International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 9 • Number 45 • 2016

A Comparative Study of Graphical Authentication Techniques for Cloud Based Application

Bhuvnesh Joshi[a] **and Komal Arora**[a]

[a]Department Of Computer Science & Engineering, Lovely Professional University, Punjab

E-mail: bhuvneshonline@gmail.com, komal.17783@lpu.co.in

Abstract: Due to increasing popularity of cloud computing it is becoming a major target of malicious users and more emphasis is now needed to ensure the security of cloud applications. Due to the shared nature of cloud computing environment there are various security concerns including but not limited to privacy, authentication, data leak etc. Authentication being one of the major component of cloud computing security require ongoing efforts to ensure secure working environment. This study is conducted to understand various graphical authentication techniques for cloud application and their comparison in order to identify current state of graphical authentication development in cloud environments.

Keywords: *Cloud Computing, Cloud Security, Graphical Authentication, Authentication, Cloud Application.*

1. INTRODUCTION

1.1. Authentication in Cloud Computing

Authentication is referred to as the mechanism of verifyinga user's identity and to ensure that secured area of application are restricted to personals with sufficient privileges. We generally use four parameters to authenticate an application user:

1. **Individual Knowledge:** Under this we verify users based on information which is only available with a particular them and is unique to every user like password, user id's etc.
2. **Possession of Individual:** Under this we verify users based on their possession's, whichis uniquely available with the each individual likesmart card, emv chip etc.
3. **Individual Physical Features:** Under this we utilize physical features of individual like retina scans, finger prints etc.
4. **Individual Activity:** Under this we utilize individual behavioral characteristics like typing pattern, internet history etc.

Using any of these techniques or combination of these techniques it is possible for us to make a secure system for authentication of users.

1.2. Approach to Knowledge Based Authentication

Due to the nature of authentication use to individual knowledge to authenticate and toidentify user is a general norm. Wherever it is necessary to limit the access to specific individual due to security, privacy or any other reasons.

Over the period of time we have developed multiple techniques and few of the major techniques which are in play in today's applications are:

Alpha Numeric Passwords: It is one of the oldest techniques to authenticate user of a system. Here users are required to provide an alpha numeric character based sequence during the registration with system and every time user is required wants to use the system he or she has to provide the exact same password in order to access the system.

PIN Codes: This techniques is very similar to alpha numeric password but instead of alpha numeric sequence which is generated by the user at the time of registration the service provider generates and provide a numeric only "Personal Identification Number" to the user which serves are the password for the user. Key point here is that PIN here is generated by the application provider to ensure its security and uniqueness.

Graphical Passwords: Since the PIN and alpha numeric password based authentication are prone to various issue like dictionary attacks, key logging brute force etc. A new technique was introduced which suggested that instead of using plain text type data for user authentication we should use graphical data for authentication.

Hybrid Password Techniques: These techniques utilizes various types of user provided data for authentication which can include text, sound sequence based password etc. Combining multiple techniques can generally be very challenging task and can make the system very complex.

Multiple Factor Authentication: Similar to hybrid authentication techniques multiple factor authentication generally uses more than one password in order to authenticate users. Generally it is done with help of unique real-time passwords along with combination of global passwords. These system can be built on multiple factor like two, three or more based on the level of security required by the system.

2. GRAPHICAL AUTHENTICATION

Graphical authentication can take advantage of all four parameters of authentication mentioned in section **1.1.**

1. Graphical Individual Knowledge: Under this we can use various techniques like verification using image recall based password, image matching passwords etc.

2. Graphical Possession of Individual: We can use graphical images which are available only with users and or pattern which can only be created by a specific user.

3. Graphical Individual Physical Features: Under this we utilize physical features of individual like retina scans, finger prints etc.

4. Graphical Individual Activity: Under this we can utilize user behavior in techniques like 3D authentication.

2.1. Advantagesof Graphical Authentication

There are various advantage associated with use of graphical authentication which makes them a good candidate for the authentication mechanism in cloud computing applications.

1. **Difficult to brute force:** Graphical entity generally require a very high amount of time to guess them due to the sheer number of combination which can be developed and nature to graphical data.

2. **Immune to dictionary attacks:** Graphical authentication based on techniques utilizing image patterns, retina scans etc.are generally assumed to be immune of dictionary attacks as obtaining these patterns is not easy task and will require physical interaction or leak from the organization.
3. **Multiple factors for Authentication:** Since graphical authentication method generally use two or more authentication parameters in combination it becomes harder to crack them.
4. **Immune to key logging:** Generally graphical authentication require more user interaction via mouse or vision rather than keyboard this give graphical authentication more immunity towards the key logging based attacks. Also we can implement the feature to avoid issue with general hotspot creation.

2.2. Issues in Graphical Authentication

Although graphical authentication provide us with various advantages but it does have various issues which hinder their utilization in traditional/cloud application environment.

1. **Harder To Implement:** Since graphics based authentication require manipulation of image and related data which becomes difficult to implement as they increase complexity by involving techniques like image processing etc.
2. **Prone to Shoulder Surfing:** Graphical image are prone to shoulder surfing attack as graphical data is easy to recognize and recall.
3. **Higher Resource Requirement:** Graphical data can consume huge amount of bandwidth and processing resourcing which may hinder its graphical authentication application in real world scenario.
4. **Prone to Leak :** Generally we cannot store the graphical data using one way encryption techniques it becomes a challenge to make sure that graphical data for authentication is secured properly and that risk of leaking of data is minimal.
5. **Replay Attack :** Simple graphical authentication techniques are prone to replay attack and it is required that this must be taken into consideration while building a graphical authentication based system.

3. GRAPHICAL AUTHENTICATION TECHNIQUES

Over the period of time there have been different graphical authentication techniques which were proposed and which tried to solve various challenges involved in implementation of graphical authentication techniques.

Recognition Based Systems: In recognition based cloud system, a user is requested to select a set of images at the time of registration and during the time of authenticationit is required that the correct image is being touched by the user in order to successfully authenticate.

Recall Based Systems: In recall based cloud computing systems, the user is required to duplicate something that they generated while registering with the cloud application. Replication of previously generated pattern or graphical sequence is the key in recall based system.

Cued Recall Based Systems: In these type of system user can be presented with hints or instruction which help them to reproduce their password which they registered initially with the cloud system. It is very similar to recall based technique but with added help of providing hints so that user can easily and correctly reproduce the password.

Hybrid Techniques: Hybrid technique as the name suggest utilizes different combination of multiple techniques to either overcome individual disadvantage of the used techniques or to produce a greater depth of difficulty for attackers by introducing multiple factor in authentication which are not easily exploitable.

Multidimensional Authentication: It is a technique in which user will have to perform series of steps in order to authenticate himself to the cloud system. The various steps will contribute to the generation of final password combination which can include data such as images, text password, gestures etc.

Multilevel Authentication: It is an authentication technique in which access to various part of the cloud application to a particular user is provided after performing various level of authentication. Once a user clear the one level of authentication he/she will get access to that level and level below the authenticated level. This approach can be very useful in hierarchical model where users can have various level of access to a particular application.

3.1. Recall Base Techniques

Déjà Vu[1] byDhamija et al., wasone of the recognition based techniques here user will have to select some specific number of images initially at the time of registration with the system. The images which were selected by the users initially were then used by the system at the time of authentication. Whenever user needs to login to the system he or she will be presented with a specific set of images which will be combination of decoy image and the correct images from the initial set provided by the user at the time of registration. User than has to identify the correct images from the given image set if the user can identify the correct image then they will be verified. This techniques is easy to implement but it has some major drawback like remembering complex or closely related images sometimes can leads to confusion among the user during login phase.

PassFaces[2] proposed by Brostoff et al., this recognition based techniques take advantage of the idea that it is easier of humans to remember human faces rather than random images. Here faces are used instead of random images at the time of registration and while logging in users is required to select the faces which were selected at the time of registration. This techniques has some serious problem as due to the ease with which faces can be remembered it is very prone to shoulder surfing, guessing and even other malicious program as the face images are transmitted plane and hence can be grabbed by the malicious program easily.

Story[3] this technique proposed a similar approach as that of PassFaces and it only have one authentication round. In case of this technique we have a unique image sequence, the image sequence and image uniqueness constitute a story. At the time of authentication user is required to choose and arrange the images present in correct order to repeat the story which was presented at the time of registration. Since this techniques is not plain selection based it is less prone to shoulder surfing.

Graphical Password with Icons[4] this technique was proposed to solve the hotspot problem which is very similar to that of key logging in textual password techniques. This technique suggested that at the time of registration users is provided with a system generated 6 icons password and at the time of authentication he or she is presented with a bigger set of icons along with the correct password icons randomly spread. This make sure that users screen behavior is equally spread and make sure that logging mouse click is not easy due to the randomization of icons and large number of available selections. However this techniques suffers with the issue of login time and icon size.

3.2. Recall Based Techniques

Draw A Secret(DAS)[5] in this technique at the time of registration users is requested to draw a password(pattern) on a two dimensional grid using a mouse or stylus. A drawn password can be made up of either one continuous pen/mouse stroke or multiple strokes. To authenticate users have to repeat the drawn pattern which they provided at the time of registration. The system stores the password as collection of coordinates of drawing encoded in form of grid as DAS password. Here user is essentially using a password but without remembering it. This technique have some difficulty in its implementation as it is very difficult to exactly repeat a pattern of drawing and human cannot repeat a task like stroke exactly same as before due to lack of absolute control.

Passdoodles[6] by Varenhorst is a techniques which is one of the recall based techniques here similar to Draw A Secret [5] users is requested to make a drawing as password. However there is no 2D visible grid in Passdoodles[6] and users is required to make a drawing with at the very least two pen strokes. Also in this technique users have choice of multiple colors. With the added features like free hand drawing and multiple color password matching in Passdoodles[6] become more difficult than the DAS.

PassShapes[7] by Weiss et. al., is a technique similar to Passdoodles[6] however it requires that eight arbitrary pen strokes are used to construct any geometric shape. At the time of authentication use can draw the same shape in any size and at any place on the login screen. Since this technique uses only 8 strokes it limits its password space as compared to other previous techniques.

Syukri Algorithm[8] this is also a recall based technique here the author proposed that instead of using random figure passwords or random geometric figures as password. Users should be required to enter their signatures as password at the time of registration. And at the time of verification users are required to reproduce their signature may be enlarged, rotated or scaled up. This techniques extract and verify signature using techniques like geometric averages etc. This technique have few advantages over the previous techniques like signature isgenerally unique to a particular user and also that faking a signature is a difficult task and also users generally keep their signatures secret and take measures that other are not able to fake their signatures easily.

3.3. Cued Recall Based Techniques

Blonder's Scheme[9] this was one of the initial graphical authentication system. In this technique user has to click on pre-selected regions on the selected image in a specific sequence which is then used as a password. It have many advantages over text based passwords like remembering images is easier as compared to random alpha numeric text. But this techniques also had some major disadvantages like that if the number of points per image becomes too much than it becomes a boring and repetitive task for user and also can make it prone to shoulder surfing attacks.

PassPoints[10]Wiedenbeck et al. this technique proposed the changes which were aimed to remove the drawbacks of the Blonder's Scheme [9] it could utilize any images unlike fixed boundaries and image as those were in Blonder's Scheme[9]. User will than have to select multiple points on the provided images to create a password at the time of registration. Since the click points were provided by users and there are potentially of thousands of click points on an image hence password space for this techniques becomes very large. But this scheme has some limitation as since it is not possible to replicate an exact point click on an image hence it introduce a tolerance level which enable clicks to be in a particular range near to original click point. If the tolerance level range is too high then security of this scheme become weak or if the tolerance level is too low this can cause issues with wrong password selection and will require more effort from user end.

Cued Click Points(CCP)[11]Chaisson et al proposed a variation of PassPoints[10]. In this technique images were presented to the users by considering the previous click point selected by the user. Next image which is display after click point selection is based on the selected click point and hence if user select a wrong click point the further images will be wrong. This made CCP more immune to guessing and midway replay attacks and a wrong guess of even a single missed click point will then lead to only wrong image. However for the legitimate users are generally found to select the correct click point within the known regions.

Persuasive Cued Click Points (PCCP) Chaisson et al.[12], proposed to add a persuasive feature to the Cued Click Point technique. In this techniques during registration a small viewport remains unshaded and user than have to select a point within the unshaded viewport. Since selection of view port is random user can choose to shuffle the viewport until he/she finds a suitable viewport. This technique also eliminates hotspot problem but shoulder surfing attacks were still possible in this technique. While authenticating users is only presented with unshaded image and he has to recall the click point and click it within the unshaded region within the viewport shown at the time of registration.

3.4. Hybrid Techniques

CAPTCHA based hybrid technique byGao et al.[13], this hybrid technique took the advantage of graphical passwords and CAPTCHA both. In this technique user while registering has to provide the images as their passwords. While authentication users have to select the correct image from the incorrect imagesand also provide a valid CAPTCHA below the password selection field this ensures that the images are being entered by the human and not any brute forcing bot. This also ensure that the data/image selection is not being replayed. This technique can be affected by malicious program like spyware etc.

Textual Graphical Password by Zhao and Li[14] is a hybrid technique which utilizes both textual passwords and graphical passwords. It was designed to be immune to attacks like shoulder surfing, spyware or other malicious programs. While registration user will select a text string as original password with varying length based on the environment on which the technique is being applied. While authenticating user will be present with an image with the original password in it and user will have to select the original password by click on the password text the click must be made within the invisible triangles (pass triangles) to be counted while entering the password.

3.5. Multilevel Techniques

3D Security Cloud Computing using Graphical Password[15] Ms. SnehaVasantet. al., this is a "Multilevel Authentication Technique" which provide different authentication techniques for different files based on their security level. In this technique they have utilized three separate technique for these security level type.

1. **Ring 1(Highest Security level):** In this level they utilized a new technique called "3D Password" where user is presented with a 3D environment and he/she has to navigate to a particular location following a particular sequence this constructs their 3D password.
2. **Ring 2(Medium Level Security):** This level utilizes "Graphical Password with Icons"(GPI)[4] and this is used to eliminate the hotspot problem which is a general problem in graphical authentication techniques.
3. **Ring 3(Lowest Level Security):** This level utilizes "Persuasive Click Point"(PCCP)[12] as mentioned earlier here user is required to perform a click point sequence with help from the system by providing the click point viewport.

3.6. Multidimensional Techniques

Multi-Dimension Password Generation Technique for Accessing Cloud Server[16] by Dinesha H A et al, proposed a multi dimension authentication technique which generate password by account for various parameters like vendor, consumer details, privileges etc. These parameters are considered as dimensions of this technique. In technique we have two entities:

1. **Service provider:** It provide different kinds of services.
2. **Client:** It is referred to as the organization or individual which utilize specific services by cloud service provider.

This technique account for all factors like services used, privileges and form a multidimensional password. With so many factor in play it greatly reduce the possibility of a brute force attack. In this technique user of an organization provide multiple images and service provider generate a password using all the details like images provide, client details, services require and then generate a password which is provided to the user at the time of registration and while login client has to provide the same password to enable the service.

A Novel Graphical Password Approach for Accessing Cloud & Data Verification[16] by RupalRawatet. al.proposed a new graphical authentication technique based which utilizes combination of graphical data, captcha data and also perform integrity check to make sure that no unauthorized modification has been made to the users data. In this technique:

1. At the time of registration client chooses a username and the numeric value is calculated from the chosen user name and which is then used to generate a Captcha.
2. In order to login user will have to remember the first digit of generate number form the user name and also the provided image.

Once user perform a successful login using image and the textual password system will perform an integrity check to ensure that the data is not modified.

Table 1
Comparison of Various Graphical Authentication Technique for Cloud Application

Authentication Techniques	*Category*	*Dictionary Attacks*	*Guessing*	*Shoulder Surfing*	*Spy-ware*	*Social Engg.*	*Cloud Specific*	*Cloud Application Suitability*	*Additional Hardware / Interface Requirement*
Déjà Vu	Recognition Based	Yes	No	No	Yes	Difficult	No	Few Cases	No
Pass Faces	Recognition Based	No	No	No	Yes	Difficult	No	Few Cases	No
Story	Recognition Based	Yes	No	No	Yes	Possible	No	Few Cases	No
GPI	Recognition	No	Yes	Yes	No	Difficult	No	Majority	No
DAS	Recall Based	Yes	Yes	Yes	No	Possible	No	Majority	Can utilize Special H/W
Pass Doodles	Recall Based	Yes	Yes	Yes	No	Easily	No	Majority	Can utilize Special H/W
Pass Shapes	Recall Based	No	Yes	Yes	No	Possible	No	Majority	Can utilize special H/W
Syukri	Recall Based	Yes	Yes	Yes	No	Possible	No	Majority	Can utilize special H/W
Blonder's Scheme	Cue Recall Based	No	Yes	Yes	Yes	Possible	No	Majority	No
Pass Points	Cued Recall	Yes	No	Yes	Yes	Difficult	No	Majority	No
Cued Click Point	Cued Recall Based	Yes	Yes	Yes	Yes	Difficult	No	Majority	No
PCCP	Cued Recall Based	No	Yes	Yes	No	Difficult	No	Majority	No
CAPTCHA Based	Hybrid	No	No	Yes	No	Difficult	No	Majority	No
S3PAS	Hybrid	Yes	Yes	No	No	Possible	No	Majority	No
3D Security	Multilevel	No	No	Yes	No	Difficult	Yes	Majority	No

Table 1 provide us with a comparison between various graphical authentication techniques and their usage within cloud applications. In table "Yes" is referred to the cases where the listed security attack is possible, "No" means algorithm has taken sufficient steps to ensure good level of resistance to listed attack. "Social Engineering" attacks are classified on the bases of difficult "Easy" is relatively easy to perform social engineering attacks, "Possible" refers to medium level difficulty, "difficult" is used for the techniques which are very hard to social engineer in order to be successful. "Cloud Specific" it defines whether the algorithm is developed specifically for cloud applications or not. "Cloud Application Suitability" it is a measure to define whether the technique is applicable to vast number of cloud application or is applicable only to a specific set of cloud application.

4. CONCLUSION

In this comparative study of graphical authentication techniques for cloud application we have identified various type of graphical authentication techniques, their differences, their drawbacks and strong points. During this study we have studied various techniques to mitigate certain type of attacks which are possible in graphical authentication techniques in cloud application. After studying characteristics of major graphical authentication techniques we have create a summarized comparison of these techniques and their applicability in cloud computing application.

REFERENCES

[1] Dhamija R. and Perrig A., "Déjà vu: A User Study Using Images for Authentication", in Proceedings of 9th USENIX Security Symposium, 2000.

[2] SachaBrostoff, M. Angela Sasse, "Are Passfaces More Usable Than Passwords? , A Field Trial Investigation, 2000.

[3] Weinshall D., "Cognitive Authentication Schemes Safe against Spyware".In IEEE Symposium on Security and Privacy (S&P), 2006.

[4] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz, "Towards usable solutions to graphical password hotspot problem", In 33rd Annual IEEE International Computer Software and Applications Conference, 2009.

[5] Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords". In 8th USENIX Security Symposium, August 1999.

[6] Varenhorst, Passdoodles: "A lightweight authentication method". MIT Research Science Institute, July 2004.

[7] R. Weiss and A. De Luca, "PassShapes - utilizing stroke based authentication to increase password memorability".

[8] Ali Mohamed Eilejtlawi, "Study and development of a new graphical password system", May 2008.

[9] G. Blonder. "Graphical passwords".United States Patent, 5,559,961, 1996.

[10] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. "PassPoints: Design and longitudinal evaluation of a graphical password system". International Journal of Human-Computer Studies, 63 (1-2): 102-127, 2005.

[11] S. Chiasson, P.C. van Oorschot, and R. Biddle."Graphical password authentication using Cued Click Points". In European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359-374.

[12] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot."Influencing users towards better passwords: Persuasive Cued Click-Points". In Human Computer Interaction (HCI), The British Computer Society, September 2008.

[13] H.C.Gao, X.Y.Liu, S.D.Wang, R.Y.Dai. "A new graphical password scheme against spyware by using CAPTCHA". In: Proceedings of the symposium on usable privacy and security, 15-17 July, 2009.

[14] H. Zhao and X. Li, “S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme”, in 21st International Conference on Advanced Information Networking and Applications Workshops, vol.2. Canada, 2007, pp. 467-472.

[15] Ms. SnehaVasantThakare and Ms. Deipali V. Gore, 3D Security Cloud Computing using Graphical Password, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 1, January 2013, ISSN (Online) : 2278-1.

[16] Dinesha H A and Dr.V.KAgrawal, “MULTI-DIMENSIONAL PASSWORD GENERATION TECHNIQUE FOR ACCESSING CLOUD SERVICES”, International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.3, June 2012.