Dyanamic Pattern Generation using Picture Dataset for Secure Authentication

Madhana Kumari
Pune University
ZCOER Pune, India

Meghana Nene
Pune University
ZCOER Pune, India

Pratiksha Nikam
Pune University
ZCOER Pune, India

Ashwini Gurne
Pune University
ZCOER Pune, India

ABSTRACT

Graphical password is in the foremost level than textual password. It overcomes the vulnerabilities of cracking password through various types of attacks. Graphical password is more secure than password in the form of text. It provides more memorable password than alphanumeric password which can reduce the burden on brain of user. It protects cloud data from shoulder surfing attack. Psychological study says that human can easily remember images than text, Hence graphical passwords are easy to remember and difficult to guess whereas textual passwords are difficult to remember and easy to guess. In Graphical password authentication technique images are used for authentication instead of texts. It combines recognition and recall based approach**.**

General Terms

Pattern Recognition, Security, Recognition based technique, Recall Based technique, Cued Click points

Keywords

Authorization, Graphical Password, Security, Shoulder surfing, cloud access, GUA

1. INTRODUCTION

Graphical passwords results into best security than the passwords in the form of text because many people try to memorize text based passwords using plain words or dictionary search. A dictionary search can also yield to get a password and a hacker can gain entry into a system in fraction of seconds. If more secure authentication is provided then we Can prevent the cloud data being hacked. The actions that human make may lead to attacks.

In this paper, we present a two-step authentication technique to provide more security to cloud data. It protects users against shoulder surfing attacks. Due to two-step authentication the user can log in the system if he provided correct password in both the phases and due to its dynamic nature it is much resistant to shoulder surfing attack and is secure among other graphical authentication schemes.

Graphical password which has been proposed by many research as an alternative to textual password. It is very safe and secure for a private or public account. Text based password need to be remembered which is very difficult for users in day to day life. Now a days for security every system requires authentication. For remembering passwords of each account is a difficult task in this changing world filled with technologies. Previously recall and reorganization technique was used for secure authentication. In this paper we have concentrated on combination of recall and recognization based technique by providing two step authentication which covers the first phase with recognition based technique and second phase with recall based technique, also we have given more priority to security of account. The paper discusses related work in the field of password authentication followed by existing system followed by improvement in existing system by proposed system. The development in the proposed system concluded the paper. Further related work is discussed in section 2, proposed system is discussed in section 3, and paper is finally concluded with the future scope in section 4

2. RELATED WORK

From the past many researchers had worked on graphical password authentication techniques. Among various graphical password authentication schemes this paper mainly focuses on providing security to cloud data and removes shoulder surfing attacks completely. Originally it was introduced by Blonder in 1996. This section is an overview of researches being done and researches going to be done. Graphical password is best alternative to text based password as it is easy to remember and hard to guess and provides much security against all types of attacks. The following related literatures are critically revised so as to provide contextual information which help in the proposed work.

Blonder et al. proposed a technique called “Blonder Scheme” where users were provided with a grid of images and the tap regions. For authentication, proper sequence of tap regions is required.

Jensen et al. proposed Recognition based technique in which user is presented with a set of random images during registration. The user has to select the particular number of images from this to set as a password. During authentication, user has to recognize those preselected images in a correct sequence. This technique is proposed for mobiles, PDAs. At First level user is required to select a theme. Images based on theme are shown to user in grid and also each image is displayed .To form a password user has to select the images in a sequence. The user needs to recognize the previously selected images and touch it using stylus in a correct sequence for authentication.

Uma D. Yadav, Prakash S. Mohod et al. proposed cued recall based technique that the user uses for password selection. The system uses cued click point to make authentication system more secure. In these techniques, for authentication, a hint is provided to user to recall a password, registered during registration phase. These techniques provide hints to user to memorize the password In this technique user is shown a highlighted image in which he has to click on any point on image to set a password the cued click points are stored as a password. In blonder technique the predetermined images and predetermined tap regions are provided to users. The user has to tap on regions in the same sequence provided during registration.

Our system is resistant to almost all types of attacks and provides more security to cloud data. In this graphical password we are combining recognition and recall-based techniques by providing two step authentications. The main reason behind this is because graphical images are more secure than the password in the form of text and also provide reliable authentication. It is easy to remember as well hard to guess. We are proposing a new concept in which cloud is secured by means of graphical image password. We are proposing a user defined algorithm & shoulder surfing attack removing technique. The algorithm is based on username & set of images.

This techniques is partioned into two groups as follows-

1. Recognition Based Technique

2. Recall Based Technique

2.1 Recognition based technique

In this technique user is presented with a set of images. At the time of authentication user selects the images provided by the server and chooses those images that was selected at the time of registration. Following are some examples which give idea about proposed method.

2.1.1 Image Pass technique -In this, during registration a grid of images is presented. The user has to select images as a password. During login user is presented with a grid which is a combination of real and decoy images. From the grid user has to select the real images in a correct sequence for authentication. The image positions will vary at every login. It is not strongly resistant to shoulder surfing as grid is only of size 4 x 3 and also the password images are fixed. So those can be easily seen and remembered by attacker.

2.1.2 Color Login techniques -In this, background color is used to decrease the login time. Multiple colors are used to confuse the imposters, but easy to use for authorized users. It is resistant to shoulder surfing attack but the password space here, is less than text-based password.

2.2 Recall based technique

In this technique user is presented with a set of questions so as to recall the password which he had put at the time of registration. Following are some examples which give idea about proposed method.

2.2.1 Draw-a-Secret (DAS) technique: In this technique, user draws a picture on grid

Each cell is denoted by discrete rectangular coordinates (x, y). The values of touch grids are stored in the order of Drawing. For authentication, user has to redraw the same picture provided at registration

2.2.2 Signature technique: The user is authenticated by drawing signature using mouse. There is no need to remember the signature but hard to draw via mouse. It is difficult to redraw the same signature in the same block. It is much more expensive

Our proposed system is easy and resistant to all attacks specifically shoulder surfing because we are providing two step authentication.

3. EXISTING SYSTEM

The existing system is a graphical password authentication system. It is a combination of Recognition based and Recall based approach. The user authentication is verified in two steps.

3.1 Registration Phase*:*

1. A user creates his profile by entering personal details and username.

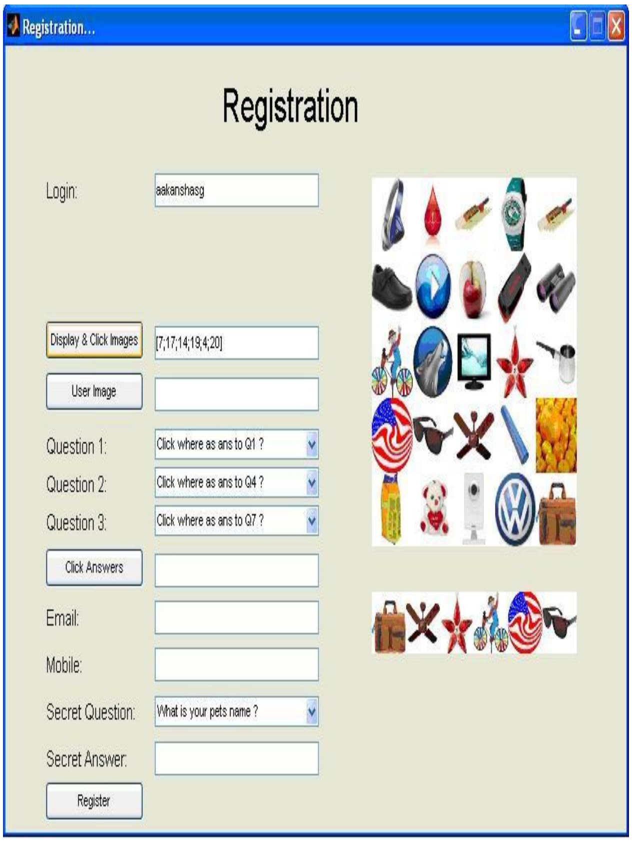
2. Then the set of images are presented to the user. These images are common to all the users. The user has to select some number of images to set as a password. The user can repeat any image. This is a password for the user's step-I authentication.

3. After this user will choose any image from the stored image database.

4. Now he is presented with question set and this image. The user has to select any three questions from this set.

5. To answer a question user has to click on the image. So for three questions there will be three different images. So there are three different images for three different questions.

6. User will be authenticated if he provides correct answer of image which he provided at registration



Registration...

Registration

Login: aakanshasg

[7;17;14;19;4;20]

Question 1: Click where as ans to Q1 ?

Question 2: Click where as ans to Q4 ?

Question 3: Click where as ans to Q7 ?

Email:

Mobile:

Secret Question: What is your pets name ?

Secret Answer:

Figure 3.1 Registeration phase[2]

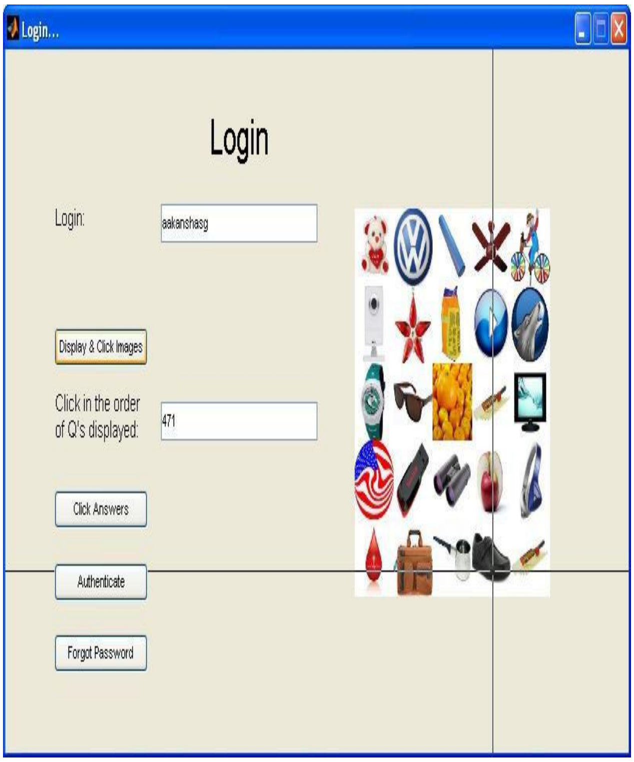
3.2 Login Phase:

1. For step-I authentication user is asked for user name and graphical password. The user has to enter a correct username and for graphical password there should be a correct selection of images in a sequential manner.

2. For step-II authentication, the preselected image and the preselected three questions are shown to the user.

3. Here the order of questions will be random. The user has to click on the correct images according to the order of questions.

4. After the successful selection in both the steps the user is an authorized user to access the particular system.



Login...

Login

Login: aakanshasg

Click in the order of Q's displayed: 471

Figure 3.2 Login Phase [2]

Center all address text. For two addresses, use two centered tabs, and so on. For three authors, you may have to improvise.

4. PROPOSED SYSTEM

4.1 Registration Phase

1. User enters the username.
2. User has to select some number of images to set as a password.
3. The user is presented with this picture and question set.
4. User has to select any three questions from the set.
5. As an answer of questions user has to click on any point on the image.
6. Click points and its respected questions are stored in database
7. Registration successful if user selects correct click points.

4.2 Login phase (Two step authentication)

1. System is asked for the username
2. heck if username already present in database
3. Number of images are provided to the user
4. Select those image which are selected at registration
5. After every login image position will get changed.
6. For more security we had proposed two step authentication.
7. Hence at next step user is provided with a page where he has to select image either by search engine or server which he had provided at registration.
8. Then those image will be enlarged and set of question will be provided
9. For each question a click point is been set as answer.
10. At every login user has to remember for which question which click point had been selected and also questions will be shuffled.

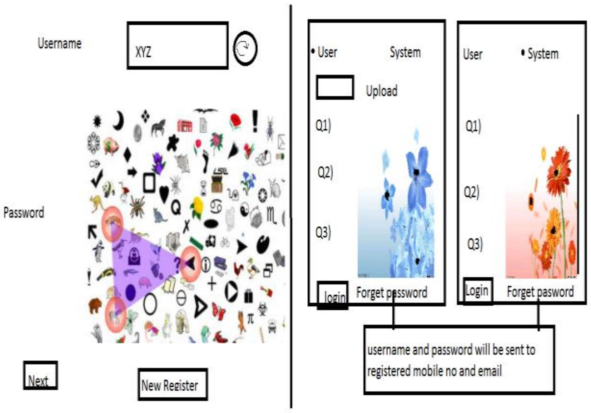


Figure 4 Existing System [2]

5. CONCLUSION AND FUTURE SCOPE

Our system combines recall and recognition techniques by providing two step authentications. Hence it is more prone to resist shoulder surfing attack. Due to two step authentication, it provides strong security against shoulder surfing attacks. Hence it is easy to access.

Images and questions will be dynamic for every login in second stage authentication .user has to select correct click point according to question which he had provided at registration

For cloud security:-

-To authenticate in sequence to connect with the services of

Cloud account.

-The user is connected securely again user should be get

Assure about the security of data which kept into the cloud.-

-Image can be taken from desktop as well as search engine

Or choose from the provided image. Images that we are

Uploading can be of any size.

If the user forgets any password that password is mailed to user's registered mail id and such a message is sent to user's registered mobile number also. So user can get the system updates although he is offline

-Image taken from desktop as well as search engine or chosen from the provided image can pose any pixel value.

-Images that we are providing are dynamic in nature to provide more security in authentication.

6. REFERENCES

[1] Shraddha M. Gurav, Prathmey k.Rane, Nilesh R. Khochare, Leena S. Gawade, "Graphical password authentication for cloud

Securing scheme" in 2014 IEEE International Conference on Electronic Systems, Signal Processing and Computing Technologies

[2] Mrs.Aakansha, "The Shoulder Surfing Resistant Graphical Password Authentication Technique" in 2016 ScienceDirect

[3] Julian Fierrez, "Graphical Password-Based User Authentication with Free-Form Doodles" in 2016 IEEE transactions on human-machine Systems, VOL. 46, NO. 4, AUGUST 2016

[4] Karmajit Petra, "Cued-Click Point Graphical Password Using Circular Tolerance to Increase Password Space and Persuasive Features" in 2016 Science direct

[5] Pawar Poonam, "Graphical Password Authentication with Cloud Securing Method" in 2015 International Journal of Multidisciplinary Research and Development 2015; 2(3): 763-76