Indonesian Journal of Electrical Engineering and Computer Science
Vol. 7, No. 2, August 2017, pp. 507 ~ 513
DOI: 10.11591/ijeecs.v7.i2.pp507-513

Qualitative Analysis of Recognition-Based Graphical Password Authentication Schemes for Accessing the Cloud

K Gangadhara Rao[1], R Vijayakumari*[2], B Basaveswara Rao[3]
[1]Dept. of Computer Science, Acharya Nagarjuna Universiy, Guntur, India
[2]Dept. of Computer Science, Krishna University, Machilipatnam, India
[3]Dept. of Computer Science, Acharya Nagarjuna Universiy, Guntur, India
Corresponding author, e-mail: kancherla123@gmail.com[1], vijayakumari28@gmail.com*[2], bbrao@alu.ac.in[3]

Abstract

Cloud computing is increasingly becoming popular as many enterprise applications and data are moving into cloud platforms. However, a major barrier for cloud application is real and perceived lack of security. There are many security mechanisms exercised to utilize cloud services. Amongst them the prominent and primitive security mechanism is the Authentication System. Traditional text based passwords are susceptible to threats. Tough passwords are hard to recall and easily recalled passwords are simple and predictable. Graphical passwords are introduced as the better alternative. Two types of graphical passwords are there-recall based and recognition based. This research reviews several Recognition-Based Graphical Password methods and analyses their security based on the estimation criteria. Moreover, the research defines a metric called a 14-point scale that would make it possible for the qualitative analysis of the graphical passwords schemes.

Keywords*: Cloud, Authentication, Graphical Passwords, Usability, Security*

1. Introduction

Cloud computing is gaining much popularity in recent years. Many organizations are attracted by its characteristics like on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service [1] and advantages such as business ease and financial saving. Thus, these organizations try to shift to the cloud infrastructure in order to exploit its advantages. Cloud computing is an automated technology service, which deliver in addition to networking and storage, customer relationship management. It is an economic model based on a hugely scalable IT platform (Data Center) to reduce the cost of provisioning, operating and de-operating its resources. This concept is very cost efficient and it provides access to almost unlimited storage. However, some recent development in cloud computing have heightened the need for promoting the security in this environment from a different security perspective (authentication, confidentiality, integrity, non-repudiation, availability), particularly cloud authentication. In fact, the safety and security of sensitive user data and applications in the cloud environment relies primarily on user authentication. As a matter of fact, the authentication feature is one of the most important security characteristics of whatever system, particularly, the cloud system. It enables verifying the legitimacy of the users before accessing to cloud resources. There are many authentication schemes that have been proposed in recent years following different approaches, specifically, we can distinguish, text password, multi-factor authentication, 3D password, third party authentication, biometric scans and graphical password. Furthermore, it has been recently shown that text-based password is the most used method among the previously cited methods. However, according to many research studies [2-8, 9,10,11,12], due to its vulnerabilities such as dictionary and brute-force attacks, key-loggers, shoulder surfing and social engineering, the text-based password scheme remains a quite weak authentication method for the cloud environment even if its ease of use. The next best alternative is the graphical password authentication system as it is economic and also motivated particularly by the fact that humans can remember pictures better than text [13]. Graphical passwords are two types- recall based and recognition based. In recognition-based methods, a

Received May 14, 2017; Revised July 11, 2017; Accepted July 26, 2017

user is given an arrangement of pictures and the client gets validated by perceiving and distinguishing the pictures, he or she chooses at the registration stage. In recall-based methods, a user is requested to recreate something that he or she made at the registration stage. This paper focuses on recognition based graphical password schemes for the purpose of analysis. It discusses on existing recognition based graphical password techniques, and possible attacks on those techniques and there by the reliability of the specified techniques by considering fourteen parameters.

2. Recognition-Based Graphical Password Schemes

Shraddha M Gurav et al [14] proposed a scheme for securing the cloud by means of image password. During registration, a set of images will be given to user, based on some calculations on the username. User has to select two images from them and two images will be given from server side. It forms full password and is stored in the database. To login to the system, user has to enter username and identify appropriate pass pictures and click on them to get access to the cloud. Sumit et al [15] proposed a shoulder surfing resistant text based graphical password scheme which consists of a circle divided into six sectors. Each sector contains twelve characters. User has to register his password and sector during registration. At the time of login, he has to rotate the sector containing the pass character into his designated sector, and then confirms it. He repeats it for N number of times where N is the length of the password. After finishing all the passes, user is allowed to access the system. This system is a bit confusing for the normal user.

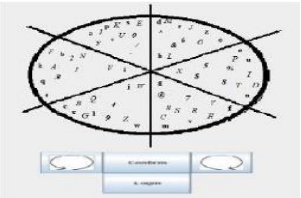

Figure 1. Scheme by Sumit et al [15]

Figure 2. Scheme by kameswara Rao et al [16]

Another shoulder surfing resistant graphical password authentication mechanism was proposed by Kameswara Rao et al [16]. In this mechanism, user password is processed as pass-characters one pair at a time sliding to the right one character at a time, wrapping around until the last pass-character forms the first element in the pair. Once the pass characters are identified, each pair is processed separately using predefined rules. Amish shah et al [17] proposed another shoulder-surfing resistant graphical password system to minimize the search time to find the pass-images on a login screen. This scheme uses texts in images instead of objects such that quicker recognition can take place. Each and every image has two characters in it. The user can select an alpha numeric pass phrase at the time of registration. During login, the user will have to move the frames with appropriate characters and arrange them as per the alignment chosen during registration.

aa	ac	af	aj	ao	au	bb
ab	ae	ai	an	at	ba	bh
ad	ah	am	as	az	bg	bm
ag	al	ar	ay	bf	bl	bq
ak	aq	ax	be	bk	bp	bt
ap	aw	bd	bj	bo	bs	bv
av	bc	bi	bn	br	bu	bw

Figure 3. Scheme proposed by Amish shah et al [17]

Figure 4. Scheme proposed by Abutalha et al [18]

Abutalha et al [18] proposed an alignment based graphical password scheme. It has two phases: select, training phase and identification phase. In first phase, user has to register username and password pictures. He is also trained to remember images in this phase. In the second phase, user has to identify and align the pass pictures displayed in circles. The number of circles displayed is equal to number of password pictures selected. Each and every circle consists only one pass picture during login. So, he has to align them and submit them to get access to the system. Another graphical password scheme was proposed by MK Rao et al [19] which combines both recall based and recognition based techniques. First, user has to produce an age sequence in recall phase and later, at every selected age the registered image must be identified in recognition phase. This scheme also provides the recovery system for the password, but it burdens the user by making him remember too many things in sequence for a password.

Figure 5. Scheme proposed by MK Rao et al [19]

Figure 6. Scheme proposed by Mrs.Gokhale et al [20]

Mrs.Gokhale et al [20] introduced a graphical password technique which has two phases called registration and login. During registration, the user has to select some even number of images to set as a password. Later, any other picture can be selected by the user to select any three questions. The answers to the questions must be any three regions on the later selected image. User has to click on region of answers and save them for login purpose along with his other details. During login, the user has to select the appropriate images and also answer the questions correctly. K. Gangadhara Rao et al [21] proposed a click based graphical password authentication system. There are two phases – registration and login. The user has to register by giving his username and password and the selected password is shifted circularly to the right by one character and stored in the database. Login procedure happens in four sages and in each stage the entered input is compared with the rotated, stored, password string by shifting one character to the left by 'n' number of times. Here 'n' represents the number of iteration. If all the four stages are successfully passed by the user, then he is allowed to access the system.

Figure 7. Scheme proposed by K Gangadhara Rao et al [20]

3. Possible Attacks on Recognition-Based Graphical Password Schemes

In this section, we discuss about the various types of attacks possible on Recognition-Based Graphical Password Schemes. Basing on the Common Attack Pattern Enumeration and Classification (CAPEC), the present attacks on recognition-based graphical passwords have

been identified and classified into six types. Such as dictionary attack, brute force attack, spyware attack, social engineering attack and guessing attack.

3.1 Dictionary Attack

Recognition based passwords use mouse to provide input rather than keyboard. Therefore they are less vulnerable to dictionary attacks like textual passwords. But still dictionary attacks are conducted by attackers on recognition-based graphical passwords by identifying passwords that users will most likely choose. This identified list is used systematically to crack the password. The attackers try to estimate the password space effectively. If prioritized entries are used to first test the most likely passwords, the dictionary attacks can be almost successful.

3.2 Brute Force Attack

Brute force attack is carried out just like the dictionary attack, except that each potential password possibility is created and utilized to attack the genuine password. These possibilities are also prioritized in more high strung threats, in order to reduce the possibility of being chosen by the user, if at all these possibilities can be guessed [6]. Brute force attack also known as Exhaustive Attack, can be carried out either online or offline. Unlike dictionary attack, the exhaustive attack provides a higher coverage but needs more processing power or time.

The method of defense against this kind of attack can be to possess a large enough password space. Text based passwords have a password space $(94)^K$ where K is the number of printable characters on the keyboard excluding the space. Generally, graphical password schemes also offer similar password space that of text based or even larger. '4-Stage Graphical Password Authentication Scheme' is a text based graphical password and its password space is $3.0495x10^6$.

3.3 Spyware Attack

In this type of attack, the user's computer is installed with some special tools which are used to record the sensitive data without his/her knowledge. Using this malware, any key or mouse movement is recorded and will be reported back outside the computer. Except in rare cases, the key listening or key logging spyware cannot be utilized to hacek the graphical password since it is not yet proven if the mouse spyware is an effective mechanism to crack a graphical password. Though the mouse tracking is successfully saved using a spyware, it is not enough to hack a graphical password. Because, other additional information such as window size and position are necessary to crack a password.

3.4 Social Engineering Attack

Social engineering is an approach of obtaining confidential information by manipulating the genuine users. The attackers of this type normally use the telephone or e-mail to trick a person into revealing their sensitive information. They act like as if they are from user's bank or credit card company etc. and enquire about the user's personal information. In case of textual passwords, it is easier to get a password or credential from a legitimate user than attempting to hack into a secured system. Whereas, a graphical password cannot be revealed to someone else. It cannot even be revealed over the telephone. It would be more time consuming to set up a phishing website just to crack a graphical password.

3.5 Guessing Attack

Password guessing attacks can be broadly classified as offline dictionary and online password guessing attacks. Users commonly choose passwords basing on some personal information like pet names, family names, and birth dates etc. Hackers attempt to guess passwords by trying out these possible passwords. The password may be textual or graphical, can be guessed by hackers up to some extent. '4-Stage Graphical Password Authentication Technique' is resistant to guessing attack. Because, though the password is guessed by the hacker, the input is taken in a special process which is unknown to user.

3.6 Shoulder Surfing Attack

Shoulder surfing is the technique of gaining knowledge of user's credentials via observing them directly or recording through video cameras as user computes the information.

The availability of high resolution cameras with surveillance equipment and telephoto lenses cause shoulder-surfing to be a major threat if attackers are specifically targeting users and have access to these users' geographic location. This is particularly troublesome in a public environment, but it is a more serious threat in a private environment. Similar to textual passwords, more graphical passwords are at risk of shoulder surfing. Right now there are just several recognition based techniques designed to confront the issue of shoulder surfing. Not one of the recall based technique is regarded as being resistant to shoulder surfing.

4. Reliability

In this section, we analyze the discussed schemes considering two parameters usability and security.

Table 1. Usability and Security Features of different graphical password techniques

		Usability Features							Security Features/Possible Attacks						
Serial No.	Graphical Password Schema	Saving Time	Saving Space	Simple	Uses Mouse	Text Based	Easily Trained	Easy to Remember	Random Display	Dictionary Attack	Brute Force Attack	Spyware Attack	Social Engineering Attack	Guessing Attack	Shoulder Surfing Attack
1	Scheme proposed by Shraddha M Gurav et al [14]	Y	N	Y	Y	N	Y	Y	N	Y	N	N	N	N	Y
2	Scheme proposed by Sumit et al [15]	N	Y	Y	Y	Y	N	Y	N	Y	N	N	N	N	Y
3	Scheme proposed by Kameswara Rao et al [16]	Y	N	N	Y	Y	N	Y	Y	Y	Y	N	N	N	Y
4	Scheme proposed by Amish shah et al [17]	Y	Y	N	Y	Y	N	N	N	Y	N	N	N	N	Y
5	Scheme proposed by Abutalha et al [18]	N	N	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y
6	Scheme proposed by MK Rao et al [19]	N	N	N	Y	N	Y	N	Y	Y	N	N	N	N	Y
7	Scheme proposed by Mrs.Gokhale et al [20]	Y	Y	N	Y	N	N	Y	Y	Y	Y	N	N	Y	Y
8	Scheme proposed by K.Gangadhara Rao et al [20]	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y

Table 2. A fourteen point evaluation of different graphical password schemes

S.No	Graphical Password Schema	A fourteen point scale of efficiency
1	Scheme proposed by Shraddha M Gurav et al [14]	7
2	Scheme proposed by Sumit et al [15]	7
3	Scheme proposed by Kameswara Rao et al [16]	8
4	Scheme proposed by Amish shah et al [17]	6
5	Scheme proposed by Abutalha et al [18]	8
6	Scheme proposed by MK Rao et al [19]	5
7	Scheme proposed by Mrs.Gokhale et al [20]	9
8	Scheme proposed by K.Gangadhara Rao et al [20]	12

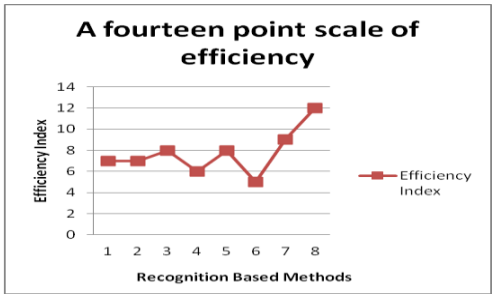

Figure 8. A line graph of fourteen point scale of efficiency scale

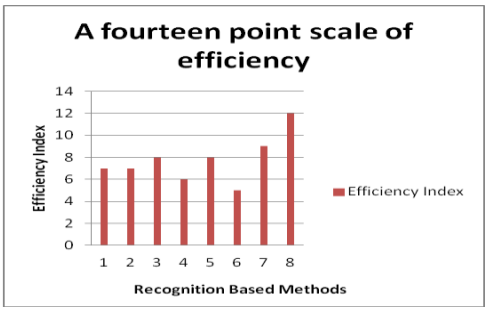

Figure 9. A histogram of a fourteen point scale of efficiency scale

5. Conclusion

Cloud computing is the fundamental change happening in the field of information technology. It is a representation of a movement towards the intensive large scale specialization. On the other hand it brings about not only convenience and efficiency problems, but also great challenges in the field of security. Authentication is one such challenge. Apart from traditional textual authentication mechanisms, there are other secure authentication mechanisms like fingerprint authentication, etc for accessing cloud [22-23]. But, they are all expensive. Graphical password authentication is the best alternative. In this paper, we have discussed various recognition based graphical password schemes for authenticating a user to get access to the cloud. We tried to analyze the specified schemes by considering two categories of parameters – usability and security features. And then, we used a fourteen point scale to evaluate the efficiency of the discussed recognition based graphical password schemes for authentication.

References

[1] Mell P, Grance T. The NIST definition of cloud computing.
[2] Hwang MS, Sun TH. Using smart card to achieve a single sign-on for multiple cloud services. *IETE Technical Review*. 2013; 30(5): 410-6.
[3] Tsaur WJ, Li JH, Lee WB. An efficient and secure multi-server authentication scheme with key agreement. *Journal of Systems and Software*. 2012; 85(4): 876-82.
[4] Hwang MS, Chong SK, Chen TY. DoS-resistant ID-based password authentication scheme using smart cards. *Journal of Systems and Software*. 2010; 83(1): 163-72.
[5] Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H. *A strong user authentication framework for cloud computing*. In 2011 IEEE Asia-Pacific Services Computing Conference (APSCC), IEEE. 2011: 110-115.
[6] Jaidhar CD. *Enhanced mutual authentication scheme for cloud architecture*. In 2013 IEEE 3rd International Advance Computing Conference (IACC), IEEE. 2013: 70-75.
[7] Yassin AA, Jin H, Ibrahim A, Qiang W, Zou D. *Cloud authentication based on anonymous one-time password*. In Ubiquitous Information Technologies and Applications, Springer Netherlands. 2013: 423-431.

[8] Jivanadham LB, Islam AM, Katayama Y, Komaki S, Baharun S. *Cloud Cognitive Authenticator (CCA): A public cloud computing authentication mechanism*. In 2013 International Conference on Informatics, Electronics & Vision (ICIEV), IEEE. 2013: 1-6.

[9] Moghaddam FF, Moghaddam SG, Rouzbeh S, Araghi SK, Alibeigi NM, Varnosfaderani SD. *A scalable and efficient user authentication scheme for cloud computing environments*. In 2014 IEEE Region 10 Symposium, IEEE. 2014: 508-513.

[10] Sabzevar AP, Stavrou A. *Universal multi-factor authentication using graphical passwords*. In 2008. SITIS'08. IEEE International Conference on Signal Image Technology and Internet Based Systems, IEEE. 2008: 625-632.

[11] Abdellaoui A, Khamlichi YI, Chaoui H. Out-of-band Authentication Using Image-Based One Time Password in the Cloud Environment. *International Journal of Security and Its Applications (IJSIA)*. 2015; 9(12): 35-46.

[12] Abdellaoui A, Khamlichi YI, Chaoui H. An Efficient Framework for Enhancing User Authentication in Cloud Storage Using Digital Watermark. *International Review on Computers and Software (IRECOS)*. 2015; 10(2): 130-6.

[13] Shepard RN. Recognition memory for words, sentences, and pictures. *Journal of verbal Learning and verbal Behavior*. 1967; 6(1): 156-63.

[14] Gurav SM, Gawade LS, Rane PK, Khochare NR. *Graphical password authentication: Cloud securing scheme*. In 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC), IEEE. 2014: 479-483.

[15] Wagh SH, Ambekar AG. Shoulder Surfing Resistant Text-based Graphical Password Scheme.

[16] Rao MK, Pravallika CV, Priyanka G, Kumar M. *A Shoulder-Surfing Resistant Graphical Password Authentication Scheme*. In Innovations in Computer Science and Engineering Springer Singapore. 2016: 105-112.

[17] Shah A, Ved P, Deora A, Jaiswal A, D'silva M. *Shoulder-surfing Resistant Graphical Password System*. Procedia Computer Science. 2015; 45: 477-84.

[18] Danish A, Sharma L, Varshney H, Khan AM. *Alignment based graphical password authentication system*. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), IEEE. 2016: 2950-2954.

[19] Rao MK, Switha TU, Naveen S. *A Novel Graphical Password Authentication Mechanism for Cloud Services*. In Information Systems Design and Intelligent Applications, Springer India. 2016: 447-453.

[20] Gokhale MA, Waghmare VS. *The shoulder surfing resistant graphical password authentication technique*. Procedia Computer Science. 2016; 79: 490-8.

[21] Rao KG, Vijayakumari R, Rao BB. 4-Stage Graphical Password Authentication Scheme for Cloud. *Journal of Theoretical & Applied Information Technology*. 2017; 95(1).

[22] Mala RP, Kumar CJ. Providing Authentication by Using Biometric Multimodal Framework for Cloud Computing. *Indonesian Journal of Electrical Engineering and Computer Science*. 2015; 15(3): 591-6.

[23] Bastina AA, Rama N. Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access. *International Journal of Electrical and Computer Engineering (IJECE)*. 2017; 7(1): 408-16.