Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 12, December-2018

A Strong Password Generator for user Authentication in Cloud Computing

Supongmen Walling
M.Tech. in Computer Science and Technology
Department of Computer Science and Technology
Indian Institute of Engineering Science and Technology,
Shibpur Howrah-711103, West Bengal, India

Sibesh Lodh
Assistant Professor
Department of Computer Science and Engineering
National Institute Of Technology, Nagaland
Dimapur-797112,Nagaland, India

Sedevizo Kielienyu
Master Of Compute Science
University of Ottawa, Ottawa,
Canada

***Abstract*- Cloud computing is a type of computing of using remote servers hosted on the Internet to store, manage and process data rather than a local server or a personal computer. In cloud computing, there is a third party service provider also called the vendor who provides various services through the network(Internet) and these services can be availed on a subscription basis.**

So this basically means we are using the vendor's services and also storing our data on his storage which means the server has to ensure tight security.

As the geography of computation is moving towards corporate server rooms, it bring more issues including security, such as visualization security, distributed computing, application security, identity management, access control and authentication. However, strong user authentication is the paramount requirement for cloud computing that restrict illegal access of cloud server.

In this regard, this paper focuses on presenting a strong user authentication framework for cloud computing, where user legitimacy is strongly verified before entering into the cloud. The proposed framework uses a strong password generator algorithm to generate one -time password, providing identity management, mutual authentication, session key establishment between the users and the cloud server. A user can change his/her password, whenever demanded. The user enters his credentials and an image to generate an OTP. In order to achieve better security than the alphanumerical password, the proposed model describes a scheme which allows strengthening the authentication process in the cloud environment using the password generator module by means of a combination of different technologies such as multi-factor authentication, one time password and

SHA1. Furthermore, security analysis realizes the feasibility of the proposed framework for cloud computing and achieves efficiency.

Keywords- C*loud computing, identity management, OTP (one time password), two-factor authentication, password generator*.

I. INTRODUCTION

Cloud computing, often referred to as simply "the cloud", is the delivery of on demand computing resources- everything from applications to data centers over the Internet on a pay-per-use basis. There are various security issues concerned with cloud computing out of which identity management and access management seems to be the most crucial one. Therefore, a strong framework should be proposed that provides identity management, mutual exclusion and session key establishment between users and cloud server.

Cloud computing and storage provides users with capabilities to store and process their data in third party data -centers, organizations use the cloud in a variety of different service models (such as SaaS, PaaS, IaaS) and deployment models (private, public , hybrid) . Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers (organizations providing software, platform, or infrastructure- as- a -service via the cloud) and security issues faced by their customers. The responsibility is shared, however, the provider must ensure that their infrastructure is secure and their clients data and applications are protected, while the user must take measure to fortify their applications and use strong passwords and authentication measures.

In recent years, cloud technologies have introduced new methods to attack organizations and individuals, broadening their threat landscape. The digital identities that individuals and organizations use, in order to access cloud resources, are one of the main areas at risk. Past incidents with LastPass, Google and Evernote , where a number of user accounts were compromised show how challenging it is to protect digital identities. Insecure management of identities and their access can cause a lot of trouble for organizations and individuals, resulting in data breaches, and noncompliance with important standards and regulations (such as HIPAA, PCI- DSS, EU GDPR) and inability to access resources, services and critical data. When switching to the cloud, part of the data is no longer stored on devices managed by the owners of the data. This combined with the growing number of users and roles in modern organizations and stricter regulations imposed by governments on privacy and data protection, further complicates the situation and raises importance of data

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 12, December-2018

access controls. Robust identity and access management is one of the approaches to minimize security risks of cloud computing [1].

In the context of identity management, the authentication phase does nothing more than link a person using an application or system to the individual's electronic identity, which the application or system can use to link the person's previous actions to new actions. It does not authorize a person to use an application or system; it simply states that a person has supplied the correct information to prove that the individual is in possession of a specific electronic identity.

To help alleviate the problem of easily guessed or simple passwords, password complexity and length requirements are frequently put into place. However, as attackers become more advanced and the stakes for gaining illicit access to systems become higher (for example: access to a person's deposit routing information), more resources are being directed at attacking even more complex passwords. After some period of time, passwords alone are simply no longer good enough for systems that require an added level of security or "assurance" that the person is who he claims to be [2].

After a person has successfully authenticated with a verifier to gain access to a system, the system can then use authorization to determine whether the person should have access to the system and if yes what level of access a person should have [3].

The ultimate goal of identity management solution is to create federated identity systems so users can be effectively identified and provisioned across company boundaries. Using federated identities, information can be securely shared between companies, enabling employees to access another company's data without manually re-authenticating.

II. RELATED WORKS

Various techniques have been proposed to tackle the problem of weak user authentication with each having its respective pros and cons. Leslie Lamport [4] introduced a remote user authentication method which was based on one-way hash encryption function and a password table. However, despite its ease of use, the scheme suffers from high hash overhead and the necessity to store the password table [5]. Min- Shiang Hwang and Tsuei- Hung Sun emphasize on the concept of smart card to overcome the weak user authentication problem [6]. They presented a scheme in which they combine smart card and third-party authentication to achieve a single sign-on authentication in an inter-cloud service. Several smart card methods have been proposed in the literature, particularly, [6], [7], [8], [9]. However, these approaches require special tools such as smart card reader for authentication process. To overcome these issues, [10] proposed a password generator model which removes the need of a smart card reader and providing a multi-level authentication. The drawback of this scheme is that it requires an external device i.e. smart phone to complete the authentication process. In this section, we have introduced some significant improvement over the above schemes in-order to improve the process of authentication in the cloud environment. In the next section, we present our proposal in this context. We introduced a three-level authentication phase that overcomes the traditional username & password scheme. A password generator model is used by both the cloud server and the client for authentication. This would improve and strengthen the entire authentication process from most common attacks. Also, this model omits the need of an external device such as smart card reader, smart phones to complete the authentication. The novelty here is the use of an image to generate one-time password as a third level of authentication.

III. METHODOLOGY

In this model the user authentication is based on 2FA (two factor authentication) and using an image to generate OTP. Two factor authentication, also known as 2FA, two step verification or TFA (as an acronym), is an extra layer of security that is known as " multi -factor authentication" that requires not only a password and user name but also something that only and only a user has on them ,i.e. a piece of information only they should know or have immediately to hand- such as a physical token. Using user name and password together with a piece of information that only the user knows makes it harder for potential intruders to gain access and steal that person's personal data or identity. Historically, two- factor authentication is not a new concept but its use has become far more prevalent with the digital age we live in. As recently as February 2011Google announced two factor authentication, online for their users, followed by MSN and Yahoo. Many people probably do not know this type of security process is called two factor authentication and likely do not even think about it when using hardware tokens, issued by their bank to use with their card and personal identification number when looking to complete Internet banking transactions. Simply they are utilizing the benefits of this type of multi factor authentication i.e. "what they have" and "what they know".

Using two factor authentication process can help to lower the number of cases of identity theft on the Internet, as well as phishing via email, because the criminal would need more than just the users name and password details.

The downside to this security process is that new hardware tokens(in the form of key fobs or card readers) need to be ordered, the issued and this can cause slow downs and problems for company's customers wanting and waiting to gain access to their own private data via this authentication procedure. The tokens are also usually small and easily lost so causing more problems for everyone when customers call in requesting new ones.

SecurEnvoy look to resolve this problem with two factor authentication by utilizing mobile phones SMS technology. With over 5 billion mobile phones in use, turning a phone into an authentication device quickly solves the need and additional cost delays of sending out hardware tokens.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 12, December-2018

Using two factor authentication without tokens is called token less- authentication, patented by SecurEnvoy. This type of authentication can be considered faster, quicker and cheaper to set up and maintain across many networks.

Here, the server uses a module called PassGenfor generating OTP using an image. Firstly, the user inserts his Un (user name) and password (Ps). The cloud server verifies the authenticity of the user. Upon receiving the login request, the cloud server sends a challenge G to the PassGen module and requests an OTP for every specific user. Note that every user is assigned a secret image Im. The user creates OTP by means of a challenge, a secret image sent by the server which is computed through the client's PassGen module. The PassGen extract a portion of the secret image and compute its hash value in order to create the OTP. The cloud server authenticates the user based on the OTP sent by the user.

IV. PROPOSED MODEL

This section describes the proposed model scheme for strengthening authentication in the cloud environment. The basic idea of the proposed model scheme is described as follows.

1. The user inserts his user name Un and Password Ps. Then the cloud server verifies the authenticity of the user.
2. Upon receiving the login request, the cloud server sends a challenge G based on every specific user and request an OTP.
3. An image Im is chosen from the cloud server upon receiving the login request. From that image, a challenge is generated which is used to create the OTP.
4. The challenge containing the image is send to the user by which, it creates the OTP. A password generation module extracts a portion from the image and computes it has value in order to generate the OTP.
5. The cloud server authenticates the user based on the OTP(in step 4) that was created in step 4.

Table-1: Notations

Im	Image
G	Challenge
Π(Im)	Portion of the image
OTP	One Time Password
β	Password Generator
Truncation α	Position from where the truncation begins.
Un and Pw	User name and password.

REGISTRATION PHASE

In the registration phase the user performs the following steps:-

1. A user U enters his user name Un and password Ps for registration.
2. Upon receiving the registration request, the cloud server sets a count value 0 and stores the triplet <Un, Ps, count> in its database.
3. The user is now registered and the cloud server sends a message that the user has been registered.

LOGIN PHASE

In the login phase the user performs the following:-

1. The user submits his user name Un and password Ps <Un, Ps> to the cloud provider, then, the cloud server S checks the authenticity of the user. If the user is authorized, go to step 2.
2. The cloud server upon receiving the login request <un, Ps>, sets the count value to 1, generates an ID and request the password generator βto create an OTP.
3. The password generatorβ, assigns an image Im for that user and generates a challenge G which is used to create the OTP.
4. β uses a function Π() to compute a portion of the image. From that portion, it computes three more sub-portions. Based on the count value, one of the sub-portion is selected which is used to generate the hash value and creates the OTP1.
5. The challenge G along with the image Im and OTP1 is send back to the cloud server. The cloud server stores ID and OTP1 is separate database and sends <G, Im, ID> to the user.
6. The client, upon receiving <G, Im, ID>, performs the same as in step 4 and generates OTP2 with the help of challenge G.The user submits <OTP2, ID> to the cloud server, after that the cloud server checks ID's are same and performs OTP2=OTP1. If conditions are met, the client is authenticated. The steps mentioned above are illustrated in figure given below.**NOTE-** Count value is maintained for every specific user.

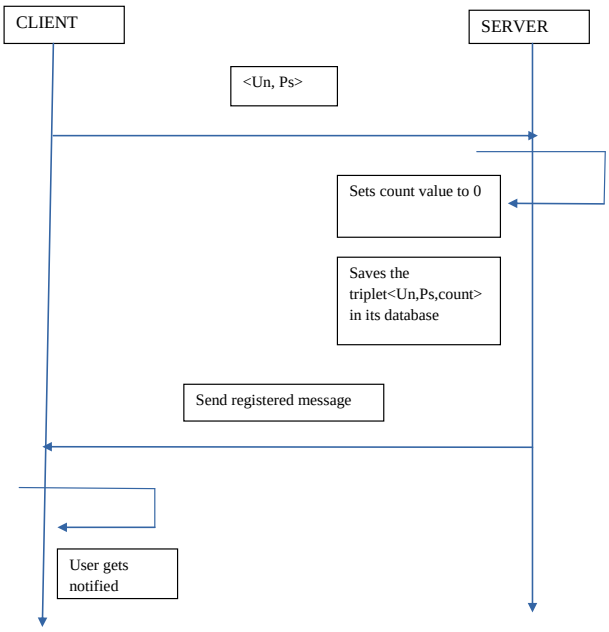

Fig. 1. Registration Phase

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 12, December-2018

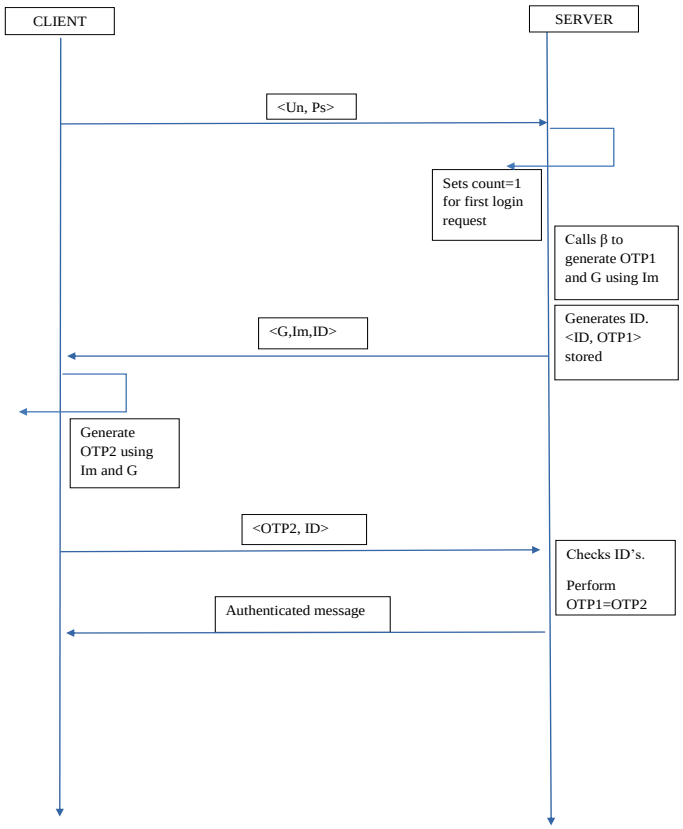

Fig. 2. Login Phase

V. TOOLS AND CONCEPTS USED IN THE PASSWORD GENERATOR

1. **Multi-factor authentication:-**enables to add a second layer security for the authentication process. It requires two or more of the following verification methods:

(1) Authentication based on something you are (biometric method).
(2) Authentication based on something you know (passwords).
(3) Authentication based on something you have (smartcards, challenge response lists, one time pads etc)

2. **One- way has functions:-** is a mapping f from some set of words in itself such that

(1) f takes a message as an input and converts it into a fixed output.
(2) f is one-way in the sense that it is easy to compute f from one way, but infeasible from the other way.

3. **Truncation α:-**is a function that enables to truncate parts of alpha numeric text in order to generate the OTP. It is used to determine the position from where the truncation begins. α is a natural number N ranging from [1,59] and can be represented as α=α1α2 where α1 and α2are respectively tens and units digit of α.

4. **The challenge G:-**is an alphanumerical code generated by the cloud server. The client uses G,Im and Π() to generate the one -time password OTP. G represents the coordinates X and Y of a point P(pixel) in the image Im and the truncation value α.

G can be represented as follows:-
G= α1||X||Im||Y|| α2 where || is the concatenation operator.

5. **Function Π() :-** is a function that enables us to cover an important number of pixels(portion of an image). From that portion, sub-portions are generated. Now, based on the login request it selects one sub-portion whose hash value is generated.

Calculation of portion of image:

1. The pixel point(X,Y) is generated by the server whose value is not on any edge of the image Im.
2. The pixel point (X,Y) is taken and its Euclidean distance from every corner(Xc, Yc) of the image Im is calculated.
3. The minimum Euclidean distance is taken from which the four co- ordinates((X, Y), (Xc, Yc), (X1, Y1), (X2,Y2)) are determined and portion of the image is formed.

X1= X if X1 is on the upper edge/ lower edge.
X2= Xc if X1 is on the left/right edge.
Y1=Yc if X1 is on the upper edge/ lower edge.
Y2= Y if X1 is on the left/right edge.

VI. SECURITY ANALYSIS

1. **Replay attack:-**After a brief time T1, the password generated will no longer be valid. This feature prevents the intruder to record the client's password. In other words, the scheme resists replay attack.

2. **Man-In-The-Middle(MITM):-** Our scheme can resist against man in the middle attack using the technique of one time password in user intercepts the password during the authentication phase, the password would be expired and could not be used for next session.

3. **Dictionary and brute- force attacks:-**The scheme resists against dictionary and brute- force attacks. In fact, the scheme uses two- factor authentication. <Un, Ps, OTP> so even if brute – force or a dictionary attack could be applied and even if the password is revealed, it will be expired password. So why to crack such an obsolete password? Obviously, these attacks are fully eliminated.

4. **Guessing attacks:-** In our scheme, we used two - factor authentication. The first factor is the user name Un and Password Ps, and the second factor is the one time password OTP created by β . Thus, in addition to the text password, we add a second level of authentication in order to strengthen the process of authentication. It is difficult for a malicious user to find or extract a password composed of at least 6

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 12, December-2018

digits. Moreover, even if a malicious user finds Ps, he can't find the OTP. In other words, the scheme withstands guessing attack.

5. **Security of the password:-** The scheme uses the β to create password automatically and these passwords are removed from entry once they are validated. The cloud database contains only client's image instead of a file of passwords. The passwords are generated for every login phase automatically, and they are available for limited period. Thus, it is clearly evident that the scheme can supply security of the passwords.

VII. CONCLUSION

Our proposed model has been implemented and tested against various security attacks and proved efficient and strong and surmounts the security flaws of login/ password scheme. Our scheme is immune to various types of attacks while providing some important security features which several schemes fails to satisfy. The obtained result shows that our scheme is more appropriate for the cloud environment compared to other related schemes. But despite of this, there are still several open problems in the cloud security, particularly data integrity. We believe that it would be a very interesting and fruitful area for future works.

ACNOWLEDGEMENT

We wish to place on record our deep sense of gratitude to our honorific guide Mr. SibeshLodh, Assistant Professor, Department of Computer Science and Engineering, National Institute of Technology Nagaland for his valuable guidance and moral support leading to the successful completion of the work. Without his continuous encouragement and involvement, this research work would not have been a reality.

We wish to dedicate this work to our parents, for they are the pillars of support,giving us confidence in whatever we do.

REFERENCES

[1] Edwin Sturrus and Olga Kulikova, " Identity and Access Management", KPMG Advisory N.V., the Netherlands
[2] The role of authentication in identity management, A Penn State Identity Services(IdS) White Paper; October 2014, http://www.identity.psu.edu/resources/documentation/current/the-role-of-authentication
[3] The Role of Authorization in Identity Management , A Penn State Identity Services (IdS) White Paper; October2014,http://www.identity.psu.edu/resources/documentation/current/the-role-of-authorization
[4] Lamport, L, " Password authentication with insecure communication.", communications of the ACM 24,770-772.
[5] kumarManoj, BalyanAayushi," Security vulnerabilities of a novel remote user authentication scheme using smart card based on ECDLP",in contemporary computing (pp 252-259), Springer Berlin Heidelberg.
[6] Min- Shiang Hwang, Tsuei- Hung Sun, "Using smart card to achieve a single sign-on for multiple cloud services", in IETE technical review, 30(5), 410-416.
[7] TsaurWoei-Jiunn, Lee Wei-Bin,"An efficient and secure multi-server authentication scheme with key agreement", journal of Systems and Software, 85(4), 876-882.
[8] Hwang, M.S., Chong S.K., and Chen,T.Y., "DoS -resistant ID -based password authentication scheme using smart cards", Journal of Systems and Software, 83(1), 163-172.
[9] Choudhury, A.J., Kumar P., Sain, M., Lim, H., and Jae-Lee, H," A strong user authentication framework for cloud computing .", in Services Computing Conference(APSCC) ,2011 IEE Asia-Pacific (pp. 110-115) IEEE.
[10] Abderrahim AbdellaouiA, "Novel Strong Password Generator for Improving Cloud Authentication", International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science 85 (2016) 293 – 300.
[11] Naoufal Ben Bouazza*, MouadLemoudden*, Bouabid El Ouahidi,"Surveing the challenges and requirements for identity in the Cloud", in proceedings of the 4thof National , 12-13 May 2014, IEEE.
[12] I. Indu, P. M. Rubesh Anand,"Identity and Access Management for Cloud Web Services",2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS) | 10-12 December 2015 | Trivandrum.
[13] AbderrahimAbdellaoui a, *, Younes IdrissiKhamlichib , Habiba Chaoui a ,"A Novel Strong Password Generator for Improving Cloud Authentication", in Procedia Computer Science 85 (2016) 293 – 300.