Volume 8, No. 2, March 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

A Review on Cloud Computing Security Using Authentication Techniques

Huma Farooq
Department of CSE, SEST
JamiaHamdard, New Delhi, India
huma.dahal@yahoo.com

Abstract:During the last two decades, the use of internet has been changing every domain of technology. It has also led to the tremendous development and implementation of cloud computing from the last few years. But the shared nature of data in the cloud makes it prone to security attacks. So different security techniques need to be implemented to prevent security breaches. Authentication is one such technique which plays a major role in Cloud Computing security. The various possible security attacks on the Cloud Service Providers (CSP) are prevented by applying different authentication mechanisms, which verifies a user's identity when a user wishes to request services from cloud servers. There are multiple authentication technologies for verifying the identity of a user before granting access to resources. In this research work, different possible authentication techniques are discussed. It is observed that biometric techniques are proving very helpful in implementing multi-factor authentication and one of the new biometric authentication techniques like palm print is being introduced as well.

Keywords:authentication; cloud computing; CSP; SSO; PKI.

I. INTRODUCTION

Cloud computing is a type of Internet-based computing for providing on demand access to shared computer processing resources, data, software, infrastructure, and platform resources which can be rapidly stipulated and released with minimal management effort. By providing different services it helps to extend capability of Information Technology (IT) [1].

The cloud computing model is composed of three essential service models and four deployment models. The three fundamental service models that are offered by cloud computing providers are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

SaaS: It is the topmost layer which provides software as a service through the internet. The customer does not need to manage the infra-structure of cloud including customer's operational systems, servers and saving area and there is no need to install and run the application on customer's own computers.

PaaS: It is the second layer which provides the sole (unshared) program environment, computing platform, developing and solution strategies.

IaaS: It is the bottommost layer that provides just the basic hardware and network components of computing infrastructure such as storage, CPU and memory; the customer installs or develops its own operating systems, software and applications. There is no need for the client to control or manage the infrastructure. An artificial server is made available for the client in this service [2].

The four different deployment models provide the basic platform for the operation of cloud services. Moreover, these models include the identity and aim of cloud. These models are discussed as:

Public cloud: It is a cloud computing model in which resources, such as e-mail services, online photo storage services, or social networking sites, are made available to the general public over the Internet by a service provider. On a pay-per-usage model, these services may be free or paid.

Private cloud: In this type of cloud computing, the cloud infrastructure is managed by the organization or a third party and is operated solely for a specific organization.

Community cloud: Here the cloud service is shared by several organizations or communities and made available only to those groups. The cloud infrastructure may be owned and operated by the organizations themselves or by a cloud service provider.

Hybrid cloud: Combination of different methods.

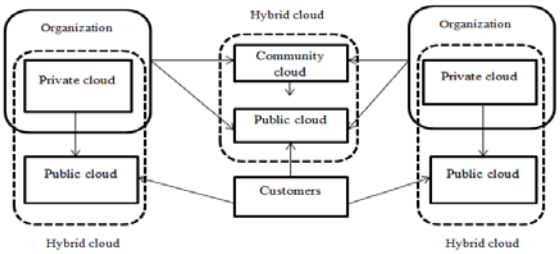

Figure 1: Cloud Computing Deployment Models

There are many advantages of cloud computing such as low cost storage and shared infrastructure. Besides these advantages, there are also many disadvantages. The most serious one being the data security of the cloud system that is due to the nature of outsourced computing or the shared nature of data. If a robust security scheme and a user-centric security policy is not implemented, the cloud system would be vulnerable to different attacks. There are three important factors of cloud security requirements. These are confidentiality, integrity and availability. These three factors are widely called as CIA. Confidentiality means protection of data from unauthorized disclosure. It depends on various factors such as encryption methods, Cloud Service Provider and length of key (in symmetric algorithm). Confidentiality plays an important role in cloud

computing by preserving control on organizations' data situated across multiple servers. Integrity is defined as the assurance that data received is as sent by an authorized entity i.e. no unauthorized person can fabricate, modify and delete sensitive information in cloud servers. Organizations can achieve greater confidence in data and system integrity by preventing unauthorized access. The objective of availability is to ensure that only authorized person can access to shared information in cloud service provider (any time and any place). Even if there is the possibility of a security breach, cloud servers must be able to continue operations. There can be various threats to availability with Denial of Service attacks (DOS) being the most popular one. Some other threats include natural disasters and equipment outages. As cloud computing is associated with having users' sensitive data stored both at client side as well as in the cloud servers, the concepts of confidentiality, integrity and authentication are very important areas that need to be taken care of in cloud computing. Various architectures have been presented that reduce the imminence of theft and decrease the misuse of shared data by the cloud service provider [3]. The privacy of the data can be managed and controlled by these methods in the cloudenvironment. Various security approaches of cloud infrastructure and their issues were studied and the aim of this research was to produce a strategy and enhance the security of cloud environment [4].

In cloud environment, authentication of user is an important factor, because it guarantees that the communicating entity is the one claimed. Many methods are being used to authenticate users in cloud computingenvironment. Single Sign On (SSO), username and password, multi-factor authentication, Mobile Trusted Module (MTM), Public Key Infrastructure (PKI), as well as biometric authentication are the main methods being used today. This study reviews various authentication techniques in cloud computing environment and these techniques are characteristically used to improve the security of Cloud computing. Followed in this paper, a brief explanation of different authentication techniques is given in section II and later sections include conclusion and references.

II. Authentication Techniques In Cloud Computing Environment

In every secure communication system particularly in wide spread network such as cloud computing, authentication is a central part. It prevents shared information from unauthorized access. The management module for authentication, authorization and accounting is AAA. If a user tries to access cloud service provider, then the AAA verifies the user's authentication information. Additionally, authentication method assures that the communicating entity is the one claimed.

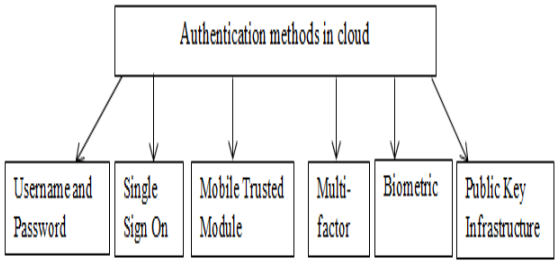

Figure 2: Authentication Methods in Cloud Computing

There are a number of authentication schemes which have been characterized into three types as:

a) Something a user knows−PIN based authentication scheme, username and password and Implicit Password Authentication System (IPAS)
b) Something a user has − smart cards or electronic tokens
c) Something a user is− biometric authentication [1].

These three are further categorized into six types discussed as under:

A. Username and Password Authentication

In this technique of authentication, confidentiality and privacy can be maintained up to some level. In order to access the information in the CSP, the username and password are required to be entered by the user to the system. It is observed that this authentication technique fails in providing a higher and reliable security because it is tough to check whether the request is from the authorized user. Furthermore, most of the users choose very easy passwords for a machine to guess. Also there is a possibility of the best password to get stolen by brute force and dictionary attacks. In cloud computing environment, the input constraints make it difficult for users to use complex passwords which lead to the usage of easy and short passwords. Moreover, users reuse their passwords for recognizing in many different servers which increases the risks to the security of user's pooled information. Strong passwords help in making brute force attacks impracticable as well as help in avoiding the dictionary attacks. It is believed that the length of the password decides the security it delivers.

Various protocols have been presented that can allow a user to use a single password authentication to recognize in numerous services securely [5]. These protocols prevent users against dictionary attack, cross-site attack, malware and phishing. The main idea of these proposed protocols is that the user's password remains secure even if the mobile device gets stolen.

B. Multifactor Authentication

To make information more secure in cloud computing environment, a combination of authentication techniques needs to be used. This scheme is more secure because it does not just validate the username and password pair but also requires another factor e.g. biometric authentication. It is one of the stronger authentication techniques. Actually, the expectation of authenticity rises exponentially when additional factors are involved in the process of verification.

For cloud computing environment, a multifactor biometric authentication system was proposed that includes finger print and palm vein [6]. The aim is to handle the biometric data in a protected fashion by keeping the data of fingerprint in the central database of the cloud security server and the biometric data of palm vein in multi-component smart cards.

C. *Mobile Trusted Module*

A set of conditions to store, measure, and report software and hardware integrity were introduced by Trusted Computing Group (TCG) through a hardware root-of-trust, that are the Mobile Trusted Module (MTM) and Trusted Platform Module (TPM). Unlike Trusted Platform Module (TPM) which is for PCs, MTM is a security aspect employed in mobile devices, [7]. The integrity and reliability of a mobile platform is ensured by the MTM [8].

Three main issues have been identified in the MTM with their promising solutions as well. The first issue is related to the requirement of balancing more or less distinct goals at the system-level designs. The second issue is the cryptographic algorithms that should be supported by MTM. The third issue is linked to the application of cryptographic primitives.

D. *Single Sign On*

The SSO is a method of accessing the multiple independent software system in such a manner that when a user logs in a system, without being provoked to re-login in each application, gains the access to all the system [9]. This process supports the users to access numerous services and reduce the threat for the administrators to direct users practically. By preventing the user to remember many passwords, it helps to improve user efficiency and decreases the amount of time the user puts in typing numerous passwords to login.

E. *Public Key Infrastructure*

Traditional authentication scheme is based on the secret key and mainly supports the placement of traditional asymmetric cryptographic algorithms, for example, RSA. To prove the identity of user, a private key is used. In the design of security protocols such as Secure Electronic Transaction (SET) and Secure Socket Layer (SSL/TLS), PKI has been used in order to be responsible for authentication. PKI mechanism has to ensure data integrity, data confidentiality, non-repudiation, strong authentication, as well as authorization. The security characteristics of cloud environment have been proposed that uses combination of SSO, Public Key Infrastructure, cryptography techniques, as well as LDAP, to guarantee the integrity, authentication and confidentiality of data and communications [10]. Thus, this model presented benefits of both single technologies and combination of them. PKI plays a key role in security and authentication of users in a distributed environment like that of mobile cloud computing, cloud computing and wireless sensor network.

F. *Biometric Authentication*

It is the process of validating if a user is whom he is demanding to be. There are three important factors of information security that are supported by biometric authentication. These factors include identification, authentication and non-repudiation. It is derived from the Greek word bios meaning "life" and metron meaning “measure". Recognition of an individual’s behavioral and physiological attributes provides the basis for this authentication technique. Besides, it is a strong authentication technique by providing the biological proof of what we are and what we know [11].

Biometric authentication is classified into two types: behavioral and physiological.

- Behavioral biometric: It depends on the behavior of the user. In this type of biometric authentication, signatures, keystrokes and voice prints are used.
- Physiological biometric: It is based on the physical characteristics of human. In this type of biometric authentication, hands, faces, iris, finger prints, palm-print and retina are used.

Palm-print is getting highly popular nowadays because this biometric modality is easy to capture and implement. It involves coarse lines which can be easily detected in the images that have been captured even by using low resolution camera. Moreover, it can be easily integrated into some already existing biometric recognition system because it does not require some special capture device. Thus it proves to be a perfect choice for implementation of multifactor authentication system.

CONCLUSION

In cloud computing, security of data is the most important issue that needs to be addressed. Out of different techniques used for maintaining security and privacy for each communication process in a cloud, authentication technique proves to be an important factor. Actually, the authentication of user becomes an important issue in cloud computing in order to protect the critical information in cloud service providers. Six main authentication techniques i.e., username and password, MTM, multifactor, PKI, Single Sign On and biometric authentication together with their subsets are playing a marvelous role in maintaining the authenticity of the shared data in cloud, thereby enhancing the security which is the main loophole or issue in a cloud computing environment.

IV. REFERENCES

[1] Babaeizadeh Mahnoush, Majid Bakhtiari, and Alwuhayd Muteb Mohammed. "Authentication Methods In Cloud Computing: A Survey". *Research Journal of Applied Sciences, Engineering and Technology* 9.8 (2015): 655-664. Web.

[2] Nancy Awadallah.” Security Threats of Cloud Computing”International Journal on Recent and Innovation Trends in Computing and Communication 5.098(2015):n.page.Web

[3] Pearson, S., Y. Shen and M. Mowbray, 2009. A privacy manager for cloud computing. In: Jaatun, M.G., G. Zhao and C. Rong (Eds.), CloudCom 2009. LNCS 5931, *Springer*, Berlin, Heidelberg, pp: 90-106.

[4] Behl, A., 2011. Emerging security challenges in cloud computing: An insight to cloud security

challenges and their mitigation. *Proceeding of World Congress on Information and Communication Technologies (WICT, 2011)*, pp: 217-222.

[5] Acar, T., M. Belenkiy and A. Küpçü, 2013. Single password authentication. *IACR Cryptology ePrint Archive*, pp: 167.

[6] Ziyad, S. and A. Kannammal, 2014. A Multifactor Biometric Authentication for the Cloud. Adv. Intell. Syst. Comput., 246: 395-403.

[7] Sidlauskas, D.P. and S. Tamer, 2008. Hand geometry recognition. In: Jain, A.K., P. Flynn and A.A. Ross (Eds.), *Handbook of Biometrics. Springer*, US, Boston, pp: 91-107.

[8] Kim, M., H. Ju, Y. Kim, J. Park and Y. Park, 2010. Design and implementation of mobile trusted module for trusted mobile computing. *IEEE T*. Consum. Electr., 56(1): 134-140.

[9] Radha, V. and D.H. Reddy, 2012. A survey on single sign-on techniques. Procedia. Technol., 4: 134-139.

[10] Zissis, D. and D. Lekkas, 2012. Addressing cloud computing security issues. Future. Gener. Comp. Sy., 28: 583-592.

[11] Bhattacharyya, D., R. Ranjan, A. Farkhod Alisherov and M. Choi, 2009. Biometric authentication: A review. Int. J. u-and e-Serv. Sci. Technol., 2(3): 13-28.