International Journal of Engineering & Technology, 7 (3.29) (2018) 319-322

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Review on authentication mechanisms in cloud computing

D. Sumathi [1] *, Sireesha Jasti [2]

[1] *Professor Malla Reddy Engineering College*
[2] *Associate Professor Malla Reddy Engineering College*
**Corresponding author E-mail: sumathi.research28@gmail.com*

Abstract

Cloud computing is one of the most significant revolutionary technologies that provide services from computing infrastructures, applications, and platforms to customers for their personal coalition whenever and wherever needed. Security is considered to be the most important key component in the challenges of cloud computing field. This work discusses about the first level key challenges of security-Authentication. Many authentication schemes have been proposed earlier. But all those schemes work as an entry level for service requisition. When the consumers face any problems during the service availability, then both the consumers and service providers need a quick outlook to the SLA. Based on the severity level of the issue, the service providers need permission to access the service area rented by the consumer. This work provides the critics and reviews of authentication mechanisms that have been carried out earlier. In addition, it also provides an overview of authentication mechanisms carried out by service providers and a comparison of various authentication mechanisms has been discussed.

Keywords: *Authentication Mechanisms; Cloud Computing; Mutual Authentication Scheme; Security Issues.*

1. Introduction

Cloud computing as an emerging technology conquers the corporate business world, educational institutions etc with its distinguished characteristics like resource pooling, unlimited storage, automatic software integration, resource provisioning etc. The key factor that draws everyone attention in this cloud computing is security, since consumers who rent space to store data in the cloud need to think of providing security to the data. Moving computation geographically into common server rooms brings issues related to security such as virtualization security, application security, access control, CIA mechanisms. The purpose of cryptography is to secure confidentiality, integrity and authenticity of the available data. User authentication is the paramount requirement in the cloud computing which restricts the users' illegal access of the data that has been uploaded. The actors in the cloud computing can be classified as data owner, user and the cloud server. Data owner outsources the data after encryption to the cloud service provider for storage. When the data owner or any user is in need of the data, they both have to be authenticated by the cloud server.

2. Authentication mechanisms

Password based authentication is one way of one-factor authentication. It is considered to be the weakest link used to access a cloud based application because users can easily tamper the passwords. The declination of the security of password-based mechanisms is premeditated as an outdated technology due to its failure in performance against the perils on the internet. This paved a way to develop as strong and resilient mechanisms, and concurrently providing a means to develop new authentication schemes namely Multi Factor Authentication (MFA) Schemes [2]. Securing access with Multi Factor Authentication

MFA Can be done in two phases namely

1) Identification phase.
2) Authentication phase.

Identification Phase:

In this phase, the identity of the end user has to be determined. It is a straightforward technique since the user has to provide his or her identity in terms of the unique user name.

Authentication Phase:

Security is added more to the process through the authentication phase. Here the user has to provide the original proof for the identity that has been claimed by the user. Various authentication techniques have been implemented to prove the proofs of identity. It can be classified into three categories:

1) Something the user knows: This mechanism is a secret bond between the user and system.
2) Something the user has: This technique verifies for the identity that has been shown as a proof. This involves a token that entails the user to press a button to receive a code to be entered into the authentication system. Examples of techniques can be smart cards and physical keys.
3) Something the user is: This mechanism measures various biometric characteristics like finger prints, hand geometry, facial patterns etc .The characteristics of the user are compared with the authentication database to find out whether the user is a legitimate user.

Knowledge-based authentication mechanisms are inexpensive, easy to implement and familiar to end users. Device-based approaches eradicate the risk of a fraud and the legitimate user having access at the same time, because only one person can own the token or smart card at a time. The theft of the authentication device could lead to the impersonation of the user until the device is discovered. Biometric systems are quite expensive and some end users feel that the physical aspect involved invades their privacy. In order to maintain the balance between these advantages and disadvantages, certain organizations seek a high level of security

that could combine multiple authentication schemes to assure a high level of confidence regarding an end user's identity. This approach is known as multifactor authentication because it combines techniques from two or more of the identity authentication categories.

A Service provider attracts the consumers to use their service by exploiting the specialized features they provide. Communication between the consumer and the service provider gets initiated through the service level agreements.

3. Related works

A remote user authentication scheme proposed by Lamport uses the server for storing the hash value of the user's password for later verification [3]. Hwang et al found that the whole system could be invalid if the password table was modified [4]. Hence they devised a new authentication scheme that uses smart card.

This scheme works on the basis of ElGamal's public cryptosystem and there is no need for the scheme to maintain a password table for user authentication. But this scheme was not able to resist impersonate attack because any user could take off the other user's ID and PWD without the secret key. An efficient password based remote user authentication scheme proposed by Chien et al states that there are many advantages like mutual authentication, freely choosing password, absence of verification table and only less hashing operations[5]. In spite of all these advantages this scheme is said to be vulnerable to attacks like reflection attack, insider attack. In 2010, Chen and Huang formulated a scheme combining CAPTCHA and visual secret sharing [6]. But this scheme was not efficient since smart card might be exposed and raises masquerading attack.

Nowadays, many research works have been focused on the security, since it is considered to be the most prominent challenge in this cloud computing world. Among the various security issues, some of the noteworthy and recent research is included which primarily focus on the authentication phase of cloud security.

This paper presents few research directions and approaches that have been set forth which assist the researches to think about a new dimension in this area. A comparison of the authentication schemes along with the research directions is shown in the tabular column given below.

S.No	Method/Scheme/Framework	Technology used for authentication
1	Analysis and Improvement of User Authentication Framework for Cloud Computing	Smart card is used. Messages are hashed and sent.
2	Authentication in the Clouds: A Framework and its Application to Mobile Users [7]	User behavior is translated into authentication scores.
3	Consolidated Authentication Model[8]	Credentials are uploaded and downloaded. Two servers namely credential server and signing server are used.
4	A Strong user authentication framework in cloud computing[9]	Identity management, mutual authentication, session key establishment between the users and the Cloud server.
5	User Authentication Platform using Provisioning in Cloud Computing Environment[10]	User authentication is done through user profiles.
6	Secure Password by Using Two Factor Authentication in Cloud Computing[11]	Adopts 2FA and anonymous password. Privacy preservation of password is done.
7	Multi-dimensional password generation technique for accessing cloud services[12]	Confidential inputs like logos, images, textual information and signatures etc are used to generate the multi-dimensional password.
8	Multi-dimensional and Multilevel authentication techniques [13]	Concatenation of passwords is done at various levels. Passwords are entered at each level and privileges are granted. Resources corresponding to that level are granted.
9	Context-aware Platform for User Authentication in Cloud Database Computing[14]	Context-aware platform for user authentication in Cloud computing is proposed.
10	A Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing [15]	Mutual authentication between the server and the client. Time bound tickets.
11	Enhanced Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing [16]	Mutual authentication is done. Password and hashing functions are used. All this are done in smart card.
12	Authentication techniques in cloud and mobile cloud computing environments[17]	Categorization based on its input, i.e. the credentials required for validating users is done
13	mutual authentication [18]	To detect the attack being initiated by the attacker by placing his virtual machine close to the legal virtual machine

The CSP has to authenticate the remote users before a request has been put forth for accessing any kind of service. Hao et al. proposes a time-bound ticket based mutual authentication scheme for cloud computing [15].

This scheme resists against lost smart card attacks, offline password guessing attack, lost ticket attack, masquerade attack and replay attack. The special characteristic in this paper is mutual authentication and secure session key generation. In addition to this additional feature, the proposed scheme is exposed two drawbacks namely Denial-of-Service attack due to lack of early wrong password detection prior to verification request creation and insecure password change. It is assumed that the attacker is able to intercept the messages between the user and the server. Pippal proposed an enhanced version of Hao's proposal in such a way that the proposed protocol resists against the Denial-of-Service attack and the password can be changed without any assistance from the cloud server in a secure manner [16]. It is clearly understood that all the existing authentication mechanisms works only towards the verification of the claimed identity of an entity. Many of the existing authentication schemes check only whether the user is legitimate user and concentrates only on verifying the identity of the user. Pippal's scheme overcomes the flaws raised in hao's scheme. Mutual authentication and session key generation is provided in this scheme. Time and tickets raised for data verification is fixed in this method. But when the user faces any issue during the service and when the service provider requires user's permission to enter into the rented area, then this authentication schemes becomes weak.

4. Analysis of security mechanisms

The most important aspects of security that the cloud provider should address to the users are Confidentiality, Availability, Integrity, Authentication and SLA. This work addresses a list of service providers and their authentication mechanisms.

In addition to services like IaaS,PaaS and SaaS, there are many services provided by the service providers. Security solutions have been devised and they are provided in terms of Security-as-a-Service (SEaaS) which is a new instance of a cloud service model.

Among the various services that are available in different forms, Authentication-as-a-Service (AaaS) is considered as the predominant factor among the variants. In order to reduce the risk of compromising sensitive information, AaaS is issued.

The below comparative analysis of some of the authentication schemes implemented in cloud and these schemes are compared based on resistance to various attacks have been discussed and shown in the below table.

Provider	Service Provider	Technology	Description
PaaS	Amazon Web Services	Multi-Factor Authentication	It request for username and password (what they know). Further, it asks for an authentication code from their AWS MFA device (what they have).
	Salesforce	Single Sign-on	Username and password
	Microsoft Azure	Multi--Factor Authentication	It requires any two or more of the following verification methods: 1) Something you know (a password). 2) Something you have a trusted device that is not duplicated. 3) Something you are(biometrics)
	GAE	Single Sign-on	Username and password
IaaS	AT & T	2FA	First factor: Username and password Second factor: Hardware or Software token
	GOGRID	Token based authentication	
	Joyent	2FA	First factor: Username and password Second factor: Hardware or Software token
SaaS	NetSuite	2FA	First factor: Username and password Second factor: Hardware or Software token
	Workday	Single Sign-on with MFA	SAML Authentication
	Cornerstone	User Authentication	Certificate-Based Authentication

S. No	Authentication Mechanisms	Attacks
1	Authentication using smart card	Physical tampering. Key and Memory reading
2	Consolidated Authentication Model	Credentials might be hacked
3	A Strong user authentication framework in cloud computing	Password verification is done locally
4	Authentication in the Clouds: A Framework and its Application to Mobile Users	Chances for theft of user credentials,
5	User Authentication Platform using Provisioning in Cloud Computing Environment	Theft of credentials like time and place of user. Accessing the location of the user also might be misused.
6	Secure Password by Using Two Factor Authentication in Cloud Computing	Theft of mobile device
7	Multi-dimensional password generation technique for accessing cloud services	Generation of password at various lead to overhead
8	Multi-dimensional and Multilevel authentication techniques	Memory space required is more
9	Context-aware Platform for User Authentication in Cloud Database Computing	Personal information stored might be available for misuse.
10	A Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing	offline password guessing attack, lost ticket attack, masquerade attack and replay attack
11	Enhanced Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing	Lost ticket attack

5. Conclusion

Various security schemes are proposed for cloud environment and most of the schemes were well adopted in entry level authentications. Time bound ticket based mutual authentication is one such a scheme which provides security feature in the access layer. The mutual authentication scheme in cloud is mainly designed to enhance the customer satisfaction and improves the level of commitment by the service provider. There are a number of security issues with cloud computing in both the sides known as cloud service
provider (CSP) side and customer/client side. From the detailed comparative analysis and existing authentication schemes it is understood that the general cloud policy insisted that this responsibility should be held by CSP and as well as the consumer. This could be implemented by designing an authentication framework which concentrates on providing security throughout the service rendering period. In addition to that, SLA could also be revised and it could be bound with the authentication framework.

References

[1] NIST Definition. [Online]. Available: www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf Cloud Computing services & comparisons. [Online]. Available: http://www.thbs.com/downloads/Comparison of Cloud computing services.pdf.

[2] Sabout Nagaraju, Latha Parthiban, SecAuthn: Provably Secure Multi-Factor Authentication for the Cloud Computing Systems", Indian Journal of Science and Technology, Vol 9(9), March 2016.

[3] L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 770–772, 1981.

[4] M. S. Hwang and L. H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28-30, 2000.

[5] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," Computers and Security, 21(4):372–375, 2002.

[6] T. H. Chen and J. C. Huang, "A novel user-participating authentication scheme," The Journal of Systems and Software, 83(5):861–867, 2010.

[7] Chow, Markus Jocobsson, Ryusuke Masuoka, Jesus Molina, Yuan Niu, Elaine Shi, Zhexuan Song, "Authentication in the Clouds, A

Framework and its Application to Mobile Users. CCSW'10, October 8, Chicago, Illinois, USA, 2010.
[8] J. Kim and S. Hong, 2011. One-Source Multi-Use System having Function of Consolidated User Authentication, YES-ICUC, 2011.
[9] Choudhury, A.; Kumar, P.; Sain, M.; Lim, H. and Hoon Jae-Lee, "A Strong User Authentication Framework for Cloud Computing", Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, pp.110-115, 12-15 Dec. 2011.
[10] Hyosik Ahn, Hyokyung Chang, Changbok Jang, Euiin Choi," User Authentication Platform using Provisioning in Cloud Computing Environment", ACN : Advanced Communication and Networking pp 132-138,2011.
[11] Z. Shen, L. Li, F. Yan, X. Wu, 2010. Cloud Computing System Based on Trusted Computing Platform.International Conference on Intelligent Computation Technology and Automation (ICICTA). vol 1, pp 942-945,2010
[12] Quorica, 2009. Buisness Analysis Evolution of Strong Authentication, September 2009.
[13] Tanvi Naik, Sheetal Koul," Multi-Dimensional and Multi-Level Authentication Techniques", International Journal of Computer Applications (0975 – 8887) Volume 75– No.12, August 2013.
[14] Manjea Kim, Hoon Jeong, Eulin Choi, "Context-aware Platform for User Authentication in Cloud Database Computing", International Conference on Future Information and Technology and Management Science and Engineering, Lecture notes in Information Technology, Vol 14,2012.
[15] Hao, Z., Zhong, S. and Yu, N. "A timebound ticket-based mutual authentication scheme for cloud computing", International Journal of Computers, Communications and Control, 6(2), pp. 227–235,2011.
[16] Ravi Singh Pippal, Jaidhar C. D. Shashikala Tapaswi," Enhanced Time-Bound Ticket-Based Mutual Authentication Scheme for Cloud Computing", Informatica 37, 149–156, 2013.
[17] Mahamudul Hasan , Md. Hasnat Riaz , Md. Auhidur Rahman," Authentication Techniques in Cloud and Mobile Cloud Computing", IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.11, November 2017.
[18] Amit Verma, Megha Mittal, Bharti Chhabra, "The Mutual Authentication Scheme to detect virtual side channel attack in cloud Computing", International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 3, March 2017.