International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Serious Assessment of Substantiation Mechanisms in Cloud Computing

T.Lakshmi narayanan	M.Lakshmi
Assistant – professor department of computer science Periyar University College Of Arts And Science College Mettur Dam, Selem ,Tamil Nadu	Assistant – professor Department of computer science Bharathidasan University College Of Arts And Science College For Women Orthanadu, Thanjavur, Tamil Nadu

Abstract

The Cloud computing is a equipment which provide squat cost scalable computation competence and a stack of services to endeavor on demand for increase. The impediment caused by data defense and seclusion are the main hindrances in its reception. Threats in Cloud computing can be faced by adopting a mixture of security measures. One such security measure is authentication. In topical 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 in progress cloud computing authentication trends has been conduct on the basis of this significant review, w identify the areas of cloud computing authentication that indeed demand further investigation.

Keywords: *Authentication method, cloud computing, cloud security ,Data authentication*

1.Introduction

The Cloud Computing example is now up-and-coming as one of the new technology, with company of all sizes access the Cloud. As cost competence, unlimited storage, backup and mending, automatic software combination, easy access to in sequence stand out as recompense, safekeeping issues stand out as the most important disadvantages of this new technology. Company big or small, before leap into the Cloud stipulates a secure Cloud. The Cloud has loads of security issues as it coordinate many technologies like networking, virtualization, memory

administration and database managing. In Cloud security, authentication is the most important factor. In cloud computing at a halt there is a need for well-defined authentication mechanisms. One of the first steps toward securing an IT system is to verify the self of its users. The process of verifying a user's identity is typically referred to as user detection and authentication [1](NIST,2010). Authentication is by and large referred to as a mechanism that establishes the validity of the claimed characteristics of the personality. There are fundamentally four kind authentication methods:

a. impressive an personage KNOWS (e.g. password, Personal ID)

b. incredible an entity POSSESSES (e.g., a token or card)

c. impressive an character IS (e.g. fingerprint or voice pattern)

d. incredible an creature DOES (e.g. history of Internet usage)

Recently many defense researchers are focusing on various original techniques of authentication in cloud computing that contain one or more of the above mentioned scheme of authentication. Therefore it becomes foreseeable to survey the various authentication method recently projected and implemented in the Cloud computing atmosphere.

The respite of the paper is ordered as follows. Section 2 discusses current trends in cloud computing. Section 3 covers the need for muscular authentication in the Cloud; section 4 surveys the freshly proposed mechanisms for authentication models in cloud; in section 5 the outline and future vocation are covered.

2. Modern Authentication movement In Cloud Computing

A number of researchers are functioning to find brawny authentication methods for cloud computing. A quantity of authentication methods are in perform. In this section, a critical review of various do research work is carried out. To simplify the review, new approaches are at odds into different categories. In each category modern apply and topical researches are discussed.

2.1 Authentication Frameworks, reproduction and planning

In the last decade, much progress has taken place in the field of authentication models. A number of Frameworks, models and architectures have been proposed by researchers. Some of the important works in this part are covered in this segment. One of the authentication architectures was anticipated by Chow et al.[2]. The architecture is sanded on the process "what an character does." They proposed an inherent authentication method for mobile users. This authentication architecture is based on the narration of the websites that the addict visits. On one tender it is opportune and easy to use; on the other hand it cannot be used as a substitution for habitual authentication in high-risk sectors, like banking. In a different prominent research by Z.Shen et al. [3], a imaginary prototype arrangement was proposed in which the Cloud computing system is held along with the trusted podium support services. Celesti et al. [4] proposed situation architecture to talk to the identity supervision problem for Cloud computing. As the subsequently advance in research a new system of authentication was wished-for that implemented mobile Out Of Bound authentication on the Public Key Infrastructure for the duration of the login phase.Lee. Et al [5, 2010] existing a scheme where Public key infrastructure is implemented. PKI is a group of hardware, software, policies, procedures and natives working together. The Consolidated Authentication Model (CAM) proposed by Kim and Hong[6, 2011]not only provides a more bendable authentication framework but also leads to safer documentation supervision in operating various mobile devices such as elegant phone, smart pad, etc. The main shortcoming of this method is the nonexistence of secure documentation protocol.

Cloud computing handles a large population of clients. Jyoti [7, 2011] proposes the strapping authentication model rather than the established client-server authentication model. The user inserts a well-dressed card in a terminal and enters the user ID and password. The confined terminal checks the power of the card and based on the results, sends a login apply for 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 solution to the server, which in go round authenticates the client.

This authentication framework has reward such as identity supervision, communal authentication, assembly key concurrence between the users and the Cloud server, and user friendliness (i.e. password change phase).

A superior mutual authentication framework has been proposed by Kumar et al., [8, 2012]. In their examine they proposed a format in which there are three phases. In the first phase the underground key initialization is made by the check provider to the user. In the second phase the user is registered by two times authentication. In the third phase substantiation is done using a nonce. The proposed scheme can also refuse to go along with lots of attacks such as password stolen, replay attack, etc.

There are some cases that necessitate to use unsigned authentication in cloud computing. In such cases the user does not would like to expose their identity, they just want that service providers identify that they are justifiable users. Zhang zhi-hua[9,2012] authors explain this predicament by proposing a non-authentication documentation unsigned scheme. The idea proposed is based on the computational Diffie-Hellman setback (CDHP).The scheme presented does not have a qualifications center and it avoids the key Revocation and the key escrow problems in the authentication schemes based on communal key certificate.

Identity authentication can‟t impede the malevolent behavior of rightful users, therefore authenticating the responsibility of cloud user manners is important in shielding the cloud. Junfeng and Xun[10,2013]presented Cloud Behavior methodical Hierarchy Process (CBAHP). The proposed method is an arrangement of AHP and cloud user activities, and they put forward BAM, a cloud user behavior endorsement model based on multi-partite graphs. It can in effect discriminate between malicious users and indisputable users, and has a low False Positive Ratio.

It is critical to understand the relationships between choices of aspects of authentication. Gonzalez [11,2013] proposes a framework for studying and upward a relationship between cloud

consumption models, tune types, entities and lifecycle reins. The patterns of earlier privacy leaks can also be used in preventing the innovative authentication attacks in cloud computing. Mohammad Farhatullah [13,2013]proposed the mishmash of authentication course of action and time alone leak exposure to ensure the privacy of perceptive in turn stored by the users in the cloud. They endeavor to explain the issue of privacy defense by authentication for redacted trees that uses the earlier isolation patterns.

Banyal et al. [14], in their essay, proposed an original multi-factor authentication framework for cloud computing. Their framework provides a mechanism that can closely incorporate with the fixed authentication systems. The framework is demonstrated by Cloud Access Management (CAM) system which authenticates the user based on numerous factors. Also they implemented a prototype sculpt for cloud computing.

2.2 Passwords and elegant license based endorsement

In the “impressive a personality POSSESSES” sort the basic authentication procedure is tokens. Tokens for authentication come in central two forms – hardware and software. These tokens are used in familiar appliances such as mobile phones. Hardware tokens are a corporal device that generates one time passwords and whose power lasts only for sole authentication incident. The main disadvantage is the fee of distribution and safety measures. Software token arises as a way out to the problems raised by hardware tokens.

In circulated servers, EAP-TLS server smart cards bid security and the plainness. Urien et al.[15,2010] in their delve into proposed a paradigm based on a gridiron of smart cards built on a situation of SSL smart cards. They to be had the scalability of the server associated to smart card grids whose distributed subtraction manages the harmony of numerous authenticating sessions.

Software tokens are in cooperated into laptops with desktops. Quorica [16,2009] - intellectual software tokens are used with tidy phones and USB devices. Their regard is due to the truth that these tokens necessitate not be carried and kept safe and sound like hardware tokens. An substitute to the software token is the exact token, which is a onetime password entered into an function for authentication. The performance presented by Dinesha and Agarwal[17] proposes age bracket of password by concatenating passwords at various levels. Authentication takes place at different levels-organization, group and user levels. At the user level, it authenticates the user "s privileges to entrée a particular Cloud supply. Advantage of this performance is that it uses a multilevel draw near. It is relatively difficult to break multilevel safety measures as compared to single point. The disadvantage of this means is that there is a menace of a password being hacked through public engineering and other non-technical show aggression.

To diminish the secretarial overhead due to compound logins and password Ashish et al. [18, 2011] proposed a single sign-on method as a means of authentication in cloud atmosphere. A single authentication allows the client to gain contact to all the resources. This SSO is implemented in the cloud architecture top layer .In this proposal the Authentication Server is the main module that provides single sign on. This enhances the stead fastness, adaptability and probability of the Cloud. Zhongjian Le et al.[19,2011] proposed a classification for protecting cloud from IP prefix hijacking. This scheme has authenticated origin autonomous system using self-certified public keys. It defends the system adjacent to all types of prefix and MKI (Malicious Key Issuer) hijacking by protocols.

2.3Biometric validation process

Bio-metric authentications are being paid more popular day by day in the critical sanctuary systems. Biometric techniques depend on the user special attribute. The universal bio-metric scheme includes fingerprints, accent recognition, expression recognition, palm prints, hand geometry, retina recognition. Each biometric appreciation scheme can be evaluate on the

basis of a number of factors such as time, evenness, acceptability, uniqueness, number of counterfeit alarms etc. The main negative aspect of these schemes is the necessities of a special scanning deviceto authenticate users, which is not pertinent for far-off and Internet users. Meticulous research is carried out in order to make straightforward biometric authentication methods for cloud user. Some of the high-flying explore works are discussed here.

In the field of voice-based biometric authentication, Zhu. et al.[21,2011]proposed a novel come close to in which a voice print cut-out for authentication was used. The authentication system is performed in two stages. First "the enrolment phase" and second "the corresponding phase". This system only uses the biometric characteristic to authenticate the user. A preferable model is to occupy both the long-established password and biometric trait for authenticating the Cloud clients. In the field of fingerprint acknowledgment, Wang,[22, 2011] proposed a system based on surreptitious splitting of finger print biometric data. In their draw near they divided and stored element of finger print data on smart card and part of it on the server. This makes attack more complicated as attacker needs to shatter two keys rather than one.

An additional biometric method in cloud computing is the face recognition. Pawle and Pawar [23,2013]in their method, on incoming the username, user "s face is captured as a password by web camera. The procedure is divided into four steps i).face imprison, ii).face revealing, iii).placement and iv).feature drawing out. This technique is simple and effortless 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 revolutionize in face dimensions due to aging. When mobile phone cameras are used, outdoor 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 entryway integrated with a Multi-factor authentication clarification for safe and sound authentication in Cloud. Security gateway is an

character provider and starts the particular sign on progression. The authentication process is agreed out by credentials, nonce generated and to end with by the multi biometric data. The credentials are verified by documentation fact list and multi biometric figures by biomex server.

3.Research instructions in cloud computing confirmation

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 authentication phase 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

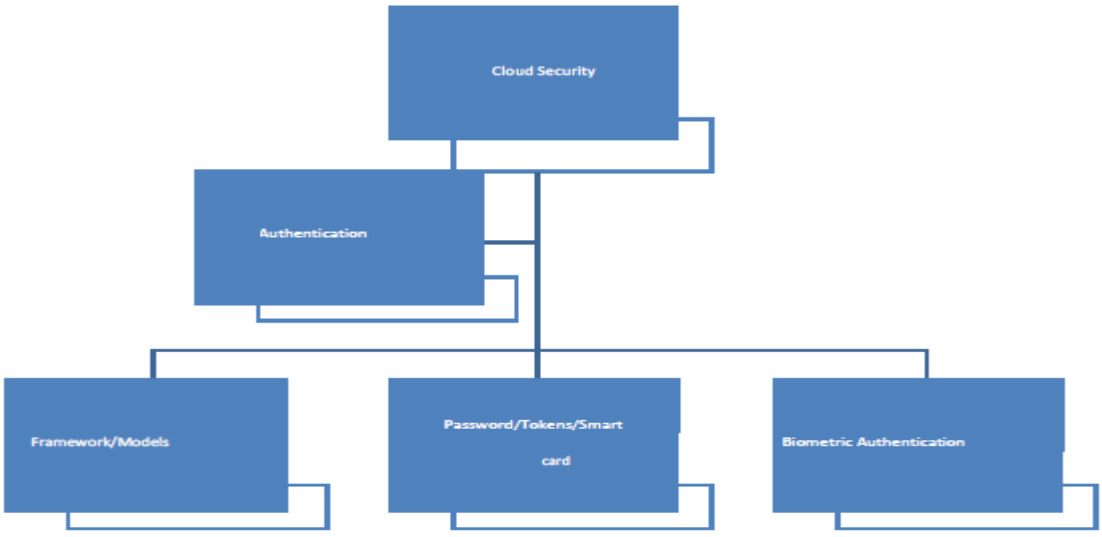

Fig4.1 Research directions in the field of clouding computing security

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.

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

(Prominent researches in cloud computing authentication with their advantages and disadvantages for future researches)

4. Conclusion

The paper witnesses the evolution of authentication. It has shown the development from the usage of hardware tokens to multi model 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 new approaches 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].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.

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

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

[6].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.

[7].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 (Junfeng and Xun, 2013)

[8].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.

[9].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.

[10].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.

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

[12.].S.Ziyad, S.Rehman 2013. Critical Review of Authentication Mechanism in Cloud Computing. International Journal of Computer Science(IJCSI), Vol.11, Issue 3, No 1,May 2014.