A Secure Hardware Based Multifarious Component Authentication Technique Using USB for Cloud Environment

Ankit Dhamija
Research Scholar,
Computer Science Department, Jaipur National University, Jaipur
dhamija.ankit@gmail.com
Deepika Dhamija
Research Scholar,
Computer Science Department, Jaipur national University, Jaipur
aghi.deepika@gmail.com

ABSTRACT

Authenticating users and establishing their identity is the first most part of any computer based application or website. This has to be the most significant point from the security aspect. With the emergence of cloud platforms and their services, our interaction with data, devices, software and applications is witnessing an unprecedented change. This issue of user authentication tops the list of threats posed by the cloud computing paradigm. In most of the applications, users are supposed to remember multiple passwords and usernames for different services offered by Cloud Service Providers (CSP's). The rise in brute force attacks makes this username-password scheme weak and thus users and organizations expect that there are multiple parameters to be passed before the user actually gets authenticated and his identity is established. The development of such multifarious components indeed enhances the security but right now it is in its early stages. Multifarious techniques such as use of Biometrics like fingerprinting, iris scanning, face recognition methods, hardware based approaches like One-time-passwords(OTP), hardware tokens and bypass methods are being proposed by researchers and industry professionals and are under continuous developments and improvements.

On the lines of multifarious component authentication, this paper proposes a simple, convenient & secure hardware based multifarious component technique using Universal Serial Bus (USB). Our proposed model provides solution to the limitations posed by the hardware based OTP scheme where a user is supposed to enter a pin or password, received on their mobile handset, on the web portal of the Cloud Service Provider. In this way, our scheme defies the possibility of a phishing attack and brute force attack by any intruder of stealing that OTP or pin and misusing it. It

Keywords---authentication, multifarious, USB, cloud

I. INTRODUCTION

Cloud computing is a current & upcoming area that contains the applications delivered as services over the Internet as well as the hardware and systems software in the data centres that provide such services [1]. Cloud computing offers concepts such as virtualization, storage, processing power, connectivity, and sharing that have benefitted to end-users and also to the service providers. No storage limits for end-users is the foremost benefit of cloud computing that reduce the concerns about the amount of remaining memory significantly [2]. Then, universal connectivity, open access, sustainability and interoperability are the other advantages of this newfound service [3].

However, Maintaining and enhancing the security and privacy in cloud environments is one of the most challenging issues that work as a hindrance element in the approach of users. This threat makes people hesitant in adopting the cloud platform. The first place where users come across the security aspect is the user authentication interface [4] and then managing accesses when users outsource sensitive data share on public or private cloud servers [5]. Authenticating users and establishing their identity becomes the core of security in the cloud computing. So, it is necessary to allow that only authorized user can access stored data [6]. The server in a traditional password authentication scheme, allow or deny any remote user based on identity and password. In general, textual password schemes are the most widely used, but they have many weaknesses. These drawbacks denotes that the user find it difficult in memorizing long or complex passwords, and the security risks can be obtained by depending short simple passwords [7].

Passwords are prone to attacks such as dictionary or brute-force attacks because passwords are only a combination of the symbols that are present on keyboards. As a result, an intruder or malicious person may attempt all possible combinations until detecting a correct password; such type of attacks is called brute-force attack. Additionally, most customers tend to pick something such as phone number, favorite game, and name to use as a password as these things are easily to remember. Consequently, intruders can build a table of significant words to hack the system, which is named dictionary attack. Furthermore, by using the password based authentication, the users are still vulnerable from the malicious attacks such as on/off-line attack, replay attack, *Man-in-the- Middle* (MITM) attack [8].

The use of only the single tier techniques has not provided adequate security to the users so the two tier approaches came into picture. It included biometric based authentication schemes which involve identifying a person by particular physiological characteristics like face recognition, fingerprint, and iris. Fingerprints are the most widely used biometric [9, 10]. However, it is not the best choice for the cloud environment because of the following reasons: 1) the biometric devices will have trouble in combining themselves to the cloud computing environment; 2) when a large number of customers are being verified at the same time, the mechanism will become slow.; 3) extra cost will be involved which is yet another big factor and hindrance issue in cloud platform.

Then 2-Factor Authentication (2FA) techniques were proposed which were based on a second authentication based on some hardware devices and it proved to be more suitable with architecture of cloud authentication. A user sends his username and password to the cloud server for authentication. The cloud server asks the user to send his second identity such as an One time Password (OTP) sent on the user's registered mobile phone or as an email which it ensures from matching of user's username/password with a cloud server's database. The user gains permit to reach a cloud server's resources when his second factor has validity in the cloud server [11]. The disadvantage of this OTP approach is that any hacker can access the sms sent to the mobile device or hack the email account of the user or they can trap the textbox value where the OTP is entered by the user on the cloud vendor's web portal.

In this paper, we propose a simple, convenient & secure hardware based multifarious component technique using Universal Serial Bus (USB). Our approach presents architecture of registering with the cloud vendor and for double authentication, they have to insert the USB device on their computer or mobile device and only then they will be authenticated. In this way, our scheme nullifies the threats posed by the hardware based OTP authentication scheme where the values received and entered by the user are prone to be hacked. Furthermore, our approach provides security for phishing attacks also.

The rest of this paper is organized as follows. The literature study and existing work exist in section II. The proposed scheme and its working are explained in detail in section III. The benefits of the proposed scheme are covered in Section IV. Finally, the Conclusion is presented in section V.

II. LITERATURE STUDY AND RELATED WORK

Viet et al. [12] proposed the first anonymous password authentication scheme that aggregates a password scheme with the *Private Information Retrieval* (PIR) scheme. The limitations of this scheme are that it requires the server to be passed a whole database to detect user and it cannot resist on-line guessing attacks.

Florencio and Herley [13] proposed a proxy web service that allows customers to arrive at web sites by employing a MITM proxy. The password customer is pre-encrypted and implemented as one-time passwords' list. Thus, the proxy cannot contain the passwords, but more correctly the keys with which the customers' passwords have been encrypted previously. This, however, is classified within a single-factor scheme. Moreover, there is a drawback to an adversary who misappropriates one-time password.

Balfanz and Felten [14] presented a smart card task using a mobile phone. They used a sequence link to a remote computer and supported the mobile device by trusting the authentication path. There are several suggestions that denoted to use a cell phone as a second factor for authentication. However, this scheme is restricted by the cellular network coverage area.

The smart card based authentication schemes [15-18] implement two factors of the authentication researches. In the first factor, users' investigation credentials are saved in the smart card while the password represents as a second factor, the smart card has been preserved by password. These two factors do not need the server to store a password file. The negative side of smart card is that it is not a simple device.

Sulochana and Parimelazhagan [19] have described a puzzle based authentication scheme in Cloud computing in which user first registers and solves the puzzle, puzzle solving pattern and time is stored and validated by local server and if user get authenticated, start accessing the Cloud services. Although this scheme ensures 2 tier authentications but static in nature, if attacker once identified the stored pattern, he could easily break the security.

Yogita et al. [20] have described that not a single technique is enough to provide security in Cloud, she has used Diffie Hellman with digital signature for providing 2 tier authentication. But digital signature uses so many parameter that`s why it is heavy enough and also requires a proper key management. Arasu et al. [21] have given an approach of Hash Message Authentication Code (HMAC) in which key, message and hash function is concatenated together for ensuring authentication. This approach describes only single tier authentication which is weak in case of Cloud computing.

Maninder and Sarbjeet [22] have provided an advance multi tier authentication scheme for enhancing security in financial transactions, in which in first tier, user has to simply pass the traditional login authentication and in second tier a fake screen will appear before user from local server, which is filled by the user by predefined stored pattern, if it is correct then only server will allow access to the resources. Problem with this approach is that it is static in nature, once user identifies or observes the pattern of fake screen from behind, he can easily break this authentication.

Satish and Anita [23] have proposed a method of fake screen for ensuring two tier authentication in Cloud computing. In this method of authentication, first user registered himself with Cloud server, and then registered his device. So secret code gets sent to the registered devices which ensure second level of authentication. This method involves additional hardware which is costly and must be along with you every time when you are going to login in the system.

Parsi and Sudha [24] have proposed method that use RSA algorithm for authentication and data transfer securely. This method involves a phase of key generation, encryption and decryption. Priyank Rajvanshi et al [25] proposed an approach of protecting the confidentiality of users' data from service providers, and ensure that service providers cannot access or disclose users' confidential data being processed and stored in cloud computing systems. They suggested an efficient and supple spreading system with open dynamic data support to make sure the accuracy of user's data in the cloud. We use erasure correcting code in the file circulation preparation to give redundancies and guarantee the data soundness. This construction considerably reduces the messaging and storage in the clouds as compared to the conventional replication-based file division techniques. By using the homomorphism token with distributed confirmation of erasure-coded data, our system achieves the storage rightness cover as well as data error localization:

B Wang et al [26] propose a simple, efficient, and publicly verifiable approach to ensure cloud data integrity without sacrificing the anonymity of data owners nor requiring significant overhead. Specifically, they introduce a security-mediator (SEM), which is able to generate verification metadata (i.e., signatures) on outsourced data for data owners. Their approach decouples the anonymity protection mechanism from the PDP.

L. B. Jivanadham [27] et al proposed an integrated authentication mechanism called the Cloud Cognitive Authenticator (CCA), an API proposed for the cloud environment integrating bio-signals, one round Zero Knowledge Protocol (ZKP) for authentication and Rijndael algorithm in Advance Encryption Standard (AES). CCA is proposed to enhance the security in public cloud through four procedures providing two levels of authentication as well as encrypting/decrypting the user id.

III. PROPOSED SCHEME

In this section, we present a multifarious component scheme which aims to provide a secure authentication mechanism for the cloud users. At first, we propose a simple block diagram of our scheme which depicts the flow of the things and functionality in a very summarized and brief manner. In this part, the general working model of multifarious component authentication using USB is depicted. We present our scheme in two different parts: Set up & registration part and the login part. Then in the first part, we show the set up and registration process of the user at the cloud service provider and we depict the use of second multifarious component i.e. the USB in our approach. Finally, in the second part, after the user has been successfully registered with the CSP, we'll show the process of making login to their account which involves the use of the USB device.

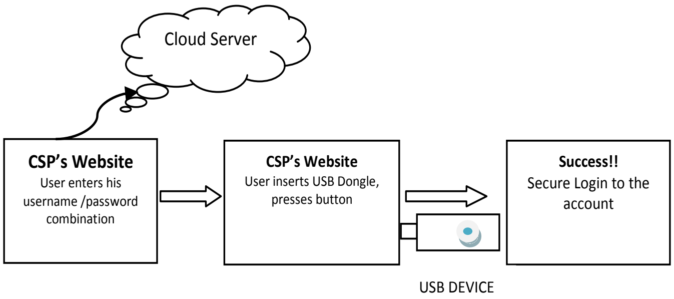
Cloud Server
CSP's Website
User enters his username /password combination
CSP's Website
User inserts USB Dongle, presses button
Success!!
Secure Login to the account
USB DEVICE

Figure 1: Block Diagram the figure 1 depicts the block diagram of the proposed scheme. It consists of the following steps:

STEP 1: User tries to login at a Cloud Service Provider's website by entering his valid username and password allotted to him by the CSP.

STEP 2: If the details entered are correct, the user is again asked to insert the USB dongle that is given to him by the CSP and which is now in his possession. User inserts the USB dongle and presses the sole button on the USB.

STEP 3: The user gets validated by the CSP and the login is successful.

This is a very simple and secure multifarious component authentication method because in the second step of the authentication process, the user is not asked to enter any pin or password through the keyboard which are prone to brute force attacks by intruders and malicious users. Instead, the user just has to press a button on the special kind of USB device given to him by the Cloud Service provider. On the press of that button on the USB, the user's identity gets established and it matches with the CSP's database and the user gets authenticated successfully.

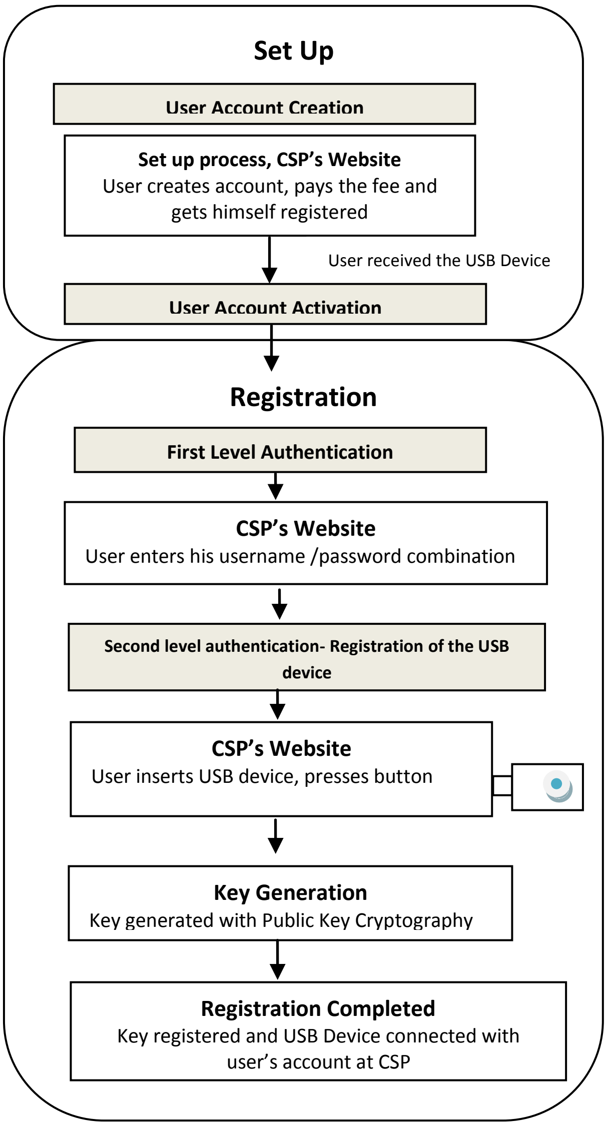
Set Up
User Account Creation
Set up process, CSP's Website
User creates account, pays the fee and gets himself registered
User received the USB Device
User Account Activation
Registration
First Level Authentication
CSP's Website
User enters his username /password combination
Second level authentication- Registration of the USB device
CSP's Website
User inserts USB device, presses button
Key Generation
Key generated with Public Key Cryptography
Registration Completed
Key registered and USB Device connected with user's account at CSP

Figure 2 displays in detail, the entire process of setting up an account and the registration process. The steps for this process are as follows:

STEP 1: The SET UP process starts with the creation of user account on the CSP website. This is just like we create any other account on any particular website to become its user.

STEP 2: While entering the user details like name, age, dob, purpose, type of service required, selecting the username etc, the user is asked to pay the required fee for the USB device that will be mailed to the user within the stipulated time frame.

STEP 3: When the user receive the USB device and the kit, he can proceed toward registering and activating that device.

STEP 4: Now, the REGISTRATION process starts with the user again going on the CSP's portal and performs the first level authentication by entering his username password combination.

STEP 5: If correct, the user is asked to perform second level authentication by inserting the USB device received for activating it. The user inserts the USB device in the USB port on PC or laptop or mobile device.

STEP 6: As the user inserts the device, a secret key gets generated and is sent to the CSP and gets stored in the database maintained by the CSP along with the user credentials. For example, the CSP's database row might look like the following:

Account Id	Username	Password	USB Device Id	USB Pin (Secret Key)
11221101	Pturner12	*******	A20012112	Axscdv213

STEP 7: This USB pin is automatically generated, transmitted and linked with the user's account at CSP's location. The registration process is complete now.

The Login Process

The login process requires the SETPS 4 to 7 to be repeated, i.e. both multifarious components have to be passed and then the user is able to login to their account. Now the user can proceed and navigate the features on the CSP's website. As and when the user needs to perform some critical operation, the web interface of CSP's website may ask the user to insert the USB device and prove its identity. The key that has been generated gets acquired and the user gets verified after the user presses the button on the device.

IV. BENEFITS OF THE APPROACH

As we have seen the working of the proposed scheme, the benefits can be figured out from the working. First, the proposed scheme prevents phishing attacks from the intruders, i.e. the user is not required to enter pin/passcode in the textbox at the web portal, instead, they just needs to press a button on the USB device and they can login without typing. Second, it denies all the brute force attacks. Third, the scheme is much better than the costlier biometric schemes that are based on fingerprinting scan, iris scan etc. Fourth, the complexity involved is much less than the other biometric based schemes. Fifth, it is an improvement over the hardware based OTP schemes as every second organization is using the OTP based hardware scheme and it is much easier to crack but this scheme avoids all such possibilities. Sixth, the user is not required to remember so many passwords.

V. CONCLUSION & FUTURE WORK

In this paper we proposed a multifarious component hardware based authentication scheme using USB where at the first level the user gets authenticated by using username password method and at the second level, the user has to insert a USB device for him to get authenticated and access the things. We presented a detailed working of the proposed scheme in two steps- the SETUP and the REGISTRATION process was explained in detail and we figured out a few benefits of the proposed scheme like it defies phishing attacks, brute force attacks, less costlier than other biometric methods and less complex than other hardware based methods like OTP. As for future work, the proposed line of research includes designing architecture for the USB device, the plugins for the browser and designing the whole process from the user, CSP and the browser's point of view.

VI. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM Magazine*, vol. 53, no. 4, pp. 50–58, April 2010.

[2] F. Fatemi Moghaddam, *Secure Cloud Computing with Client-Based Control System: Protection of Stored Cloud-Based Data by Increasing End-User's Role*, Chapter 1: Cloud Computing, 1st Edition. Saarbrücken: Lambert Academic Publishing (LAP), 2013, pp. 9-2.

[3] D.G. Chandra, and R.S. Bhadoria, "Cloud Computing Model for National E-governance Plan (NeGP)," in *Proc. 4th International Conf. on Computational Intelligence and Communication Networks (CICN)*, Mathura, 2012, pp. 520-524.

[4] F. Fatemi Moghaddam, M. T. Alrashdan, and O. Karimi, "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments," *Journal of Advances in Computer Networks*, vol. 1, no. 3, pp. 238–241, 2013.

[5] F. Fatemi Moghaddam, M. T. Alrashdan, and O. Karimi, "A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments," in *Proc. IEEE 2nd International Conference on Cloud Networking (CloudNet)*, San Francisco, USA, November 2013

[6] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, Vol.34, No.1, Jan. 2011, pp.1-11.

[7] M. Zhou, Z. Rong, W. Xie, W. Qian, and A. Zhou , "Security and Privacy in Cloud Computing: A Survey", *Proc. of the Sixth International Conference Semantics Knowledge and Grid (SKG'10)*, Beijing, China, Nov. 2010, pp.105-112.

[8] S. Shin, K. Kobara, and H. Imai, "A Secure Construction for Threshold Anonymous Password-Authenticated Key Exchange", *IEICE Transactions on Fundamentals*, Vol.E91-A, No.11, 2008, pp.3312-3323.

[9] A. Jain and L. Hong, "On-line fingerprint verification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 19, 1997, pp. 302-314.

[10] M. Abdalla, M. Izabachene, and D. Pointcheval, "Anonymous and Transparent Gateway-Based Password-Authenticated Key Exchange", *Proc. International Conference on Cryptology and Network Security (CANS'08)*, Hong Kong, China, Dec. 2008, pp.133-148.

[11] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, D. Zou, "A Practical Privacy preserving Password authentication Scheme for Cloud Computing", *Proc. of the IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW'12)*, May 2012, Shanghai, China, pp.1204-1211.

[12] D. Q. Viet, A. Yamamura, and T. Hidema, "Anonymous Password-Based Authenticated Key Exchange", *Proc. of 6th International Conference on Cryptology in India (Indocryp'05)*, Bangalore, India, Dec. 2005, pp.233- 257.

[13] D. Florencio and C. Herley, "One-Time Password Access to Any Server Without Changing the Server", *Proc. of the International Supercomputing Conference(ISC'08)*, Taipei, Taiwan, 2008, pp.401-420.

[14] D. Balfanz and E. W. Felten, "Hand-held computers can be better smart cards", *Proc. of the 8th Conference on USENIX Security Symposium*, Washington, D.C, USA, 1999, pp.3-11.

[15] S. Jeon , H. S. Kim, and M. S. Kim, "Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards", *J. of Security Engineering*, Vol.8, No.2, Apr. 2011, pp.237-254.

[16] W. S. Juang, "Efficient password authenticated key agreement using smart cards", *J. of Computers and Security*, Vol. 23, No.2, pp.167-173, 2004.

[17] M. L. Das, A.Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", *IEEE Transactions on Consumer Electronics*, Vol.50, No. 2, pp.629-631, 2004.

[18] H. Y. Chien, J. K. Jan, and Y. M Tseng, "An efficient and practical solution to remote authentication: smart card", *J. of Computers and Security*, Vol.21, No. 4, pp.372-375, 2002.

[19] V. Sulochana and R. Parimelazhagan, "A puzzle based authentication scheme for cloud computing," International Journal of Computer Trends and Technology, IJCTT, vol. 6, no. 4, pp. 210-213, Dec. 2013.

[20] P. Rewagad and Y. Pawar, "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing," International Conference on Communication Systems and Network Technologies, CSNT, IEEE, pp. 437-439, 2013.

[21] S. E. Arasu, B. Gowri and S. Ananthi, "Privacy-preserving public auditing in cloud using HMAC algorithm," International Journal of Recent Technology and Engineering, IJRTE, vol. 2, issue 1, Mar. 2013.

[22] M. Singh and S. Singh, "Design and implementation of multi-tier authentication scheme in cloud," International Journal of Computer Science Issues, IJCSI, vol. 9, issue 5, no. 2, Sep. 2012.

[23] S. Kumar and A. Ganpati, "Multi-authentication for cloud security: A framework," International Journal

of Computer Science & Engineering Technology, vol. 5, no. 4, pp. 295 303, Apr. 2014.

[24] P. Kalpana and S. Singaraju,, “Data security in cloud computing using RSA algorithm,” International Journal of Research in Computer and Communication technology, IJRCCT, vol. 1, no. 4, pp. 143-146, Sep. 2012.

[25] P. Rajvanshi et al, “Data Protection in Cloud Computing”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-3, August 2013

[26] B Wang et al, “Storing Shared Data on the Cloud via Security-Mediator”, IEEE 33rd International Conference on Distributed Computing Systems ISSN 1063-6927, 8-11 July, 2013, Page(s) 124-133,

[27] L. B. Jivanadham et al, “Cloud Cognitive Authenticator (CCA): A public cloud computing authentication mechanism”, International Conference on Informatics, Electronics & Vision (ICIEV), Print ISBN: 978-1-4799-0397-9 17-15 May 2013, Page(s): 1 – 6.