Critical Review of Authentication Mechanisms in Cloud Computing

S.Ziyad[1] and S.Rehman[2]
Department of Information System
Salman bin Abdul Aziz University, KSA

Abstract

Cloud computing is a technology, which provides low cost, scalable computation capacity and a stack of services to enterprises on demand for expansion. The complications caused by data security and privacy are the main hindrances in its acceptance. Threats in Cloud computing can be faced by adopting various security measures. One such security measure is authentication. In recent years a lot of research has been carried out throughout the world and several schemes have been proposed to improve authentication in the Cloud. Keeping in view the importance of authentication in cloud security, a survey of current cloud computing authentication trends has been conducted. On the basis of this critical review, we identify the areas of cloud computing authentication that indeed warrant further investigation.

Keywords:*Authentication Methods, Cloud Computing, Cloud Security, Data Authentication, Consolidated Authentication Model, Multimodal Biometric.*

1. INTRODUCTION

The Cloud Computing paradigm is now emerging as one of the new technologies, with companies of all sizes accessing the Cloud. As cost efficiency, unlimited storage, backup and recovery, automatic software integration, easy access to information stand out as advantages, security issues stand out as the major disadvantages of this new technology. Companies big or small,before leaping into the Cloud demand a secure Cloud. The Cloud has many security issues as it coordinates many technologies like networking, virtualization, memory management and database management. In Cloud security, authentication is the most important factor. In cloud computing still there is a need for well-defined authentication mechanisms. One of the first steps toward securing an IT system is to verify the identity of its users. The process of verifying a user's identity is typically referred to as user identification and authentication [1](NIST,2010). Authentication is generally referred to as a mechanism that establishes the validity of the claimed identity of the individual. There are basically four kind authentication methods:

a. Something an individual KNOWS (e.g. password, Personal ID)

b. Something an individual POSSESSES (e.g., a token or card)

c. Something an individual IS (e.g. fingerprint or voice pattern)

d. Something an individual DOES (e.g. history of Internet usage)

Recently many security researchers are focusing on various new techniques of authentication in cloud computing that include one or more of the above mentioned methods of authentication. Therefore it becomes inevitable to survey the various authentication methodsrecently proposed and implemented in the Cloud computing environment.

The rest of the paper is organized as follows. Section 2 discusses recent trendsin cloud computing. Section 3 coversthe need for strong authentication in the Cloud; section 4 surveys the recently proposed mechanisms for authentication models in cloud; in section 5 the summary and future workare covered.

2. RECENT AUTHENTICATION TRENDS IN CLOUD COMPUTING

A number of researchers are working to find strong authentication methods for cloud computing. Anumber of authentication methods are in practice. In this section, a critical review of various research work is carried out. To simplify the review, new approaches are divided into different categories. In each category, current practice and recent research are discussed.

2.1 Authentication Frameworks, Models and Architectures

In the last decade,much development has taken place in the field of authentication models. A number of frameworks, models and architectures have beenproposed by researchers. Some of the prominent works in this area are covered in this section.One of the authentication architectureswas proposed by Chow et al.[2]. The architectureis based on the method “what an individual does.” They proposed an implicit authentication method for mobile users. This authentication architecture is based on the history of the websites that the user visits. On one hand it is convenient and easy to use, on the other hand it cannot be used as a replacement for regular authentication in high-risk sectors, like banking. In another prominent research by Z.Shen et al. [3], a theoretical prototype systemwas proposed in which the Cloud computing system is secured along with the trusted platform support services. Celesti et al. [4] proposed a reference architecture to address the identity management problem for Cloud computing.As the next development in research a new method of authentication was proposed that implemented mobile Out Of Bound authentication on the Public Key Infrastructure during the login phase.Lee. Et al [5, 2010]presented a scheme where Public key infrastructure is implemented. PKI is a collection of hardware, software, policies, procedures and people working together.The Consolidated Authentication Model (CAM) proposed by Kim and Hong[6, 2011]not only provides a more flexible authentication framework but also leads to safer credential management in operating various m devices such as smart phone, smart pad, etc.The disadvantage of this method is the absence of secure credential protocol.

Cloud computing handles a large community of clients.Jyoti[7, 2011] proposes the strong authentication model rather than the traditional client-server authentication model. The user inserts a smart card in a terminal and enters the user ID and password. The local terminal checks the validity of the card and based on the results, sends a login request to the Cloud server generates a onetime key and sends it to the user's mobile. The user sends the user ID, password and one time key to the server, which in turn authenticates the client. This authentication framework has advantages such as identity management, mutual authentication, session key agreement between the users and the Cloud server, and user friendliness (i.e. password change phase).

An improved mutual authentication framework has been proposed by Kumar et al., [8, 2012]. In their research they proposed a scheme in which there are three phases. In the first phase the secret key initialization is made by the service provider to the user. In the second phase the user is registered by double authentication. In the third phase authentication is done using a nonce. The proposed scheme can also resist many attacks such as password stolen, replay attack, etc.

There are some cases that need to use anonymous authentication in cloud computing. In such cases the user does not want to reveal their identity, they just want that service providers know that they are legitimate users. Zhang zhi-hua[9,2012] authors solve this problem by proposing a non-authentication certificate anonymous scheme.The scheme proposed is based on the computationalDiffie-Hellman problem (CDHP).The scheme presented does not have a certification center and it avoids the key Revocation and the key escrow problems in the authentication schemes based on public key certificate.

Identity authentication can't stop the malicious behavior of legitimate users, therefore authenticating the trustworthiness of cloud user behavior is important in protecting the cloud. Junfeng and Xun[10,2013]presented Cloud Behavior Analytic Hierarchy Process (CBAHP). The proposed process is a combination of AHP and cloud user behavior, and they put forward BAM, a cloud user behavior authentication model based on multi-partite graphs. It can effectively distinguish between malicious users and genuine users, and has a low False Positive Ratio.

It is essential to understand the relationships between various aspects of authentication. Gonzalez[11,2013] proposes a framework for studying and developing a relationship between cloud deployment models, service types, entities and lifecycle controls.The patterns of previous privacy leaks can also be used in preventing the new authentication attacks in cloud computing.Mohammad Farhatullah[13,2013]proposed the combination of authentication procedure and privacy leak detection to ensure the privacy of sensitive information stored by the users in the cloud. They try to solve the issue of privacy preservation by authentication for redacted trees that uses the previous privacy patterns.

Banyal et al. [14], in their paper, proposed a new multi-factor authentication framework for cloud computing. Their framework provides a mechanism that can closely integrate with the traditional authentication systems. The framework is verified by Cloud Access Management (CAM) system which authenticates the user based on multiple factors. Also they implemented a prototype model for cloud computing.

2.2 Passwordsand Smart Card based Authentication

In the 'Something an individual POSSESSES' categorythe basic authentication technique is tokens. Tokens for authentication come in basic two forms – hardware and software. These tokens are used in common appliances such as mobile phones. Hardware tokens are physical devices that generates one time passwords and whose validity lasts only for single authentication event. The main disadvantage is the cost of distribution and security. Software tokenarises as a solution to the problems raised by hardware tokens.

In distributed servers, EAP-TLS server smart cards offer security and the simplicity. Urien et al.[15,2010] in their research proposed a paradigm based on a grid of smart cards built on a context of SSL smart cards. They presented the scalability of the server linked to smart card grids whose distributed computation manages the concurrence of numerous authenticating sessions.

Software tokens are incooperated into laptops and desktops. Quorica [16,2009] - intelligent software tokens are used with smart phones and USB devices. Their popularity is due to the fact that these tokens need not be carried and kept safe like hardware tokens. An alternative to the software token is the demand token, which is a onetime password entered into an application for authentication.The technique presented by DineshaandAgarwal[17] proposes generation of password by concatenating passwords at multiple levels. Authentication takes place at different levels-organization, team and user levels. At the user level, it authenticates the user's privileges to access a particular Cloud resource. Advantage of this technique is that it uses a multilevel approach. It is quite difficult to break multilevel security as compared to single level. The disadvantage of this method is that there is a risk of a password being hacked through social engineering and other non-technical attacks.

To reduce the administrative overhead due to multiple logins and passwordAshish et al. [18, 2011]proposed a single sign-on scheme as a means of authentication in cloud environment. A single authentication allows the client to gain access to all the resources. This SSO is implemented in the cloud architecture's top layer.In this scheme the Authentication Server is the main component that provides single sign on. This enhances the reliability,adaptability and feasibility of the Cloud.Zhongjian Le et al.[19,2011] proposed a system for protecting cloud from IP prefix hijacking.This scheme has authenticated origin autonomous system using self-certified public keys.It defends the system against all types of prefix and MKI (Malicious Key Issuer) hijacking by protocols.

L. B. Jivanadham [20, 2013]proposed an authentication scheme known as cloud cognitive authenticator(CCA).It applies one round zero knowledge protocol (ZKP) for authentication. CCA is an API designed for cloud environment that integrates bio-signals, ZKP and Rijndael's algorithm.CCA improves security in a public cloud by providing bi-level authentication. It also provides encryption and decryption of user ids.Electro dermal responses are used for first level authentication. The main advantage of CCA compared to other existing models is that it provides two levels of authentication combined with the encryption algorithm.

2.3 Biometric Authentication Methods

Bio-metric authentications are getting more popular day by day in the critical security systems. Biometric techniques depend on the user's personal characteristic. The common bio-metric scheme includes fingerprints, voice recognition, face recognition,palm prints, hand geometry, retina recognition. Each biometric recognition scheme can be analyzed on the basis of several factors such as time, consistency, acceptability, uniqueness, number of false alarms etc. The main drawback of these schemes is the requirement of a special scanning deviceto authenticate users, which is not applicable for remote and Internet users. Exhaustive research is carriedoutinorder to simplify biometric authentication methods for cloud user. Some of the prominent research works are discussed here.

In the field of voice-based biometric authentication, Zhu. et al.[21,2011]proposed a novel approach in which a voiceprint template for authentication was used. The authentication system is performed in two stages. First 'the enrolment phase' and second'the matching phase'. This method only uses the biometric trait to authenticate the user. A preferable model is to employ both the traditional password and biometric trait for authenticating the Cloud clients.In the field of fingerprint recognition, Wang,[22, 2011] proposed a system based on secret splitting of finger print biometric data. In their approach they divided and stored part of finger print data on smart card and part of it on the server. This makes attack more difficult as attacker needs to break two keys rather than one.

Another biometric method in cloud computing is the face recognition.Pawle and Pawar [23,2013]in their method, on entering the username, user's face is captured as a password by web camera. The technique is divided into four steps i).face capture, ii).face detection, iii).alignment and iv).feature extraction. This technique is simple and easy to implement but essential fact is the need for the camera. The other drawbacks are that the face features may differ depending on lighting conditions, time of the day, presence of accessories on the face, beards, deformities due to medical conditions, and the most important is the change in face dimensions due to aging. When mobile phone cameras are used, external conditions like lighting increases the error rate too much due to which Android facial recognition fails in 30-40% cases [24].

Wang et al. [22] proposed an enterprise-based gateway integrated with a Multi-factor authentication solution for secure authentication in Cloud. Security gateway is an identity provider and starts the single sign on process. The authentication process is carried out by credentials, nonce generated and finally by the multibiometric data. The credentials are verified by credential directory and multi biometric data by biomex server.

3. RESEARCH DIRECTIONS IN CLOUD COMPUTING AUTHENTICATION

With the growing popularity of cloud, companies are investing heavily in the research of cloud computing security. In this paper some of the significant and latest research is included which mainly focus on the authenticationphase of cloud security. After the thorough review of literature in cloud computing authentication, some new directions and approaches are set forth that can facilitate the researchers in this area. The distribution of our approach of study is shown as in fig. 4.1

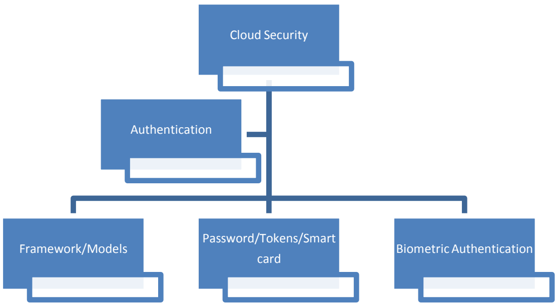

Fig. 4.1 Research directions in the field of cloud computing security

Some of the prominent future research directions are shown in table 4.2

Table 4.2 Prominent researches in Cloud Computing Authentication with their advantages, disadvantages and future researches

Method /Scheme	Year	Advantages	Disadvantages	Future Directions
Authentication in the Clouds: A Framework and its Application to Mobile Users [2]	2010	Authentication is done on the clients' behavior hence theft of the device is not a threat.	Authentication score is checked against a certain threshold. Hence a best result depends on application.	The flexibility of the system provides support to latest and evolving Cloud authentication systems.
Two Factor Authentication [3]	2010	It is robust and efficient against phishing and replay attacks.	Theft of mobile phone leads to breach of security.	Need to design a system that will authenticate the user with the feature other than possession of Mobile phone.
A strong user authentication framework for cloud computing [7]	2011	Identity management, Mutual authentication and Session key agreement.	Password and smartcard Verification is done by the local system. Performance unknown.	Providing formal security proof.
Consolidated authentication model [6]	2012	Secure protocols allow the credentials to freely roam in cloud computing environment.	Credential store is the repository for credentials, posing serious threat of being hacked.	Design and implementation of the proposed scheme.
Single Sign On[17]	2011	Central server supplies credential to the application server. Hence no multiple authentication for different applications	If the central server is hacked then entire server is hacked.	Security measures for central authentication server to be reviewed.
Multidimensional Password Generation[16]	2012	Multiple levels of authentication	Overhead is more in multilevel authentication	Security levels need to be strengthened.
Voiceprint biometric authentication[20]	2011	The algorithms make the voiceprint data invertible.	Size of codebook database depends on number of users. Hence increase in number of users causes an increase in the overhead.	More efficient homomorphic algorithms together with more reliable biometric feature can be implemented for secure Cloud.
Remote authentication on secret splitting [21]	2011	Three factor authentication makes system secure from network attacks and authentication factor attacks.	Biometric data matching is done at the terminal. There is a threat of the template leakage	More recent trend of biometric trait could be used for authentication. Match on card technology can be implemented.
Face Recognition System (FRS) on Cloud Computing for User Authentication[22]	2013	This technique is simple and easy to implement.	It will not work in the absence of camera also face features might become different depending on lighting conditions, time of the day etc.	Work can be done in the direction of removing its limitations such as face recognition after ageing, makeup, jewelry.
ALP: An Authentication and Leak Prediction Model for Cloud Computing Privacy by [12]	2013	It solves the issue of privacy preservation by authentication & confidentiality approach for redacted trees that uses the previous privacy patterns.	The approach is based on the previous information, so it cannot cover new attack patterns.	In this approach the clustered documents are organized as trees. However, there is a possibility of extending the same approach to graphs and forests as well.

4. CONCLUSION

The paper witnesses the evolution of authentication. It shows the development from the usage of hardware tokens to multi modal biometrics to authenticate the client. Research is still in progress finding new methods and schemes to authenticate the user in order to challenge the security threats faced by the Cloud. These newapproaches by various researchers offer a good foundation for further research and development in the field of Cloud security.

REFERENCES

[1] NIST Computer Security Handbook,http://csrc.nist.gov/publications/nistpubs/800-12/

[2] Chow, Markus Jocobsson,RyusukeMasuoka, Jesus Molina, Yuan Niu, Elaine Shi, Zhexuan Song, "Authentication in the Clouds, 2010.A Framework and its Application to Mobile Users. CCSW'10, October 8, 2010, Chicago, Illinois, USA.

[3] 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). 2010 ,vol 1, pp 942-945.

[4] A. Celesti, F. Tusa, M. Villari, APuliafito, 2010. Security and Cloud Computing: InterCloud Identity Management Infrastructure. 19th IEEE International Workshop onEnabling Technologies: Infrastructures for CollaborativeEnterprises (WETICE), 2010 , pp 263-265.

[5] S. Lee, I. Ong, H.T. Lim, H.J. Lee, 2010.Two factor authentication for Cloud computing. International Journal of KIMICS, August 2010, volume8, pp. 427-432.

[6] J. Kim and S. Hong, 2011. One-Source Multi-Use System having Function of Consolidated User Authentication, YES-ICUC, 2011.

[7] AmlanJyotiChoudhury, PardeepKumar,MangalSain, Hyotaek Lim, Hoon Jae-Lee, 2011. A Strong User Authentication Framework for Cloud Computing. Asia - Pacific Services Computing Conference, 2011, IEEE.

[8] Sanjeet Kumar Nayak,SubasishMohapatra,BanshidharMajhi, 2012.An Improved Mutual Authentication Framework for Cloud Computing.International Journal of Computer Applications, Volume 52, issue. 5, August 2012.

[9] Zhang zhi-hua, Li jian-jun, Jiang Wei, Zhao Yong Gong Bei1, 2012. An New Anonymous Authentication Scheme for Cloud Computing. The 7th International Conference on Computer Science & Education (ICCSE 2012), July 14-17, 2012. Melbourne, Australia

[10] (Junfeng and Xun, 2013)TianJunfeng and Cao Xun, “A Cloud User Behavior Authentication Model Based On Multi-partite Graphs”, Third International Conference on Innovative Computing Technology (INTECH), 29-31 Aug. 2013,London, Pages 106 – 112.

[11] Nelson Mimura Gonzalez, Marco Antônio Torrez Rojas, Marcos ViníciusMaciel da Silva, Fernando Redígolo, Aframework for authentication and authorization credentials in cloud computing.12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[12] Tereza Cristina Melo de BritoCarvalho, Charles Christian Miers, Mats Näslundand Abu Shohel Ahmed, 2013. A framework for authentication and authorization credentials in cloud computing. 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[13] Mohammad Farhatullah, 2013. ALP: An Authentication and Leak Prediction Model for Cloud Computing Privacy. 3rd IEEE International Advance Computing Conference (IACC), 2013.

[14] Rohitash Kumar Banyal, Pragya Jain, Vijendra Kumar Jain, 2013. Multi-factor Authentication Framework for Cloud Computing. Fifth International Conference on Computational Intelligence, Modeling and Simulation, IEEE, 2013.

[15] Pascal Urien , Estelle Marie, Christophe Kiennert, 2010. An Innovative Solution for Cloud Computing Authentication: Grids of EAP-TLS Smart Cards. Fifth International Conference on Digital Telecommunications, 2010.

[16] Quorica, 2009. Buisness Analysis Evolution of Strong Authentication, September 2009.

[17] Dinesha H A, 2012. Multi-level Authentication Technique for Accessing Cloud Services. International Conference on Computing, Communication and Applications (ICCCA), IEEE, 22-24 February 2012, pp 1-4.

[18] Ashish G. Revar, Madhuri D. Bhavsar, “Securing User Authentication using Single Sign-On in Cloud Computing, 2011.International Conference on Engineering (NUiCONE), 2011, Nirma University.

[19] Zhongjian Le,NaixueXiong, Bo Yangand YuezhiZhou ,2011. SC-OA: a Secure and Efficient Scheme for Origin Authentication of Interdomain Routing in Cloud Computing Networks.IEEE International Parallel & Distributed Processing Symposium.

[20] L. B. Jivanadham, A.K.M. MuzahidulIslam YoshiakiKatayam, Cloud Cognitive Authenticator (CCA) A Public Cloud Computing Authentication Mechanism, 2013, IEEE.

[21] Hua-Hong Zhu, Qian-Hua He, Hua-Hong Zhu, Hong Tang, Wei-Hua Cao, 2011. IEEE international Conference on Cloud and Service Computing on Voiceprint-Biometric Template Design and Authentication Based on Cloud Computing Security.

[22] Wang, P., Ku, C. C., & Wang, T. C., 2011.A New Fingerprint Authentication Scheme Based on Secret-Splitting for Enhanced Cloud Security. www.intechweb.org.

[23] Akshay A. Pawle, Vrushsen P. Pawar, 2013. Face Recognition System (FRS) on Cloud Computing for User Authentication. International Journal of Soft Computing and Engineering (IJSCE), Volume-3, Issue-4, September 2013.

[24] http://blog.kaspersky.com/biometric-authentication.

First Author: Shabana Ziyad is working as a lecturer in Salman Bin Abdul Aziz University, KSA. She has an undergraduate degree in applied sciences and Masters in Computer Application from P.S.G college of Technology, Coimbatore, India. Her research interest includes Biometric Authentication and Cloud Computing. She has a number of research papers in the field in Cloud Computing.

Second Author: Shabana Rehman is working as lecturer in Salman Bin Abdul Aziz University, KSA.She did her Ph.D in computer Science from JamiaMillia Islamic in 2012 and completed her Masters in Computer Application in 2007. Her research interest includes computer security, software engineering and cloud computing. She has number of research papers in the field of software security, software engineering and cloud computing.