not exactly real hence there a false sense of security and anxiety about what cloud data is actually secured and controlled. Although some security measures were applied to cloud infrastructure still the customers are expecting more security aspects for their data in clouds. This author said in this paper following attacks which can affect the cloud security:

1. **Password Guessing Attack**: This includes a variety of attack which can be done for obtain the user password.

2. **Replay Attack**: This attack includes track the authentication package and reproduce the information to the unauthorized users.

3. **Man-in-the-middle Attack:** Here the attacker poses to be a user and tries to get the password from the server.

4. **Masquerade Attack:** The attacker pretends to be a verifier and authentication keys from the user.

5. **Insider Attack:** Here the attacker intentionally steals the private information of the user.

6. **Phishing Attack:** Social Engineering sites such as fake emails, websites command the user expose his password or authentication keys.

7. **Shoulder Surfing Attack:** Social manufacturing attacks definite to password systems where the attacker secretly directs observing the password when the user enters it. The additional security can be achieved only through total transparency. We can implement security by taking in to account following points :

i. Cloud computing architecture
ii. Portability and interoperability
iii. Data centre operations
iv. Notification and remediation
v. Application Security
vi. Encryption and Key management
vii. Identity and access management.

D.Ranjith,J.srinivasan proposed "Identity Ecosystem" eliminates the need for individuals to manage multiple username and passwords for different online services. The Strategy highlighted four guiding values about identity solutions in order to have an ideal "Identity Ecosystem":

- Privacy-enhancing and voluntary identity solutions
- Secure and resilient identity solutions
- Interoperable identity solutions
- Cost-effective and easy to use

Garima Gupta1, P.R.Laxmi2 and Shubhanjali Sharma3 proposed

Techniques to secure data in cloud

1 Authentication and Identity

Authentication of users and even of communicating systems is performed by various methods, but the most common is cryptography. Authentication of users takes place in various ways like in the form of passwords that is known independently, in the form of a security token, or in the form a assessable measure like fingerprint. One problem with using usual identity approach in a cloud environment is faced when the activity uses multiple cloud service providers (CSPs). In such a use case, synchronizing identity information with the enterprise is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution. [4]

2 .Data Encryption

If preparation to store sensitive information on a large data store then need to use data encryption techniques. Having passwords and firewalls is good, but people can bypass them to access the data. When data is encrypted it is in a form that cannot be read without an encryption key. The data is totally useless to the interloper. It is a technique of translation of data into secret code. Suppose want to read the encrypted data, should have the secret key or password that is also called encryption key

Information integrity and Privacy

Cloud computing provides information and resources to valid users. Resources can be accessed through web browsers and can also be accessed by hateful attackers. A suitable solution to the problem of information integrity is to provide mutual hope between provider and user. Another solution can be providing proper authentication, authorization and accounting controls so the process of accessing information should go through various multi levels of checking to ensure authorized use of resources.

3. Availability of Information (SLA)

Non accessibility of information or data is a major issue concerning cloud computing services. Service Level conformity is used to provide the information about whether the network resources are available for users or not. It is a trust bond between consumer and provider .An way to provide availability of resources is to have a backup plan for local resources as well as for most crucial information. This enables the user to have the information about the resources even after their unavailability.

4. Secure Information Management

It is a technique of information security for a collection of data into central storehouse. It is comprise of agents running on systems that are to be monitor and then sends information to a server that is called "Security Console". The security console is managed by admin who is a human being who review the information and takes actions in response to any alerts. As the cloud user base, dependence stack increase, the cloud security mechanisms to solve security issues also increase, this makes cloud security management much more complicated. Cloud providers also provide some security standards like PCI DSS, SAS 70.

Mrs. Devyani Patil proposed
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 defence for data privacy in PASS category of CC. For strong access control PASS chooses a mandatory access control model which grants access grant allocation. Whenever such type of access control want to implement in CC a good security labelling 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[5]

The trusted third party can be tried upon for security :

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 Lap, implement the strongest available authentication process in distributed environments guaranteeing user mobility and flexibility.

2) Creation of **Security Domains-**

For creation of security domains association is a group of legal entity 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 Cloud which can interoperate means exchange of data and computing resources through defined interfaces.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 division in which data is appear indefinable to another unauthorized person. In which privacy and honesty 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.

4) Certificate-Based **Authorization –**

Relation between resources and users is more adhoc 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. Such type of certificates are issued by a certification authority that acts as a trust centre 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 provide something as input like username, token, retina scan or thumbprint. It is useful only when data is top Confidential e.g. Military or Defence.

8) Grid Based Authentication:

It is a second factor authentication which is provided by trust 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.

10) Machine Authentication:

In this efficient method in which users can typically right of entry their account from normal machines allowing for stronger authentication to be performed without any impact on users experience.

11) One Time Password: (OTP)

It is a animatedly generate 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. Asynchronous - In asynchronous token device used as challenge response scheme to authenticate user.

12) Global Authorization:

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

III .CONCLUSION

For the large distributed system like cloud Authentication and Authorization is a very important term. This term is helpful for all protection issues for both to user as well as cloud providers which solve multiple issues like **Password excellent, Repudiation**. **Session hijacking. Middle attacks Session replay, Spoofing**.. Explore about this security issues is still in improvement 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] D.Ranjith#1, J.Srinivasan*2
# Department of Computer Science and Applications, Adhiparasakthi College of Arts and Science,Kalavai,Vellore-632506

[2] Mrs. S. M. Barhate1, Dr. M. P. Dhore2 *(shwetab73@yahoo.com, Dept. Of Electronics & Computer Science RTM Nagpur University, Nagpur, India) 2(mpdhore@rediffmail.com, Dept. Of Electronics & Computer Science RTM Nagpur University, Nagpur, India).*

[3] ***Manuscript received June, 2013****.*
Sanjoli Singla*, M.Tech(CSE) Student, RIMT-IET(Punjab Technical University), Mandi Gobindgarh, India,* ***Jasmeet Singh****, Assistant Professor in CSE Department,RIMT-IET(Punjab Technical University), Mani Gobindgarh, India,*

[4] Garima Gupta1, P.R.Laxmi2 and Shubhanjali Sharma3 .1Department of Computer Engineering, Government Engineering College, Ajmz Gupt garima09@gmail.com .2Department of Computer Engineering, Government Engineering College, Ajmer laxmigweca@gmail.com 3Department of Computer Engineering, Government Engineering College, Ajmer

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

[6] Umer Khalid, Abdul Ghafoor, Misbah Irum, Muhammad Awais Shibli *a National University of Sciences* & *Technology, H-12, Islamabad 44000, Pakistan*

[7] Umer Khalida, Abdul Ghafoor, Misbah Irum, Muhammad Awais Shibli *a National University of Sciences* & *Technology, H-12, Islamabad 44000, Pakistan*

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

[9] Hyokyung Chang and Euiin Choi
Dept. of Computer Engineering, Hannam University, Daejeon, Koreahkjang@dblab.hannam.ac.kr, eichoi@hnu.kr