A review paper on Authentication Services in Cloud Computing Environment

Mamta Tewari[#1]

[#]*Computer Science Department, Uttarakhand Technical University*
BTKIT, Dwarahat, Almora, India
[1]mamta20tewari2gmail.com

***Abstract*—Cloud computing is a new paradigm which gives an opportunity to avail services on rent basis. Although clouds have gone a long way but still security is the main concern associated with them. The breached information can be used by the rivals or an enemy in a most destructive way. So, every cloud vendor wants to provide the best security than others. Authentication is one such issue that deals with the security part. It is quite important to have a strong authentication framework while working with clouds. The information and resources needs to be used by the authenticated user so that there is no tempering with them. This paper gives an insight of some authentication frameworks that are proposed for clouds and also analyse their applicability as per the requirement of the user.**

***Keywords*— Cloud Computing, Authentication, authentication factors, one time password**

I. INTRODUCTION

Cloud computing has given a new definition of managing and handling the resources in present era of advanced technology. Cloud can be defined as an on demand service providing mechanism in which the cloud owners own the required resources and gives the access to their customers as per their need on rent. The customer is free to choose the service he/she wants and pay the required amount for it. Before the inclusion of clouds, the organizations used to invest on the resources and its maintenance and everything was their responsibility but nowadays when cloud computing is ubiquitously used it is completely the headache of the cloud provider. They provide the required service to the customer.

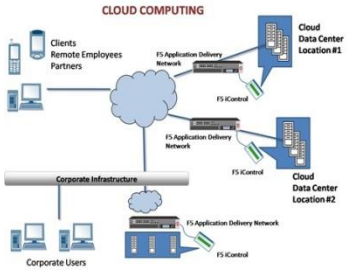

Fig. 1 A cloud computing environment

In cloud computing the cost of accessing an application is reduced, no overhead of managing the services of the organization and increased efficiency is achieved.

A. Concerns in cloud computing

Although cloud has given us new option for utilizing resources over internet but many issues are associated with it. A survey was conducted by Fujitsu from the user's viewpoint where it was found that safety and reliability are the major concern of a user. Figure 2 is the result of Fujitsu Journal customer questionnaire and gives the concerns that were highlighted by the user. The highest rated concern among users was of security.

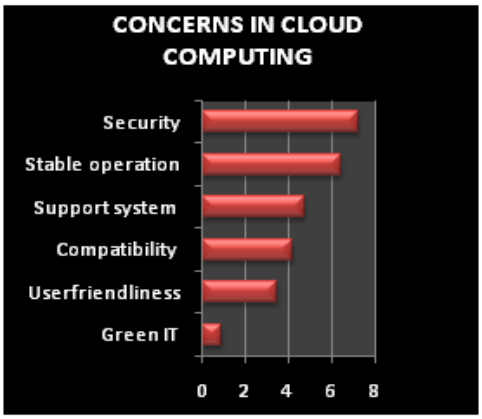

Fig. 2 Concerns in cloud computing

II. SECURITY IN CLOUD

Cloud has brought a new revolution in IT world and has given a lot more options to user but the major concern while working with the clouds is of security. No matter how beneficial is cloud computing for us but it is futile if we do not have a strong security framework for it. As described in [18] the security related concerns in cloud are depicted in figure 3. This paper focuses on authentication issue related to cloud services security. Before going through the various techniques proposed for authentication, we need to understand its basics, factors and types.

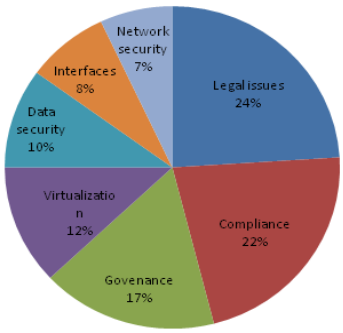

Fig.3 [19] Security problems with grouped categories

A. Authentication:

Authentication is the process of verifying the identity of an individual to check whether the person is the one that it claims to be. It is really important to verify the credentiality of an individual for accessing a particular service. Unavailability of authentication in a system can lead to catastrophic consequences.

1) Authentication factors: There exists following three types of authentication factors:

- something the consumer knows like passwords, pin etc
- something the consumer has like atm card, smart card etc
- something the consumer is like the biometric features of a person for eg fingerprint, iris detection

2) Authentication types: The authentication services are classified as:

- *Single factor authentication:* In this kind of authentication there is only one parameter to check the user credentiality.
- *Two factor authentication*: It combines any two of the above mentioned parameters to authenticate users. The combination of ATM card and password is an example of two factor authentication.
- *Multifactor authentication*: Multifactor authentication combines two or more than two authentication factors to give provide a high degree of security for the systems dealing with critical information.

III. DIFFERENT AUTHENTICATION FRAMEWORKS FOR CLOUD

A. One time password for Multi-cloud environment [2]

These day's organizations depends on more than one cloud for providing services as they don't want to be source deprived at any point of time. So this requirement leads to dependency among the clouds which further leads to the need of a strong security framework for multi cloud environment which is a daunting task. A definition of Muti-cloud is given by Vukolic [3] as "cloud of clouds which says that the term cloud computing should not end up as a single cloud".

Due to the limitations of static passwords a more dynamic approach of one time password (OTP) is being evolved. OTP [4] is a secure technique for managing passwords as there is no chance of forgetting or misuse of it due to the fact that it is used only one time.

1) *OTP basics [5]:*

OTP generation algorithms typically make use of pseudorandomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging. Finally, in some systems, OTPs are printed on paper that the user is required to carry.

2) OTP for multi cloud:

In this approach OTP technique is deployed for multi cloud environment. For this we need to design an authentication framework which can generate OTP and can connect to all clouds. OTP can generated using the OTP generation algorithms and can generate OTPs for ach login session.

B. Advanced secure user authentication framework for cloud computing [6]

It utilizes the concept of remote user authentication schemes by applying the two factor authentication. This framework ensures that only legitimate users can get access the cloud services. This paper tries to overcome the flaws present in Choudhury et al [7] remote user authentication framework which is vulnerable to masquerade attack, the OOB (out of band) attack and the password change flaw.

This scheme consists of following stages:

- Registration phase
- login phase
- authentication phase
- password change scheme

Basically the author has proved that the advanced technique is better from the scheme proposed by Choudhury et al in the following ways :

- Withstanding masquerade attack: Even if the smart card is stolen and attacker hack the card details but it is of no use.
- Avoiding OOB attack: advanced secure user authentication scheme does not use onetime key K. Instead, it uses h(K') to encrypt the message to ensure protocol is secure. Thus, it avoids transmitting K through OOB channel and avoid OOB attack.
- A secure Password change policy is provided in this scheme.
- The time delay and communication overhead is very less in this scheme as compared to Choudhury et al.

C. A consolidated authentication model in cloud computing environment [8]

Due to increasing needs of Internet access through smart phones and smart pads, it is essential to have service provider systems, which allows to access services through a variety of devices. CAM provides a safe and convenient user authentication model that mobile device users can effortlessly use credentials in cloud computing environments.

1) Consolidated authentication model (CAM): CAM consists of consolidated authentication mechanism and policy compliance mechanism. The clients uploads or downloads credentials from credential server(CS), credential server is a kind of repository of all kind for secure credentials. The signing server(SS) creates a digital signature by the Client's request. Consolidated authentication mechanism consists of account management module (AMM), credential roaming module (CRM) and proxy signature module (PSM).

AMM deals with

- Initialization and key sharing operations
- Creating account protocol
- Modify and remove account protocol

CRM deals with

- Credential upload protocol
- Credential download protocol from credential server(CS)
- Credential download protocol from direct solutions like PKCS#12 [9] and PKCS#15 [10].

Proxy signature operations

- Proxy signature protocol

2) Comparison of CAM with PKI:

- CAM: User's device requests proxy signature to signing server and service provider verifies it. PKI: User's device generates digital signature and service provider verify it.
- After simulation of RSA signing and verification for each platform it is found that CAM is a time saving and robust authentication framework than traditional PKI based authentication system and solves existing problems by satisfying framework requirements, protocol requirements and privacy protection requirements.
- For operating various mobile devices like mobile, smart phones etc CAM provides a flexible authentication framework and a safer credential management system.

D. Anonymous RFID authentication for cloud services [11]

Anonymous authentication is a technique enabling users to prove that they have privilege without disclosing real identities and it is useful in such situations where it is enough to ensure that the claiming party is the registered user. It introduced practical threat known as big brother attack. Sometimes the person responsible for maintaining the server is interested in detailed profile of registered user to track their profile details and misuse it later. To avoid such kinds of attack it is required that the identity of the user should remain anonymous.

Anonymous RFID authentication is inspired by this and tries to provide a solution for server side corruption. The authentication between the user and service is performed by Radio Frequency Identification (RFID) which is a means of identifying objects with the help of Radio Signals. A typical RFID system is setup by a set of readers, a number of RFID tags and a backend server. In general sense, an RFID tag is known as a small integrated circuit with a unique identifier which transmits data over the air in response to interrogation by an RFID reader [19]. A smart tag, on the other hand, has on-board processors that are typically capable of performing cryptographic operations. RFID authentication is based on threshold cryptosystems [12]

In cryptography, a cryptosystem is called a "threshold cryptosystem", if in order to decrypt an encrypted message a number of parties exceeding a threshold is required to cooperate in the decryption protocol. The message is encrypted using a public key and the corresponding private key is shared among the participating parties. Let n be the number of parties. Such a system is called *(t, n)*-threshold, if at least *t* of these parties can efficiently decrypt the cipher text, while less than *t* have no useful information. Similarly it is possible to define *(t, n)*-threshold signature scheme, where at least *t* parties are required for creating a signature [13].

The secret is distributed among n participants or shadow holders [16] and at least t members are required to be together to reveal the secret.

ElGamal or Paillier [14] [15] are two widely used threshold cryptosystems and both the protocols proposed in this paper

supports any two of these threshold cryptosystems. But for ease ElGamal is used in this paper. RFID uses (2, n) threshold cryptosystem which means two parties a server and a tag can decrypt the cipher to pass authentication.

The paper proposes anonymous and mutual RFID authentication protocol. It uses RFID tags to authenticate users without revealing the identities of the tags.

Two protocols are proposed in this:

- First protocol provides the anonymous and unilateral authentication. It is based on (2,n)-threshold homomorphic encryption and provides anonymous authentication even when the server is fully corrupted.
- Second protocol provides the anonymous and mutual authentication.

IV. CONCLUSION

This paper discussed four techniques of authentication in cloud environment and gets an insight of their working and applicability. The OTP for multi cloud environment gives an effective password technique than the traditional static passwords which are vulnerable to several kinds of attacks. OTP is time saving for multiple process clouds.

The advanced user authentication technique is an improved remote user authentication technique which is strong against the masquerade attack, OOB attack, provides a secure password change scheme. Time delay and communication overhead is less as compared to earlier schemes.

The CAM is an authentication useful in providing authentication for various mobile devices such as mobile phones, smart phones etc as CAM provides a credential roaming in cloud environment.

The anonymous RFID authentication technique tries to overcome the server side attacks where the identity of user can be used illegally. A practical threat called as big brother attack is introduced in this paper. It is useful when the user authentication is done without revealing their identities and provides the anonymity, privacy, authentication and unlinkability.

REFERENCES

[1] Masayuki Okhuhara, Takuya Suzuki, Tetsuo Shiozaki, :Security Architectures for Cloud computing.

[2] Chowdhary et al., One time password for muti cloud environment, International Journal of Advanced Research in Computer Science and Software Engineering 3(3),March - 2013, pp. 594-597

[3] M. Vukolic, "The Byzantine empire in the inter cloud", ACM SIGACT News, 41,2010, pp.105-111

[4] W.B.Hsieh, J.S.Leu: “Design of a time and location based one time password authentication scheme”, 7th IEEE International Conference,2011

[5] http://en.wikipedia.org/wiki/One time_password

[6] Rui Jiang, Advanced secure user authentication framework for cloud computing

[7] Amlan Jyoti Choudhury, Pardeep Kumar, Managal Sain, Hyotaek Lim, Hoon Jae-Lee, “A Strong User Authentication Framework for Cloud Computing”, Proceedings of 2011 IEEE Asia-Pacific Services Computing Conference, Jeju, South Korea, December 12-15, 2011, pp.110-115.

[8] 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

[9] RSA Lab. PKCS #12 v1.0: Personal Information Exchange Syntax, (1999) June.

[10] RSA Lab. PKCS #15 v1.1: Cryptographic Token Information Syntax Standard, (2000) June

[11] INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, Muhammed Ali Bing ¨ ol et al., Anonymous RFID authentication for cloud services ,Vol.1, No.2

[12] Threshold Cryptosystems, ser. Lecture Notes in Computer Science,vol. 435. Springer, 1990.

[13] http://en.wikipedia.org/wiki/Threshold_cryptosystem

[14] T. E. Gamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,”in Proceedings of CRYPTO 84 on Advances in cryptology. Springer-Verlag New York, Inc., 1985, pp. 10–18.

[15] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in Advances in Cryptology – EUROCRYPT ’99, International Conference on the Theory and Application of Cryptographic Techniques, ser. Lecture Notes in Computer Science. Springer, 1999, pp. 223–238.

[16] Yvo Desmedt, Yair Frankel, “Thresold Crptosytem” .

[17] devcentral.f5.com/articles/cloud-computing-its-the-destination-not-the-journey-that-is-important#.Uq1IJ9IW1aQ

[18] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd ed. New York, NY, USA: John Wiley & Sons, Inc., 2003

[19] Gonzalezet al. Journal of Cloud Computing: Advances, Systems and Applications2012,1:1