ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Review of Authentication Mechanisms in Open Distributed System and Cloud Computing

Arifa Juhi Ansari

Research Scholar, Dept. of Computer Science & Engineering, Shri Ram Institute of Technology, Jabalpur, India

ABSTRACT: While authentication within organizations is a well-understood problem, traditional solutions are often inadequate at the scale of the Internet, where the lack of a central authority, the open nature of the systems, and issues such as privacy and anonymity create new challenges. For example, users typically establish dozens of web accounts with independently administered services under a single password, which increases the likelihood of exposure of their credentials; users wish to receive email from anyone who is not a spammer, but the openness of the email infrastructure makes it hard to authenticate legitimate senders; users may have a rightful expectation of privacy when viewing widely-accessed protected resources such as premium website content, yet they are commonly required to present identifying login credentials, which permits tracking of their access patterns.

KEYWORDS: user authentication, authorization, virtual machines

I. INTRODUCTION

In its basic form, authentication is a well-understood concept in information security. Yet, many scenarios call for slight variations on the basic theme, where existing solutions do not directly apply; new techniques need to be developed. In the context of password-based user authentication, for example, users often reuse the same credentials (i.e., their passwords) when establishing accounts with dozens of independently administered services. Under such circumstances, a user whose password is compromised is unlikely to remember every place at which she needs to update her login information. At best, recovery from compromise is a lengthy, manual process. Based on work first published as, this paper describes an authentication mechanism that addresses these challenges for SFS, a secure, global file system. To attain its goals, the system employs proactive two-party signatures, a special kind of digital signatures, in which a private key is split between two parties, both of whom must approve and participate in signing authentication requests. This property enables a design in which an authentication server keeps a signature log describing all network accesses performed on behalf of the user, which provides a valuable audit trail in case of a break-in. Moreover, proactive two-party signatures allow private key shares to be updated, so that old shares cannot be combined with new ones to sign messages or to recover the private key. While a number of proactive protocols have been proposed in the cryptographic literature, they were all based on threshold schemes that cannot be applied to the practically relevant two-party case. Our novel construction fills this deficiency, providing a solution that is at the same time easy-to-implement and cryptographically secure. As another example, in spam-filtering systems, a legitimate sender wants to authenticate himself to the recipient as a non-spammer. Leveraging an existing social network, this type of authentication can be accomplished by demonstrating a short chain of social contacts connecting the sender to the recipient— assuming that users do not maintain social relationships with spammers. Discovering these chains requires sharing social information, which introduces privacy concerns. Chapter 3 defines a privacy model for demonstrating proximity in social networks. Using insights from this modeling, we derive efficient cryptographic protocols

Enabling parties to determine shared friends while exposing minimal information about their social contacts. We then describe how to integrate these privacy mechanisms within an improved prototype of the Re: (Reliable Email) white-listing system. Compared with Re:'s initial design, the cryptographic solution derived from this new privacy model better addresses the system's privacy goals, and avoids the computational bottleneck due to Re:'s earlier use of a general-purpose privacy-preserving protocol. A different flavor of authentication is at play in group access control: when accessing a group-protected object or service, a user only needs to authenticate herself as a member of the relevant group. Controlled access to the resource is thus enforced, while affording a degree of protection to the identity

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

of the user who "anonymously identifies" herself.

Of widely used network file systems, SFS's goals are probably most similar to those of AFS. AFS is a file system designed to work over the wide-area network. AFS has been particularly successful in large organizations—for instance permitting the user community of an entire university to share access to the same file systems. Unfortunately, AFS does not adapt as well to settings with many different administrative realms. AFS's security is based on the centralized Kerberos authentication system in which a central authority manages all of the accounts and servers in a given administrative realm. Cross-realm authentication is possible, but requires cooperation from realm administrators. Thus, users must typically type a separate password for each realm in which they wish to access servers. Since the central Kerberos server stores a secret that is effectively equivalent to the user's password, it is inadvisable for users to have the same password in different Kerberos realms. The SSH remote login tool supports a mode of authentication based on public keys. The user registers his private key with an agent process on the local ma-chine, and stores the corresponding public key in a file .ssh/authorized keys in his home directory on the server. SSH public key authentication is very convenient. Users therefore typically end up copying their authorized keys file to all of their different accounts. Unfortunately, changing public keys requires many accounts to be updated, and users are likely to forget to update accounts on infrequently used machines. Perhaps most relevant to P2SS are the various token- and hardware-based user-authentication systems. As smart cards and other physical security devices gain more computational power, it will become increasingly practical for them to compute digital signatures. Such configurations will be even more desirable if they can keep an audit trail of all signed messages in case the device is stolen or otherwise compromised. P2SS schemes enable such scenarios, while additionally allowing users to recover from compromised devices without changing their public keys. To compromise a user's public key permanently, an attacker would need to break the user's hardware device (or steal a backup of the user's share) and compromise the centralized signature server before the user had an opportunity to recover from the first event.

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 :

a. Cloud computing architecture
b. Portability and interoperability

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

c. Data centre operations
d. Notification and remediation
e. Application Security
f. Encryption and Key management
g. 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

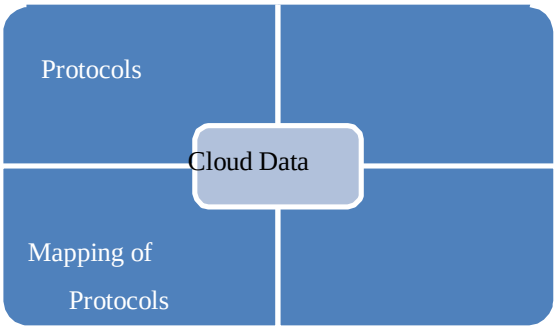
Authorization

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

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 iimportant 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-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

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 – 2016.
[2]. Grace A.Lewis, "The Role of Standards in Cloud Computing Interoperability", Technical note, Software Engieering Institute, October 2015.
[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 2016.
[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, 2016
[6]. Davit Hakobyan, "Authentication And Authorization Systems In Cloud Environment", Master Of Science Thesis, Sweden, 2015.
[7]. Jianhua Che, Yamin Duanb, Tao Zhang, Jie Fan, "Study on the security models and strategies of cloud computing", Scienceverse Science Direct , Elsevier, 2015
[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 2016.
[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, 2012.
[10]. Burt Kaliski, The Mathematics of the RSA Public-Key Cryptosystem, RSA Laboratories
[11]. Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndael", 2013
[12]. Joan Daemen, Vincent Rijmen, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197, November 26, 2011.
[13]. Joshua Holden, Mohammad Musa, Edward Schaefer, and Stephen Wedig, "A Simplified AES Algorithm", January 2016 .
[14]. Ronald Rivest, "MD5 Message-Digest Algorithm", rfc 1321, April 2014 .
[15]. Neil M.Haller, "THE S/KEY ONE-TIME PASSWORD SYSTEM", 2013.
[16]. Neil Haller, "A One-Time Password System", October 23, 2014.
[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),2014.