International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

An Optimized Approach to Secure Password through Graphical Images in Cloud Computing

Teshu Gaurav Singh[1], Mr. Somesh Dewangan[2], Dhairya Kumar Gopal[3]

[1] Student Department of CSE, DIMAT Raipur, Chhattisgarh, India
Teshu.singh@gmail.com

[2] Professor Department of CSE, DIMAT Raipur, Chhattisgarh, India
Somesh_4@yahoo.co.in

[3] Asst. Professor Department of CSE, KITE Raipur, Chhattisgarh, India
dhairayagopal@gmail.com

Abstract: ***The evolution of cloud computing is driving the next generation of internet services. Alphanumeric password is difficult to remember. Rather than that graphical password is better option. Images and photos are all to easy to remember than numbers or alphabets, nevertheless images takes far more space than alphabets or maybe numbers. So we need an optimization. In this paper we have been representing the authentication fond of cloud by applying graphical password using better space & time period complexity. We proposed an algorithm during which username & password is given. Code is graphical password. This can be just like another existing methods but it will reduce the actual complexity of a few of the existing algorithms.***

Keywords: *Graphical password, Password optimization, Secure Cloud authentication, eases to remember, Shoulder Surfing, Dictionary attacks.*

1. Introduction

Cloud computing is a new paradigm for utilization of scalable resources over the internet. It is a relatively new cyber infrastructure, implying service oriented architecture (SOA) for computing resources.Recently there has been a great emphasis to offer more security for passwords. The 21st century is definitely the more advancing age of world-wide-web as well as related contents, highly exposing data which innovated before an additional or say in respect of many just a few seconds. Probably much traditional opportunity for authentication is textual Security password. Users' first alternative for authentication is frequently textual passwords. Mostly users choose short and simple password to be able to be easily memorized and it is usually recalled on the login-time. In common many experts have surveyed that the normal users is necessary to memorize at the very least 3 account points. again in addition for this the user needs to remember password for banking, e-commerce, online community sites together having email accounts. Limited and uncomplicated textual passwords are simple remember, but might end up being easily hacked although random and lengthy passwords are attached but hard to take into account. to overcome that matter graphical authentication systems were proposed. And also in today's changing world they were easily prone to be able to shoulder surfing catches. Many others authentication strategies was proposed to be able to overcome the glen humeral joint browsing on attacks but a real can at least assist in improving the overall performance of graphical information authentication scheme.

2. Author Name(S) And Affiliation(S)

2.1. 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 (SMS), 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.

2.2. 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.

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

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

A grid contains multiple number connected with blocks. User have to select a routine blocks. Back ground of grid is going to become 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.

Advantage-
- Very simple remember.

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

2.4. 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 opportunity 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.

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

2.5. 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.

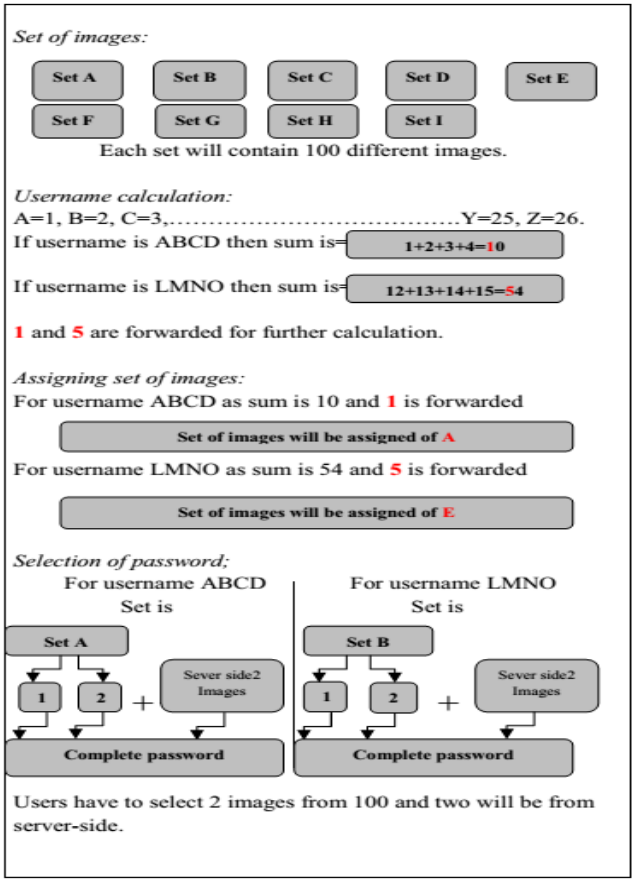

Figure 1: Password generation through images

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.

3. Gaps in Literature Review

3.1 Shoulder Surfing-

Shraddha M. Guravet.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.

3.2 Dictionary attacks

Attacker can try for all the words from dictionary randomly. If any one of them matched it's going to process login phase.

3.3 User Identification

User identification can vary. It is 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 correct password.

3.4 Spoofing Attack

A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypasses access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this.

3.5 Space & Time complexity

If we are going for graphical password rather than alphanumeric password, it's 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.

3.6 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.

Table 1: Comparison 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-HaungGuo 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

4. Problem Identification

Integration of mobile devices with collaborative applications is crucial for the following reasons (apart from the conventional reasons related to availability of heterogeneous and collective computing and communication resources):

The most current information resides on mobile devices: e.g., user specific data like the location, users' decisions such as schedules, policies and any other user parameters.

Synergy brought in by the multitudes of handheld devices needs to be leveraged by Internet/Grid infrastructures (e.g., disaster evacuation re-routing on a college campus based on collective perception and real-time collaboration).

A backup networking infrastructure can be provided by mobile server devices, which is crucial in case of sabotage or transient outage of the power grid or the backbone network. For example, if handheld devices of staff and police are enabled to serve as ad-hoc network nodes in sports stadiums, college campuses, airports or malls, emergency rerouting in case of a backbone outage can still be performed and people can employ their mobile devices to query real-time evacuation information pertaining to their location in the format/language of their choice. Rapid incremental

reprogramming to effect structural changes in the collaborative applications can help when response is needed to emergencies/disasters or emerging situations. The tragic events of September 11 powerfully demonstrate the need for such a system. Despite the fact that New York City already had a disaster plan, their ability to handle the attack was limited. Their disaster coordination base, located under the Twin Towers was destroyed, as was the Verizon telephone switching station nearby. The loss of these two facilities crippled the ability of the authorities to effectively coordinate personnel and resources, with possibly tragic consequences.

These factors make for a strong case for putting server functionality on mobile devices – this can usher in the quantum change needed for the next generation of collaborative applications. To integrate a variety of heterogeneous, possibly mobile, devices with varying data formats, operating systems, network protocols, and computing and communications capabilities, an adaptive yet uniform view is a must. Typical heterogeneous environments would include legacy applications, and mobile devices with limited resources and weak connectivity. We need to develop techniques to enable handheld servers to support multiple transaction states and maintain consistency despite disconnection.

5. Proposed Methodology

In proposed methodology I used set of graphical image with alphanumeric password.
Set of images:-

Figure 2: Set of images

Each set will contain 20 different images. User name calculations A=0, B=1,C=2,D=3,E=4,……Y=24,Z=25.

Example 1). If username is ABCD then sum is =

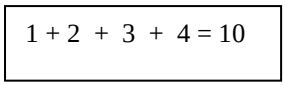

Figure 3: An example to set images counting.

1=B has 20 set of images.
0=A has another 20 set of images.
Those 20 & 20 images will mix up & will form new set of 400 images at client side only. User has to select any one from those 400 images & finally that image will be user password.

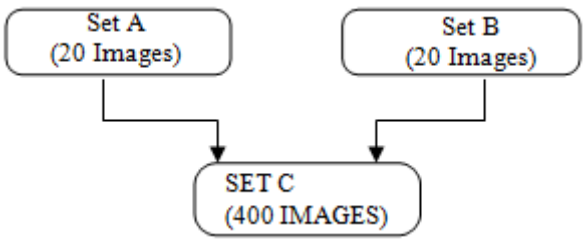

Figure 4: Creating a new image combination of images.

Example 2) If username is LMNO then sum is 12+13+14+15.=54
5=D has 20 set of images.
4= E has another 20 set of images.
Those 20 +20 will form another 400 images.
User has to select any one from them.
& the same will user password.

6. 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. Neural Network techniques can be used to achieve high level of security. Neural Network is best technique for inconsistent data.

7. Conclusion

Alphanumeric password is not an easy task to remember when we have a huge number of passwords 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, Soits 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. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However this scheme is completely new to the users and the proposed authentication techniques should be verified extensive. The research performed during this work revealed further possibilities. The first objective would be to introduce greater flexibility in the choice of authentication mechanisms for the user. To provide a generic solution for authentication, we aim to design a common Authentication-as-a-Service API in OpenStack. Additionally, we also aim to introduce open platforms for authorization delegation within OpenStack.

8. 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.

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] Author1_Name, Author2_Name, Web Caching and Replication, Addison-Wesley(Publication_ Name), USA, 2014
[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.comet.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-TwuLiaw, Li-Lin Hsiao, Chih-Yuan Huang Department of Information Management Shih Hsin University Taipei, Taiwan {mhguo, htliaw,, Hsiao}@cc.shu.edu.tw, mikehuang.tw@gmail.com, et.al
[6] 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
[7] Open ID Authentication As A Servicein Open Stack asib Hassan Khan, JukkaYlitalotand 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.co,ahmed.shohel @ericsson.com 20117thInternationalConferenceonInformationAssuranceandSecurity(IAS)

Author Profile

Teshu Gaurav Singh received the B.E. degree in Computer Science & Engineering from ITGGDU Bilaspur (C.G.) in2007. He completed C-DAC(DAC) from MET Mumbai. Recently he is M.Tech. scholar from DIMAT, Raipur(C.G.)