IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 30-35
www.iosrjournals.org

User Authentication Issues In Cloud Computing

Mrs. S. M. Barhate[1], Dr. M. P. Dhore[2]
[1](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)

Abstract: *Cloud Computing is an emerging concept for geographically distributed data centres and resources which are made available online as services. In cloud computing, interoperability means the ability of an organization to move its workload easily from one cloud environment to other. As the resources are being shared among the servers and users, the files or data is more vulnerable to attacks. Thus interoperability brings with it the challenges of security and privacy. There exists a possibility for unauthorized users to enter and access the data in cloud. In this situation virtual machines are allotted to the cloud users. These machines have legitimate logins which can be easily cracked. This paper reviews the user authentication and authorization issues for secured interoperability in cloud computing.*

Keywords- *Cloud computing, interoperability, user authentication, authorization, virtual machines*

I. Introduction

Cloud Computing is form of distributed computing in which a specific application may run on different linked computers simultaneously. Cloud computing has provided with various extraordinary facilities like doing complex calculations with ease, mass storage, ubiquitous computing, low storage cost, ease of access etc. To use this facility the most easy and known security provided for access are static passwords. But the cracking of these passwords is easy as users don't use complicated passwords, or don't change their passwords on and off, or may use same password to access multiple services. Hence the security of data on cloud computing is the necessity of the hour.

NIST defined cloud computing as a model for enabling convenient, on-demand network access to a shared pool of computing resources which can be rapidly provisioned and released with minimal management efforts or service provider interaction.[1] NIST, OMG, DMTF as a part of their efforts related to standardization for cloud interoperability have developed use cases for cloud computing. These use cases are divided into cloud management, cloud interoperability and cloud security. Here since we are concentrating on interoperability related issues we would consider the interoperability use cases which are as follows:

1. User Authentication
2. Workload Migration
3. Data Migration
4. Workload Management

The use case for *user authentication* corresponds to a user or program that needs to be identified in the cloud environment. It is important to differentiate between two types of users of cloud environments i.e. end users and cloud-resource users. End users are users of applications deployed on cloud resources. Because these users register and identify with the application and not with the infrastructure resources, they are usually not aware that the application is running on cloud resources. Cloud-resource users are typically administrators of the cloud resources. These users can also set permissions for the resources based on roles, access lists, IP addresses, domains. The second type of user is of greater interest from an interoperability perspective. This paper is analysing the first interoperability use case which is user authentication. All the user authentication issues, the algorithms and the protocols used for securing user authentication are analysed in detail.[2]

II. Security issues in cloud computing

Cloud computing is not much secure by nature. Cloud security is not exactly tangible hence there a false sense of security and anxiety about what cloud data is actually secured and controlled. There are concerns related to the integrity and confidentiality of data. There should appropriate security measures for cloud customers to achieve their belief. Although some security measures were applied to cloud infrastructure still the customers are expecting more security aspects for their data in clouds. The cloud data is vulnerable to various kinds of attacks. This paper studies following attacks which can affect the cloud security:

1. **Password Guessing Attack**: This includes various attacks which can be done for obtaining the user password.
2. **Replay Attack**: This attack includes tracking the authentication packet and reproduces the information to the unauthorized users.
3. **Man-in-the-middle Attack:** Here the attacker poses to be a user and tries to acquire 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 deliberately steals the private information of the user.
6. **Phishing Attack:** Social Engineering sites such as fake emails, websites demand the user reveal his password or authentication keys.
7. **Shoulder Surfing Attack:** Social engineering attacks definite to password systems where the attacker secretly directs observing the password when the user enters it. [3]

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 .[4]

III. Introduction to User Authentication And Authorization

Cloud computing provides customers with highly scalable and on-mend computing resources. NIST specified three cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructural as a Service (IaaS), each service models target a specific need of customers.

- Software as a Service offers applications that were provided by the cloud service providers and hosted by the cloud provider.
- 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.

Various cloud services and cloud service providers are beneficial for customers who seek specific computing resource, it creates some security challenges to the customers seeking different cloud services however.

1. Cloud service providers request customers to store their account information in the cloud and they have the access to this information. This presents a privacy issue to the customer's privacy information.
2. Many SLAs have specified the privacy of the sensitive information. It is difficult for customers to make sure the proper rules are enforced. There is a lack of transparency in the cloud that allows the customers to monitor their own privacy information.
3. When a customer decides to use multiple cloud service, the customer will have to store the password in multiple cloud. As the user takes cloud subscription of any cloud service that much number of copies of the users information are created. This is a security issue for the customers and the cloud service providers.
4. The multiple copies of account will lead to multiple authentication processes. For every cloud service, the customer needs to exchange their authentication information.
5. Cloud service providers use different authentication technologies for authenticating users, this may have less impact on SaaS than PaaS and IaaS, but it is present a challenge to the customers.[4]

The key concept to user authentication is that a user who established an identity by connection with cloud computing can use the same identity with other clouds also.

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 audit their activities. Thus authentication and authorization are critical components of a cloud identity strategy and provide portability and extensibility beyond enterprise boundaries.

Authentication

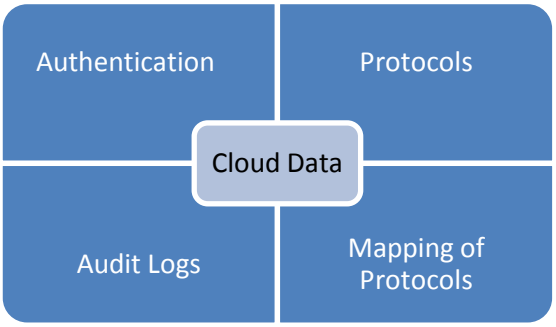
Authentication is the process for confirming the identity of the user. The traditional authentication process allows the system to identify the user through a username and then validate their identity through password. There are even stronger methods of user authentication such as x.509 certificates, one-time passwords (OTP), and device fingerprinting. These can be combined to provide a stronger combination of authentication factors. Federated identity allows a user to access an application in one domain, such as a Software-as-as-Service (SaaS) application, using the authentication that occurred in another domain, such as a corporate Identity Management (IdM) system.

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. The advancement here is the centralization of the authorization policy regardless of the location of the user or the application. 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.

IV. Techniques used in user Authentication and Authorization

Identity and Access Control Service should provide identity management and access control to cloud resources for registered entities. Such entities can be people, software processes or other systems. In order to give a proper level of access to a resource, the identity of an entity should be verified first, which is the authentication process that precedes the authorization process. Besides authentication and authorization processes, audit logging mechanism should be used to keep track of all successful and failed operations regarding authentication and access attempts by the application. Confidentiality is achieved by different encryption mechanisms, which is the procedure of encoding data by means of cryptographic algorithms[5,6]. Providing such a service will guarantee privacy of sensitive and private data and the intended entity can only decode it. Cryptographic algorithms, which are computationally hard to crack together with encryption and decryption procedures, digital signatures, hashing, certificates, key exchange and management form an encryption system which can be delivered as a service and assure confidentiality and non-repudiation in a cloud environment[7].



Cloud Security Model

Algorithms For User Authentication And Authorization: The central idea behind the Security provision is to avoid the unwanted intrusion of unauthorized users and right at the entry point. That is all the users whether new of existing are not allowed to access the data or resources without proving their identity. The request from the users are first encrypted and then sent to the cloud files. The algorithms used to encryption process are discussed as follows:

- **RSA Algorithm:** RSA encryption algorithm is used for making the communication safe. Usually the users' requests are encrypted while sending to the cloud service provider system. RSA algorithm using the system's public key is used for the encryption. Whenever the user requests for a file the system sends it by encrypting it via RSA encryption algorithm using the user's public key. Same process is also applied about the user password requests, while logging in the system later. After receiving an encrypted file from the system the user's browser will decrypt it with RSA algorithm using the user's private key. Similarly when the system receives an encrypted file from the user it will immediately decrypt it using its private key. As a result the communication becomes secured between the user and the system.[8,9]

- **AES Algorithm & MD5 Hashing Algorithm**: When a file is uploaded by an user the system server encrypts the file using AES encryption algorithm. In this 128, 192, 256 bit key can be used. The key is

generated randomly by the system server. A single key is used only once. That particular key is used for encrypting and decrypting a file of a user for that instance. This key is not further used in any instance later. The key is kept in the database table of the system server along with the user account name. Before inserting the user account name it is also hashed using md5 hashing. This insures that unauthorized person cannot retrieve the key to decrypt a particular file for a particular user by simply gaining access and observing the database table of the system server. As a result the key for a particular file becomes hidden and safe. Again when the encrypted file is uploaded for storing to the storage server, the path of the encrypted file along with the user account is kept and maintained in the database table on the storage server. Here user name is used for synchronization between the database tables of main system server and the storage server. The encrypted files on the storage server are inserted not serially.[10,11,12]

- **OTP Password Algorithm:** In this algorithm one time password has been used for authenticating the user. The password is used to keep the user account secure and secret from the unauthorized user. But the user defined password can be compromised. To overcome this difficulty one time password is used in the proposed security model. Thus whenever a user logs in the system, he will be provided with a new password for using it in the next login. This is usually provided by the system itself. This password will be generated randomly. Each time a new password is created for a user, the previous password for that user will be erased from the system. New password will be updated for that particular user. A single password will be used for login only once. The password will be sent to the users authorized mail account. Therefore at a same time a check to determine the validity of the user is also performed. As a result only authorized user with a valid mail account will be able to connect to the cloud system.[14,15]

- **Data Encryption Standard Algorithm:** Data Encryption Standard algorithm is a type of symmetric-key encipherment algorithms. Symmetric-key encryption is a type of cryptosystem in which encryption and decryption are performed using a single (secret) key. As we can see, secret key play a very important role in DES security, so that a good key generation unit required. Using Dynamic key generator, the generated key has characteristics of unpredictability and unrepeatability. Using this approach the dynamic key generator can achieve the high speed and can be reduce logic complexity.

- **Rijndael encryption Algorithm:** Rijndael is the standard symmetric key encryption algorithm to be used to encrypt sensitive information. Rijndael is an iterated block cipher, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function). As input, Rijndael accepts one-dimensional 8-bit byte arrays that create data blocks. The plaintext is input and then mapped onto state bytes. The cipher key is also a one-dimensional 8-bit byte array. With an iterated block cipher, the different transformations operate in sequence on intermediate cipher results (states).

Protocols Used`In The Process of User Authentication And Authorization

Identity and Access Control Service should provide identity management and access control to cloud resources for registered entities. Such entities can be people, software processes or other systems. In order to give a proper level of access to a resource, the identity of an entity should be verified first, which is the authentication process that precedes the authorization process. Besides authentication and authorization processes, audit logging mechanism should be used to keep track of all successful and failed operations regarding authentication and access attempts by the application. Confidentiality is achieved by different encryption mechanisms, which is the procedure of encoding data by means of cryptographic algorithms. Providing such a service will guarantee privacy of sensitive and private data and the intended entity can only decode it. Cryptographic algorithms, which are computationally hard to crack together with encryption and decryption procedures, digital signatures, hashing, certificates, key exchange and management form an encryption system which can be delivered as a service and assure confidentiality and non-repudiation in a cloud environment.

Authentication Protocols used are as follows:

- **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. In our purposed model we use Challenge-Handshake Authentication Protocol (CHAP) for authentication.[17]

- **Lightweight Directory Access Protocol:** Most companies are storing their important information in some type of Lightweight Directory Access Protocol server. SaaS providers can provide delegate the

authentication process to the customer's internal LDAP/AD server, so that companies can retain control over the management of users.

- **Single Sign-on (SSO) protocol:** This protocol is part of the shared security system of a cloud environment. The system consists of a SAML server which provides SSO services for application service providers: SAML server issues SAML ticket which contains an assertion about the client's identity verification, thus confirming that it has been properly authenticated or not. Once the user is authenticated, he or she can request access to different authorized resources at different application provider sites without the need to re-authenticate for each domain.

Audit Logging

The ability for an enterprise to track what applications users are accessing is a alarm with respect to both security and regulatory perspective. But this has becomes a serious challenge since users and applications are no longer staying within the enterprise and working instead within the Cloud. Multiple failed authentication events or authenticated users attempting unauthorized application access will highlight potential security and fraud related activities. In addition, regulated industries require audit trails to prove that only authorized users have accessed or attempted to access certain confidential systems. Federation solutions provide the central gateway for users accessing cloud apps, whether from their desk or remote, via the company computer, personal computer or mobile device. This central point of access also provides a central point of auditing and reporting.

V. Conclusions

In the recent situation of Networking system, cloud Computing is very important concept for both the developers and users. But security is the major challenging issue in cloud computing. Without appropriate security and privacy measures designed for clouds, this potentially revolutionizing computing paradigm could become a huge failure. Data security has become the vital issue of cloud computing security. Interoperability means easily moving the workloads from one cloud to another. The interoperability used case has the basic and first important requirement of secure and safer user authentication and authorization. The main idea behind this study was to take a first step towards cloud security. The preliminary or the most basic attack possibility of user access is checked upon by using different algorithms. Each algorithm uses different protocols in view of providing best possible check to user authentication and authorization.

In this paper we dealt with different algorithms used for user authentication and authorization in cloud computing. Different algorithms such as RSA, AES, MD5, OTP password generation algorithm, DES, Rijndael encryption Algorithm were studied. RSA Algorithm is deterministic and hence becomes fragile in long run. But the other algorithms discussed make the model highly secured. Each of this algorithms discussed were developed to provide best ever possible solution to the user authentication and authorization issues. Different protocols such as LDAP, EAP, & SSO protocols were also studied. Even if some intruder gets access of the data accidentally or intentionally, he will not be able to decrypt it.

References

[1]. Wayne A Jansen, NIST, "Cloud Hooks: Security and Privacy Issues in Cloud Computing**"** Proceedings of the 44th Hawaii International Conference on System Sciences – 2011.

[2]. Grace A.Lewis, "The Role of Standards in Cloud Computing Interoperability", Technical note, Software Engieering Institute, October 2012.

[3]. Shikha Choksi, "Comparative Study on Authentication Schemes for Cloud Computing", IJEDR, Volume 2, Issue 2, ISSN 2321-9939.

[4]. Abdel Majid Hassan, Mansoor emam, "Additional Authetication and Authorization using registered E-mail id for cloud computing", International Journal of Soft Computing and Engineering(IJSCE), ISSN 2231-2307,Volume-3, Issue-2,May 2013.

[5]. Dawei Sun, Guiran Chang, Lina Sun, and Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", Scienceverse Science Direct , Elsevier, 2011

[6]. Davit Hakobyan, "Authentication And Authorization Systems In Cloud Environment", Master Of Science Thesis, Sweden, 2012.

[7]. Jianhua Che, Yamin Duanb, Tao Zhang, Jie Fan, "Study on the security models and strategies of cloud computing", Scienceverse Science Direct , Elsevier, 2011

[8]. "Cloud Data Security Using Authentication And Encryption technique, Sanjoli single, Jasmeet Singh, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 7, July 2013.

[9]. R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Laboratory for Computer Science, Massachusetts Institute of Technology, Cam-bridge, November, 1977.

[10]. Burt Kaliski, The Mathematics of the RSA Public-Key Cryptosystem, RSA Laboratories

[11]. Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndael", 1999

[12]. Joan Daemen, Vincent Rijmen, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197, November 26, 2001.

[13]. Joshua Holden, Mohammad Musa, Edward Schaefer, and Stephen Wedig, "A Simplified AES Algorithm", January 2010 .

[14]. Ronald Rivest, "MD5 Message-Digest Algorithm", rfc 1321, April 1992 .

[15]. Neil M.Haller, "THE S/KEY ONE-TIME PASSWORD SYSTEM", 1993.

[16]. Neil Haller, "A One-Time Password System", October 23, 1995.
[17]. Sadia Marium et al, "Implementation of EAP with RSA for Enhancing the Security of cloud Computing", International Journal of Basic And Applied Sciences, 1(3),2012.