 ISBN:978-93-5254-640-4

Authentication Technique by Using USB Token in Cloud Computing

Basel Saleh Al-Attab
Research Scholar, Yemen nationality
School of Computational Sciences, S. R. T. M. University, Nanded , India
atbbael@gmail.com

Dr. H. S. Fadewar
Assistant Professor
School of Computational Sciences, S. R. T. M. University, Nanded , India
fadewar_hsf@yahoo.com

Abstract— ***The user's authentication is considered as the vital concern in the Cloud computing environment. It is the mechanism of ensuring the security, privacy and the identification of the authorized user of the cloud server. Due to the inadequacy of the current authentication techniques in providing high level security to the users in the cloud computing environment, this paper attempts to propose a different component hardware based authentication scheme using USB. The significance of the proposed technique lies in the fact that it defies phishing attacks and brute force attacks. It is also less costly than other biometric methods and less complex than other hardware based methods.***
Keywords— *Cloud Security, Authentication, CPS, Token*

I. INTRODUCTION

The Cloud Computing paradigm has been emerged as one of the most important new technologies used in various companies and organizations. Such significance resulted from its features that include easy access to information, cost efficiency, unlimited storage, backup and recovery, and automatic software integration. Yet, there are still some difficulties related to security system. Like any other security system, the cloud security system requires three important factors known as CIA: confidentiality, integrity and availability[6]. In Cloud Computing, the first factor, confidentiality, plays a major role in preserving control on organizations' data situated across multiple distributed databases. Integrity, however, denotes the fact that an unauthorized person is not allowed to come into access to the stored information. In this sense, it is only the authorized person who is permitted to modify, fabricate and delete sensitive information in cloud servers. As a result, companies and organizations can attain great confidence in data and system integrity. The main goal of availability is to ensure that an unauthorized person cannot access to shared information in cloud service provider (any time and any place). This factor enables the cloud servers to continue operations any time, even in the possibility of a security breach such as Denial of Service attacks (DOS), natural disasters as well as equipment outages which can constitute a threat to availability [1].

Accordingly, authentication is seen as an integral part of a network's security system. It is defined as the mechanism of the identification as it ensures the validity of the identity of a user together with a computer and a service. Depending on network operating system and connection type, authentication can be accomplished by the use of either the single tier or the two tier techniques. The former is the common traditional approach. Yet, it has not provided high level security to the users. Therefore, the latter has emerged as the alternative.

The two tier approach includes biometric based authentication schemes which involve identifying the authorized person by particular physiological features such as fingerprint, face recognition, and iris. Here, the user's fingerprint is viewed as the most widely used biometric scheme. Nevertheless, biometric based authentication scheme is not the best choice for the cloud environment because of the following reasons: the biometric devices have trouble in combining themselves to the cloud computing environment; when a large number of customers are being verified at the same time, the mechanism becomes slow, extra cost will be involved which is yet another big factor and hindrance issue in cloud platform.

Therefore, the current study aims at proposing a new authentication technique in cloud computing environment by using USB Token. This paper is organized as follows: in addition to Introduction, the existing authentication methods are presented in section II. The third section presents the literature study and existing work. The proposed scheme and its working are explained in section IV. Finally, the conclusion is presented in section V.

II. AUTHENTICATION METHODS

There are different methods used for the user's authentication, in this section, these methods can be classified into three types as shown in figure1.

A. Knowledge Based Authentication

Knowledge Based Authentication scheme indicates the use of the single tier technique that depends on employing the username and password method. Under this method, the user can access into the stored data through using a particular username and password to login to the cloud server. Employing such a technique in which users usually use easy passwords has many security risks related to the revealing of the users' private data in case of compromising that server, for such passwords can be easily guessed. In this view, using the password based authentication suffers from the traditional security attacks such as on-line, off-line, Man-in-the-Middle

(MITM), and dictionary attacks [2]. Moreover, users always do not have complete trust with that foreign server. The features of this method of authentication can be listed as follows[3]:

- Easy to implement.
- Requires no special equipment.
- Easy to lose or forget.
- Vulnerable to shoulder surfing.
- Security based on password strength.
- Cost of support increases.
- Familiar to a lot of users.

Here are the two types of Knowledge Based Authentication scheme:

1) *Text (Alphanumeric) based password*: Text-based password includes Personal Identification Numbers (PINs), Personal Unblocking Key (PUK), and alpha numeric password.
2) *Graphic (Image) based password:* The main reason for using graphic based password is that the graphic images are easily recalled than the text password. The graphical password techniques can also be classified into three groups as follows[4]:
   - Recognition Based Technique: In this technique, the user is presented with a collection of images, icons or symbols. During authentication, the user selects the set of candidates.
   - Pure Recall Based Technique: In this technique, the user reproduces his/her password without using any hint or gesture.
   - Cued Recall Based Technique: In this technique, framework of reminder, gesture and hint is considered. Using this technique, in which the user reproduces his/her password, becomes more accurate.

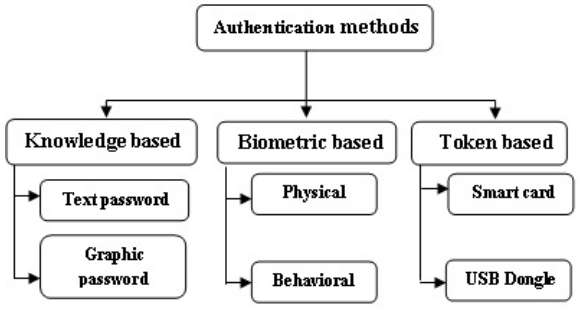

Fig. 1 Authentication methods

B. Biometric Based Authentication

The word 'biometrics' comes from two ancient Greek words: 'bios' = 'life' and 'metron' = 'measure'. The biometric authentication is a process in which a user is recognized automatically based on his physiological or behavioural features. The biometric authentication method supports the three important factors of information security: authentication, identification and non-repudiation. The objectives of biometric authentication are security, cost, computation speed, accuracy, user acceptance, and environment constraints [1]. This method can be categorized into two types: physical and behavioural biometrics. The physiological biometric involves the user's facial features, palm prints, retinal patterns, finger print, iris pattern, and hand geometry. In behavioural biometric, the user's identification is, however, based on his behaviour such as signature and keystroke dynamics [5].

C. Token Based Authentication

This method involves physical devices such as smart cards, USB device (Dongle) given to an authorized user of computer services for ease authentication. It provides full local administration and support for multiple advanced security applications such as digital signing, pre-boot authentication and disk encryption. Under this technique, the Token authentication client generates and stores private keys on-board highly secure smart card or dongle -based authenticators, which allow users to securely carry all their digital credentials wherever they go. Some of the features of Token authentication method can be listed below:

- Strong two-factor authentication for network and data protection.
- Enables local administration and usage of devices.
- Support for full client customization, including security configuration, policies and user interface .
- Seamless integration with any certificate-enabled application based on industry standard APIs.
- Enables enhanced password management applications for protecting PCs and securing onsite local network access, using eToken Network Logon.
- Support for Virtual Keyboard enables the user to enter passwords without using a physical keyboard and provides protection against kernel level keyloggers.

III. LITERATURE STUDY

Chow et al.[13] proposed a framework for authentication in cloud computing, in which authentication relied on the user's behaviour. Although the flexibility of the system has provided a support to latest and evolving Cloud authentication systems, the authentication score is checked against a certain threshold. Hence, the best result depends on application. Z. Shen et al. [7] proposed a trusted computing platform. It is robust and efficient against phishing and replaying attacks. Yet, it needs to design a system that authenticates the user with a particular feature rather than possession of Mobile phone. In this sense, for instance, the theft or loss of the mobile phone may lead to a security breach. Moreover, Choudhury et al.[8] proposed a strong user authentication framework for cloud computing. It provides formal security proof, identity management, mutual authentication and session key agreement. However, the performance is unknown as the password and smart card verification is done by the local system. Kim et al. [9] also proposed a consolidated authentication model. Secure protocols allow the credentials to freely roam in cloud computing environment. The credential store is the repository for credentials, posing a serious threat of being hacked. In addition, Dinesha [10] proposed a Single Sign On scheme, under which the central server supplies credential with the application server, so no multiple authentication for different applications is permitted. Thus, if the central server is hacked, then, the entire server is hacked, too. Furthermore, Akshay et al.[11] proposed a face recognition system, which is viewed as simple and easy to implement. However, it becomes nonsense in the absence of camera or when the face features are changed due to lighting conditions, time of the day, age, etc. Finally, Mohammad [12] proposed ALP model to solve the issue of privacy preservation by authentication and

confidentiality approach for redacted trees that uses the previous privacy 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. This approach is based on the previous information, so it cannot cover new attack patterns.

IV. PROPOSED SCHEME

In this section, we present a different component scheme which aims to provide a secure authentication mechanism for the cloud users. Our scheme depends on using USB Token (dongle). The USB contains the USB device ID and the USB device pin-keys (secret keys) generated randomly by a particular algorithm. These USB pin-keys are sent to the Cloud server by using secret channels to be stored with the username and the USB device ID in the Cloud server. In every successful login to the Cloud server, the USB generates new secret key randomly, stores it in the USB, and then, sends it to the Cloud server after encrypting it as a database for the user's authentication. The proposed scheme works in two processes: registration and the login. It is a very simple and secure authentication method because in the authentication process, the user is not required to enter any pin or password through the keyboard which is prone to brute force attacks by intruders and malicious users. Instead, the user just has to put the special kind of USB device given to him by the Cloud Service provider. After putting the USB along with the username, the user's identity gets established and matches the CSP's database, and accordingly, he/ she gets authenticated successfully.

The steps of the registration process are as follows:

Step1: The user inserts the USB device in the USB port on PC or laptop or mobile device.

Step 2 : The user creates a user account on the CSP website by insert username.

Step3: As the user inserts the device, a secret key gets generated and, then, sent to the CSP to be stored in the database maintained by the CSP along with the user's details.

Step 4: This USB pin is automatically generated, transmitted and linked with the user's account at CSP's location. The registration process is complete now.

For example, the CSP's database row might look like the following:

Account Id	Username	USB Device Id	USB Pin (Secret key)
1011211	User21	A10012211	Byxdsc101

The steps of the login process as follows:

STEP 1: The user tries to login to a Cloud Service Provider's website by entering his valid user name.

STEP 2:The user is again asked to insert the USB dongle given to him by the CSP.

STEP 3: The username along with the secret key of the dongle are sent to CSP to validate.

STEP 4: The user gets validated by the CSP and the login is successful.

STEP 5:The USB generates new secret key randomly, stores it in the USB, and then, sends it to the Cloud server.

V. CONCLUSION

In this paper we proposed a different component hardware based authentication scheme using USB device. At the first level, the user gets authenticated by using username, and at the second level, he/she has to insert the USB device given to him by the CSP to get authenticated and permitted to access. We presented our working of the proposed scheme in two processes: the registration and the login. The significance of the proposed technique lies in the fact that it defies phishing attacks and brute force attacks. It is also less costly than other biometric methods and less complex than other hardware based methods.

For future work, the proposed line of research includes designing architecture for the USB device and designing the whole process from the user, CSP and the browser's point of view.

VI. REFERENCES

[1] Mahnoush Babaeizadeh, Majid Bakhtiari and Alwuhayd Muteb Mohammed," Authentication Methods in Cloud Computing: A Survey", Research Journal of Applied Sciences, Engineering and Technology 9(8): 655-664, 2015 ISSN: 2040-7459; e-ISSN: 2040-7467 © Maxwell Scientific Organization, 2015.

[2] Ali A.Yassin, Hai Jin, Ayad Ibrahim, Weizhong Qiang, Deqing Zou, " A Practical Privacy-preserving Password Authentication Scheme for Cloud computing", 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum.

[3] kumar Abhishek, sahana roshan, Prabhat Kumar, Rajeev Ranjan, " A comprehensive study on multifactor anthentication schemes" , advances in computing and information technology ,volume 177 , 2013.

[4] Pawar Poonam A, Gayake Nalini B, Mane Kalpana T, Mudpe Ashwini M. ," Graphical Password Authentication with Cloud Securing Method", International Journal of Multidisciplinary Research and Development 2015; 2(3): 763-768.

[5] Babaeizadeh, M., M. Bakhtiari and M.A. Maarof,"Authentication method through keystrokes measurement of mobile users in cloud environment". Int. J. Adv. Soft Comput.2014.

[6] Basel Saleh Alattab, H.S.Fadewar, "Security Issues and Challenges in Cloud Computing" , International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-2, Issue-7, May 2014 .

[7] Z. Shen, L. Li, F. Yan, X. Wu, "Cloud Computing System Based on Trusted Computing Platform", International Conference on Intelligent Computation Technology and Automation (ICICTA) 2010.

[8] Amlan Jyoti Choudhury, Pardeep Kumar, MangalSain, Hyotaek Lim, Hoon Jae-Lee," A Strong User Authentication Framework for Cloud Computing". Asia - Pacific Services Computing Conference, 2011, IEEE.

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

[10] Dinesha H A, "Multi-level Authentication Technique for Accessing Cloud Services". International Conference on Computing, Communication and Applications (ICCCA), IEEE, February 2012.

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

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

[13] 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". 2010, Chicago, Illinois, USA.