International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 8, August - 2014

A Review of Graphical Image as Authentication Approaches in Cloud Computing

Teshu Gaurav Singh
Student Department of CSE
DIMAT Raipur
Chhattisgarh, India

Mr. Somesh Dewangan
Professor Department of CSE
DIMAT Raipur
Chhattisgarh, India

Dhairya Kumar Gopal
Department of CSE
KITE Raipur
Chhattisgarh, India

***Abstract*- Graphical password is somewhat better than alphanumeric password. Images and photos are easy to remember than digits or alphabets, but images takes more space than alphabets or numbers. So we need some kind of optimization. In this paper we are representing the authentication given to cloud by using graphical password with better space & time complexity. We proposed an algorithm in which username & password is given. Password is graphical password. This can be similar to another existing methods but it will reduce the complexity of some of the existing algorithms.**

Keywords- Graphical password, Password optimization, Secure Cloud authentication, ease to remember, Shoulder Surfing, Dictionary attacks.

I. INTRODUCTION

Recently there has been a great emphasis to provide more security for passwords. The 21st century stands out as the more advancing age of world-wide-web and related contents, highly exposing information which innovated before a second or say in respect of many seconds. Probably the most traditional opportinity for authentication is textual Pass word. Users first option for authentication is often textual passwords. Mostly users select short and simple password to be able to be easily memorized and is particularly usually recalled on the login-time. In common many experts have surveyed that the normal users is required to memorize at the very least 3 account particulars. again in addition to this the user has got to remember password for banking, e-commerce, social networking sites together with email accounts. Short and uncomplicated textual passwords are simple remember, but might be easily hacked whilst random and lengthy passwords are secured but hard to think about. to overcome this matter visual authentication systems were proposed. But in addition in today's changing world these were easily prone to shoulder surfing assaults. Many others authentication schemes was proposed to overcome the shoulder browsing on attacks but such a can at least assist in improving the performance of graphical private information authentication scheme.

II. LITERATURE REVIEW

1. Secure User Authentication in Cloud Computing Management Interfaces-Liliana F. B. Soares et.al.-

This report proposed variable factor authentication. The convergence to help Single Sign-On (SSO) models is being used to eradicate or decrease account password management complexity.
Such mechanisms could be based on public-key cryptography and might resort to several technologies to boost user knowledge, specifically Quick Response (QR) limits, Short Message Services (SMSes), Honest Program Modules (TPMs), as effectively as contactless Near Industry Connection (NFC). Another trend leans towards adoption of risk-based authentication. Efforts for locking down authentication are mainly being undertaken with the Initiative for Open up AuTHentication (OATH) with the Fast IDentity On the world wide web (FIDO) alliance. Security is offered from proxy gateway level.

Advantages-
authentication could be evolving to device-centric and user-centric.

Disadvantages-
Phishing attack & spam attack can be possible in this technique.

2. Multi-level Authentication Technique for Accessing Cloud Services-

This paper provides the rigid authentication system by introducing the particular multi-level authentication technique which generates/authenticates the particular password in multiple levels obtain the cloud solutions. In this particular report, details of offered multilevel authentication technique are presented as well as the architecture, activities, information flows, algorithms in addition to probability of accomplishment in smashing authentication.

This method has two distinct entities:

i) Cloud service provider, and
ii) Authenticated customer corporations that gain access to the particular cloud solutions.

Cloud service corporation, provides the solutions & Authenticate users develop the effect of checking the understanding before using cloud.

Various levels connected with password authentication/generation are-

(1) Organization level.
(2) Team level.
(3) User Level.

There can be multiple levels involving level two & level 3.

Advantages-

- This method gives multiple advanced of security, which is much better then previous methods.

- Hacker need to help break the password in any respect level.

Disavantages-

- It's realy tedious work not to ever forget multiple passwords.

(3). Grid Based Scheme - Authentication Using Graphical Password in Cloud, Ming-Huang Guo et.al.-

A grid contain multiple number connected with blocks. User have to select a routine blocks. Back ground of grid is going to be some images. User think that he is choosing the sequence connected with images, but actually he's planning to select a routine of grid prevents.

That selected sequence will possibly be user's all occasion password.

Advatage-

- Very simple remember.

Disadvantage-

- Shoulder Searching, Thesaurus attacks. may be possible with this structure.

(4) Multi-factor Authentication Framework for Cloud Computing- Rohitash Kumar Banyal et.al.

Security at static occasion is hack ready. Suppose if all of us blocked any user by 10, 000 static indicates, then a creative hacker can just find a new opportinity intended for hacking. So security from dynamic time is very much required. Giving security from dynamic time is very difficult task, but this report gives an algorithm to present security dynamically. Suggested a shared authentication structure between user & impair.
This method offered three steps-

(1) Sign up Phase.
(2) Get access Stage.
(3) Impair Authentication Phase.

User ought of do their sign up honestly. Then mutual authentication is conducted between user & cloud.

Advantages-

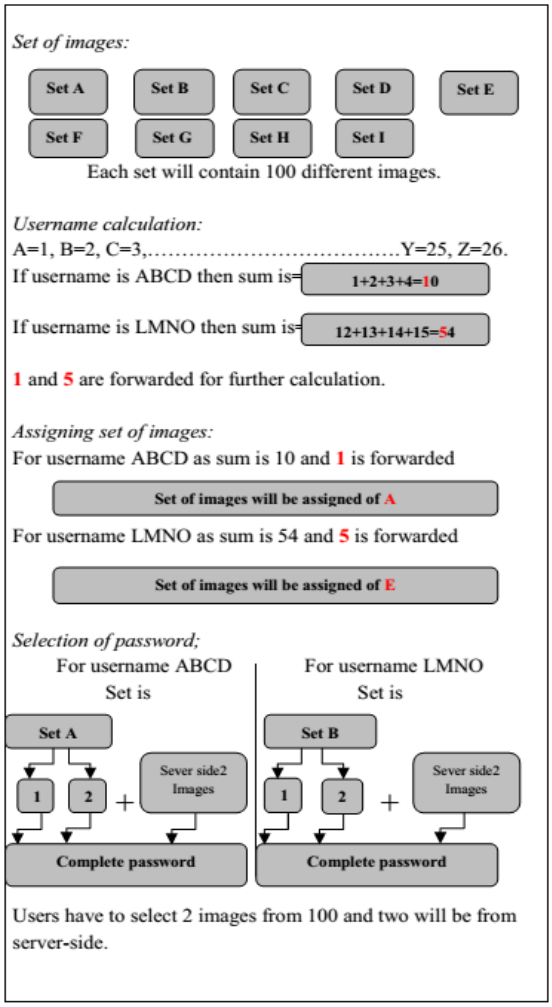
- Multi-level dynamic protection provide greater advanced of security.

Disadvatage-

- User identification vary. Its very trial to identify appropriate user accurately.
- Spoofing attack can be possible in this technique.

(5) Graphical Password Authentication-ShraddhaM. Gurav et.al

This paper proposed very easy method and that is simple to remember. In the offered method user should get into their username. On the basis of user name some pictures are caused. user selects any one of these that will be his in history password.



Advantages-

- Highly safeguarded Mechanism.
- Very easy to not forget password on an extended time.

Disadvantage-

- Shoulder Surfing & Dictionary attack can be possible in this structure.
- It will take more space in database. So processing might be very slow.

Table:- Comparision table of literature review

Performance Matrices	Lilina F.B. et.al	Rasib Hana khan et al [10]	Rohitash Kumar Banyal et al [11]	Dinesha H A et al[12]	Ming-Haung Guo et al [13]	Dhairya Kumar et al	Shradha M. Gurav
Identity Manage-ment	YES	YES	YES	YES	YES	YES	YES
USER Privacy	YES	YES	YES	YES	YES	YES	YES
Mutual Authentication	YES	YES	YES	YES	YES	YES	YES
Password Change	NO	NO	YES	N0	YES	YES	YES
Session Key Agreement	NO	NO	YES	YES	YES	NO	NO
Replay Attack	YES	YES	YES	NO	YES	YES	YES
MITM	YES	NO	YES	YES	YES	NO	YES
DOS	YES	NO	NO	NO	NO	YES	NO
Impersonation Attack	NO	NO	YES	NO	YES	NO	YES
Password Guessing Attack	NO	NO	YES	NO	YES	YES	YES
GUI	NO	NO	YES	YES	YES	YES	YES
Dynamic Security	NO	NO	YES	YES	YES	YES	YES
Phishing Attack	NO	YES	YES	NO	YES	NO	YES
Ease to Remember	NO	NO	NO	YES	YES	YES	YES

III. GAPS IN LITERATURE REVIEW

(1)Shoulder Surfing- ShraddhaM. Gurav et.al proposed a very nice,, new & secure mechanism. All graphical password are easy to remember but shoulder surfing is very easy task for attacker. When user selects his password at registration phase unauthorized person can see easily his selected password. Although this scheme is very much secure then older schemes , but it need to store a huge number of images, which slows down the processing speed.

(2)Dictionary attacks- attacker can try for all the words from dictionary randomly. If any one of them matched its going to process login phase.

(3)User Identification - User identification can vary. Its very difficult task to identify correct user accurately. If we will go for fact or common identification it will be very easy task for dictionary attacker to guess the corrct password.

(4)Spoofing Attack

(5)Space & Time complexity- If we are going for graphical password rather than alphanumeric password, its going to take more space & will cause to slow down our process, while retrieving the data.So during Graphical

password we must take care about space & time complexity.

(6)**Multiple Password**-Providing multiple password to user is one of the easiest way to secure the system but remembering multiple password can be a tedious task for user.

(7)Phishiung Attack & Spam Attack-

IV. FUTURE SCOPE

Providing static time security is less secure than dynamic security mechanism. Our system is dynamically secure but in future we will need is more dynamic mechanism to secure our data.During graphical password processing speed is a biggest concern. So in future mechanism can be analyzed & faster scheme can be implemented with highly security.

V. CONCLUSION

Alphanumeric password is not an easy task to remember when we have a huge number of password to remember. What solution is graphical password. But graphical password is an easy task to guess. For that some schemes provide a set of images on the basis of user name, So its very tedious task to guess images among different set of images. But another problem arise is processing speed more image will take more space, so processing speed is going to be slow. What we need is some kind of optimization.

VI. ACKNOWLEDGMENT

I am very much grateful to Department of CSE, DIMAT to give me opportunity to work on graphical image as approach to authentication process in cloud.. I sincerely express my gratitude to Mr. Somesh Dewangan, Dept. of MCA, DIMAT for giving constant inspiration to complete this work. I am really thankful to my all friends for their blessing and support.

VII. REFERENCES

1. Graphical Password Authentication system in an implicit manner,SUCHITA SAWLA*, ASHVINI FULKAR, ZUBIN KHAN Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India. March 15, 2012.
2. Secure User Authentication in Cloud Computing Management Interfaces.Liliana F. B. Soares, Diogo A. B. Fernandes, Mário M. Freire and Pedro R. M. Inácio Instituto de Telecomunicações, Department of Computer Science, University of Beira Interior Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal Emails: {lsoares,dfernandes}@penhas.di.ubi.pt, mario,inacio}@di.ubi.pt
3. Multi-factor Authentication Framework for Cloud Computing Rohitash Kumar Banyal Dept. of Computer Engineering Rajasthan Technical University Kota, Rajasthan, Iindia e-mail: rkbayal@gmail.com et.al 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation
4. Graphical Password Authentication , Cloud securing scheme - ShraddhaM. Gurav et.al 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies
5. Authentication Using Graphical Password in Cloud Ming-Huang Guo, Horng-Twu Liaw, Li-Lin Hsiao, Chih-Yuan Huang Department of Information Management Shih Hsin University Taipei, Taiwan {mhguo, htliaw,, Hsiao}@cc.shu.edu.tw,
6. mikehuang.tw@gmail.com, et.al
7. Multi-level Authentication Technique for Accessing Cloud Services Dinesha H A Agrawal V K CORI CORI Bangalore, Karnataka Bangalore, Karnataka sridini@gmail.com vk.agrawal@pes.edu .
8. Open ID Authentication As A Servicein Open Stack asib Hassan Khan, Jukka Ylitalotand Abu Shohel Ahmed* Aalto University, School of Science and Technology, Finland t Ericsson Research, Finland Royal Institute of Technology(KTH),School of ICT, Sweden rkhan@cc.hut.fi, jukka.ylitalo@ericsson.com ,ahmed.shohel@ericsson.com 2011 7th International Conference on Information Assurance and Security(IAS)
9. Graphical Passwords as Browser Extension:Implementation and Usability Study- Kemal Bicakci et.al research is supported by TUBİTAK (The Scientific and Technological Research Council of Turkey) under project number 107E227.
10. Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme Susan Wiedenbeck and Jim Waters College of IST Drexel University Philadelphia, PA 19104 USA {sw53, jw65}@drexel.edu et.al
11. Shoulder Surfing Resistant Password Authentication Mechanism (Using Convex hull Click Scheme) Professor Sandeep Samleti ,Chandan Kumar , Vijay Prakash Nitin Kumar, Sunil Kumar Department of Information Technology, Army Institute of Technology Pune, India.
12. A Survey on Recognition-Based Graphical User
13. Authentication Algorithms Farnaz Towhidi Centre for Advanced Software Engineering, University Technology Malaysia Kuala Lumpur, Malaysia farnaz.towhidi@gmail.com (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.