Secure Authentication Model using Grid based Graphical Images with Three Way Validation

Mr. Sachin R. Jadhav
Department of Information Technology,
Pimpri Chinchwad College of Engineering, Nigdi,Pune,India.
srjadhav02@gmail.com

Miss. Neha Shelot
Department of Information Technology ,
Pimpri Chinchwad College of Engineering, Nigdi,Pune,India.
shelot391@gmail.com

Miss. Priyanka Shankar
Department of Information Technology ,
Pimpri Chinchwad College of Engineering, Nigdi,Pune,India.
priyankashankar.786@gmail.com

Abstract— The most common computer authentication method is to use text usernames and passwords which have various drawbacks. For example users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. This paper provides additional layer of security to normal textual password by using graphical password for authenticating the user. As graphical passwords are vulnerable to shoulder surfing attack so we will send one-time generated password to users and even send credentials to users authorized email-id. Using the instant messaging service available in internet, user will obtain the One Time Password (OTP).

Keywords*-Graphical password, captcha,brute force attack, authentication, security*

*****

I. INTRODUCTION

Authentication is the process of determining that theperson requesting a resource is the one who is owner of that account. Most of the authentication system these days use a combination of username and password for authentication. Due to the less power of remembering, most users tend to choose short and simple passwords which are easy to remember. Like alphanumeric, text-based passwords, graphical passwords are knowledge-based authentication mechanisms.

Graphical passwords make use pictures instead of textual password and are partially accepted the fact that humans can remember pictures more easily than a string of characters. A graphical password is an authentication system that works by having the user to select password from images, in a specific order, presented in a graphical user interface. Graphical passwords provide better security than text-based passwords because many people, in an order to remember text-based passwords, use plain words.

The idea of graphical passwords was given by Greg Blonder in 1996. An OTP is a set of characters that can be used to identify the user . Once the password is used, it is no longer used for any further authentication. Even if the attacker gets the password, it is most likely that it was already used once, as it was being transmitted, thus useless to the attacker..

II. LITERATURE REVIEW

- ***Re-Captcha***

It is a type of challenge-response test used in computing to ensure that the response is not generated by a computer. Re-Captcha [1] is a popular Captcha system which uses successful decoding. This validation is typically used in contact forms and registration forms to fight against spam bots. To use it, you'll only need to include the Re- Captcha API, and get an API key on the website.

Re-Captcha technology works together with the Re- Captcha library available on web server, so no need to use it in a network which is not connected to the internet. You need to get API keys. Websites that use forms will need to be secured from spamming by "Spam-Bots". Spam-Bots will visit your site and fill out forms that are not secured. This can result in

comment spamming in forums, spam emails being sent from your server, and other spam related activities. The "Re-Captcha" allow us to add an image with a special code to web forms. This requires the person who is filling form must type

correct password while submitting it.Graphical based passwords schemes can be broadly classified.

2.1 Recognition Based System

Recognition based system is called as cognometric system. Recognition based techniques involve identifying whether the user has recognized correct images. Techniques are used they are as follows:-

Dhamija and Perrig [2] proposed a graphical authentication scheme based on the Hash Visualization technique. In this system, the user is asked to select a certain number of images from a set of random pictures generated by a program.Later, the user will be required to identify the preselected images in order to be authenticated.

Fig 1. Dhamija and Perrig

Algorithm is as follows:-

1. Using this algorithm, the user creates an image portfolio, by selecting a subset of images out of a set of sample images.
2. To authenticate the user, the system presents a challenge image set, consisting of n images.
3. This challenge set contains m images out of the portfolio. So the remaining n-m images are decoy messages.
4. To authenticate user must select correct images which are as a part of portfolio.
5. To set up a image portfolio, the user selects a specific number of images from a larger set of images presented by a server.
6. After the portfolio selection phase, we use a short training phase to improve the memorability of the portfolio images.
7. During training, the user points out the pictures in the portfolio from a challenge set containing decoy images.
8. The selection and the training phase need to occur in a secure environment, such that no other person can see the image portfolio.

Advantage is that it's easy to remember.

Disadvantage is that the server needs to store the seed of the portfolio images of each user in plain text. Even the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

2.2 Pure-Recall Based System

In recall-based system users need to reproduce their passwords without being given any reminder, hints or gesture.

• Draw a Secret (DAS) [3] algorithm is a technique which works in following steps:-

1. A grid is provided of size G*G. Each cell the grid has some coordinates (x, y) assigned to it.
2. The pattern drawn by the user is stored in the form of sequence of coordinates.
3. In this technique, the user is required to draw the pattern in one stroke.
4. While authentication the user needs to draw same pattern without any hint. If the user successfully draws the pattern in the exact manner, he is authenticated.
5. It is widely used in mobile applications for drawing pattern lock system.
6. Consider the following example as shown in fig2.In which the sequence of coordinates stored are (2,2), (3,2), (3,3), (2,3), (2,2), (2,1).

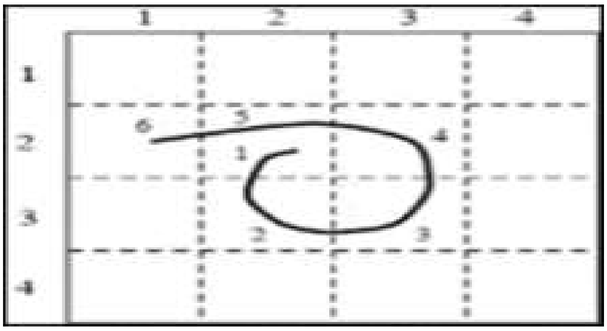


Fig 2. DAS

Advantage is that it is alphabet independent hence there is no language restriction. It is easy to implement.

Disadvantage is that user cannot remember the exact stroke order. If user is not familiar with the input devices then this technique is difficult to use. It provides less password space.

2.3 Clue-Recall Based System

Cued recall based systems which are also called Icon metric Systems. In cued recall-based system, a user is provided with a hint so that he or she can recall his/her password.

• The "PassPoint" system by Wiedenbeck, etal. [4]. In this user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence.

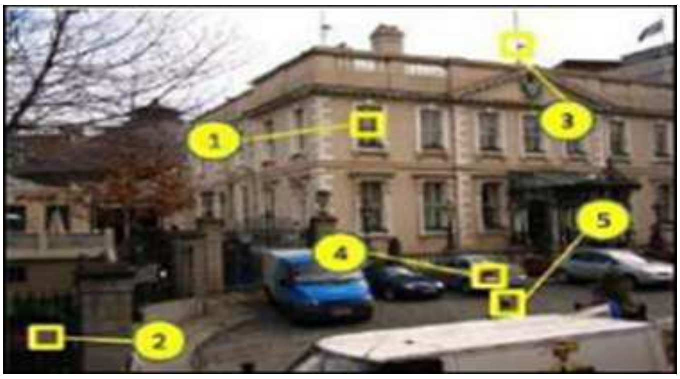


Fig 3. PassPoint

Algorithm is as follows:

1. To login, the user has to click again closely to the chosen points, in the chosen sequence. For humans sometimes it is impossible to click repeatedly on exactly the same point, the system allows for an error tolerance r in the click locations (e.g.; a disk with radius r=10 or 15 pixels).
2. This is done by quantizing (discretizing) the click locations, using three different square grids.
3. Each grid has width of the three grids is staggered with respect to the previous grid by a distance 2r vertically and a distance 2r horizontally.
4. If there were only one quantization grid then a selected click point could be close to a grid line and small variations in the user's clicking could lead to a click in a different grid square, thus leading to the wrong password.

Advantage of this algorithm is that it overcomesBlonder algorithm thus by selecting any natural image and having as many click points as possible which make the system more secure.

Disadvantage is that it is time consuming and difficult to memorize the click points, thus number of trials is required for authentication.

2.4 Hybrid System

Hybrid systems are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes.

Click-Draw Based Graphical Password Scheme[5].This scheme (CDGPS) combines the properties of PassPoint, DAS and Cued Click Points. Specifically, there are two operational steps in CDGPS:they are: image selection and secret drawing.

The image selection refers to the concept and technique from the choice-based schemes, users are required to select and remember the ordered sequence of images like a story and then further select some of them (e.g., one or two images) for the following step. The step of secret drawing, which refers to the concepts and techniques from both the click-based and the draw-based schemes, requires users to click-draw something like for e.g., a digital number or a letter on their selected images. In the second step, users should draw their own secrets by using series of clicks.

2.5 Comparison of existing system

Graphical Password Scheme/Technique	**Brute Force Attack**	**Dictionary Attack**	**Guessing Attack**	**Shoulder Surfing Attack**
Graphical Password as an OTP	Y	Y	Y	Y
Pass Point	Y	N	Y	Y
Blonder Scheme	Y	N	Y	Y
Picture Password Scheme	Y	N	Y	Y
Pass Face	Y	Y	Y	Y

Table 1. Comparison between algorithms based on attacks

2.6 Provided Security for various attacks

- **Brute Force Attack:-**

A hacker uses a computer program or script to try to sign in with possible password combinations, usually starting with the easiest-to- guess passwords. (So just think: if a hack has a company list, he or she can easily guess usernames. If even one of the users has a"Passwordabc", he will quickly be able to get in.)It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords.

- ***Dictionary Attack:-***

A hacker uses a program or script to try to login by cycling through combinations of common words. In contrast with a brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words for example a dictionary Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short , such as single words found in dictionaries or simple, easily predicted variations on words, such as appending a digit. Overall, graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

- **Guessing Attack:-**

Most networks are not configured to long and complex passwords, and an attacker needs to find only one weak password to gain access to a network. Not all authentication protocols are equally effective against guessing attacks. For example, LAN Manager authentication is case-insensitive, a password guessing attack against it does not need to consider whether letters in the password are uppercase or lowercase..Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text based passwords.

- **Spyware Attack:-**

Except for a few exceptions, key logging or key listening spyware cannot be used to break graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

- **Shoulder Surfing Attack:-**

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder surfing. None of the recall-based based techniques are considered shoulder-surfing resistant.

- **Social Engineering Attack:-**

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

III. Implementation of secure authentication model using grid based graphical images with three way validation

In this proposed system we use image as a password. In this we are implementing new security mechanism for Web application. We are providing three way authentication , first Username in encrypted format and second Captcha as Graphical password means user have to select four images from three by three grid, then that image Id are get stored in the database. After that while login user have to give the correct username and password, after giving correct username and password. User has to choose correct grid and select the correct images in sequence they have been first selected. If the images are matched with the database then an OTP is send, if OTP confirmed then the third email will be send to their registered email address containing their login credentials. The block diagram of proposed method is as follows:-

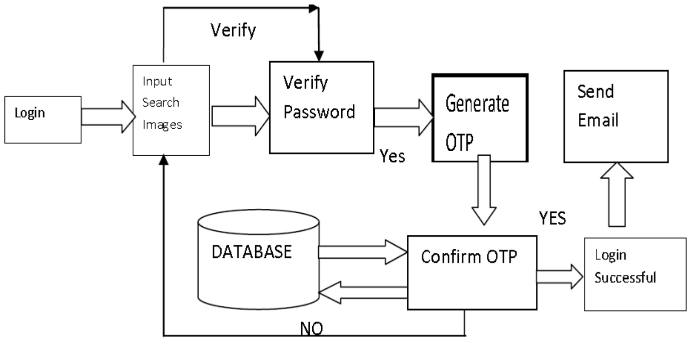


Fig 4. System Architecture of Secure Authentication model using grid based graphical images with three way validation

Components are explained as follows:-

1. **Login: -** It is the act of logging in to a database, mobile device, or computer, especially a multiuser computer or a remote or networked computer system. In this the user login into the account using user-id and password.
2. **Input search images:-**So in this we will show user some images in grid form and they have to select the images as a password from that grid.
3. **Verify Password:-**In this the user will do first login and select the images as they were selected at the registering time. Then the admin will verify the images and the pattern entered by the user are correct or not by checking in database.
4. **Generate and confirm OTP:-**In this component or module once the image is verified successfully then an OTP will be generated and send to user. The user entered OTP is correct then an email will be sending on the registered mail.
5. **Database: -** A database is a collection of information that is organized so that it can be easily accessed, managed and updated in this system the images selected as Captcha are stored in the database which is used will verification of the password. There will be centralized database where all users' login and personal information will be there.

IV. Result & Analysis

Login Page:-

In this user will login using email address and will choice correct sequence of images as password to login to account. If he forget password he can get the password on its mail address.

Fig 5: Login Page

Registration Page:-

In this user will create its account by filling name, email and sequence of images as graphical password.

Fig 6:Signup page

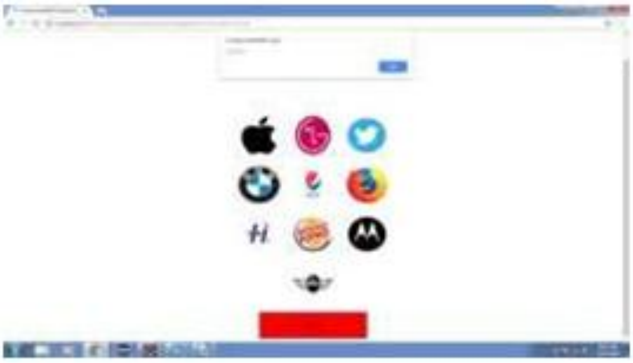


Fig 7: Logo images as a password

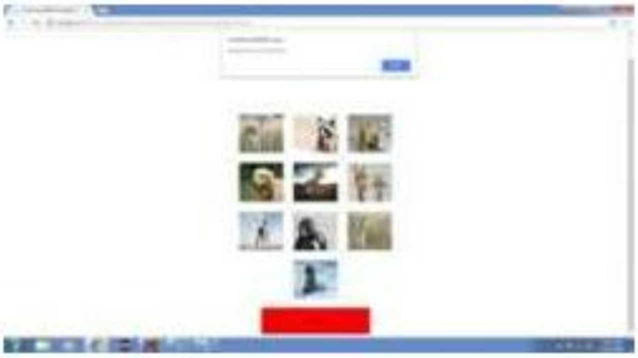


Fig 8: Animals images as a password

Attacks And OTP:-

Brute Force algorithm is as follows:-

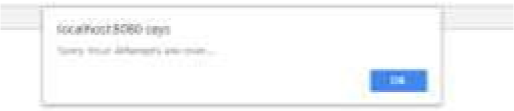
```
{

String tempPasswd = rbean.getPassword(); int
OrignalLength = tempPasswd.length();
System.out.println("Orignal Passwd
Length"+OrignalLength);

String OngoingPasswd=pbean.getPassword(); Int
OngoningLength=OngoingPasswd.length();
System.out.println("Ongoing Passwd
Length"+OngoingPasswd); if(OngoningLength >
OrignalLength)

System.out.println("Brute Force attack Detected");
System.out.println("<script>");
System.out.println("alert('Sorry Your Attempts are over....')");

System.out.println("window.location =
'login.html;'"); System.out.println("</script>");
```



localhost:8080 says

Sorry Your Attempts are over....

Fig 9:Brute Force Attack

SQL Implementation is as follows:-

```
String passwordType =
request.getParameter("passwordType"); try {

String email = request.getParameter("email");
System.out.println("Email is " + email); String[] operator
= {"=","~","^","|","!"};

String[] words = {" select"," or"," drop"," where"," if"};

int temp,sqlFlag = 0; boolean
sqlInectFlag; CharSequence check;
for(String str:operator)

{

temp = email.indexOf(str); if(temp != -1)
{

sqlFlag++;

System.out.println("SQL Injection Detected");
```

localhost:8080 says

SQL Injection Detected...

Fig 10:SQL Injection Attack

Fig 11: OTP recieve

Admin Page:-

In this admin can add images to the password and can add movies so that user may know which movies are been released

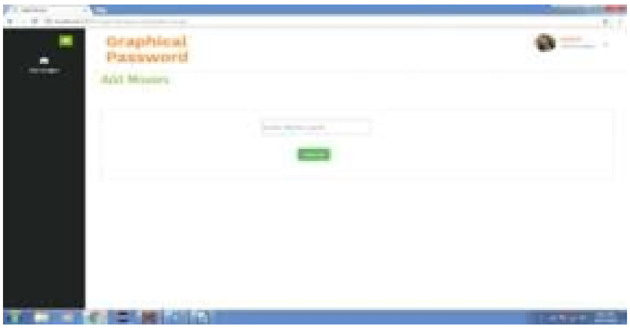


Fig 12: Add Movies Names

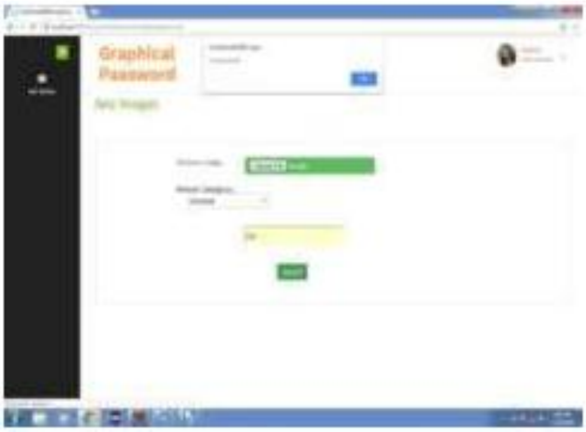


Fig13: Add Images

Database

In this there are two important database one is password through which we are going to check whether enter sequence of images as password is correct or not and second one is user info which contains overall info of user.

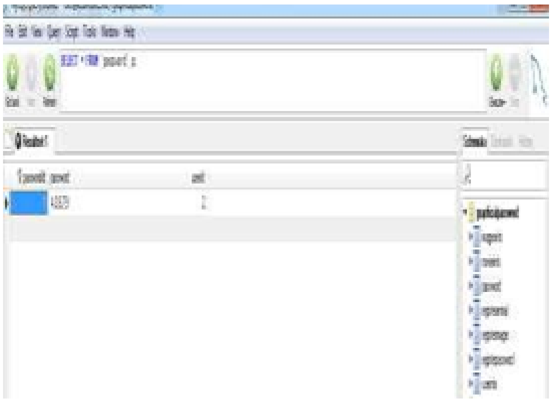
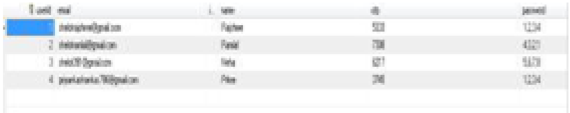


Fig 14: Password Database



userid	email	name	otp	password
1	[illegible]	[illegible]	503	1234
2	[illegible]	[illegible]	738	4321
3	[illegible]	Neha	627	5678
4	[illegible]	[illegible]	298	1234

Fig 15: User info database

Thus we have implemented three way security model for authentication.

V. Conclusion

We conclude that, our Grid based visual image authentication model provides more security to data and protection against different attacks. Our proposed system is based on graphical password. In this we apply various attacks and notify user if anyone tries to get their password by displaying message. For successful login user has to select correct sequence of image which is chosen by user during a registration. After successfully providing the sequence of images, system will generate OTP for validating user. This system provide OTP which provide more security to data and even after successful login it sends its login credentials to valid registered email-id. So this model provides 3 way authentication system to secure users data over internet.

References

[1] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin; 1999, “The design and analysis of graphical passwords”, Proceedings of the Eighth USENIX Security Symposium, USENIX Association 1–14.

[2] J. Thorpe and P. C. v. Oorschot, “Towards Secure Design Choices for Implementing Graphical Passwords,” in 20th Annual Computer Security Applications Conference (ACSAC) Tueson, USA. IEEE, 2004.

[3] Susan Wiedenbeck, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, NasirMemon; 2005a, “Design and longitudinal evaluation of a graphical password system”, Academic Press, Inc. 102-127

[4] Rachna Dhamija, Adrian Perrig; 2000, “Déjà Vu: A User Study. Using Images for Authentication”, in the proceeding of the 9th USENIX security Symposium.

[5] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah K. Mammi; 2008, “Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique”; IEEE Explore.

[6] Rachna Dhamija; 2000, “Hash visualization in user authentication”, Proceedings of CHI 2000 ACM, The Hague, the Netherlands.

[7] Improved Security Using Captcha as Graphical Password.

[8] Ibrahim FurkanInce, IlkerYengin, andYucelBatu Salman,―Designing Captcha Algorithm: Splitting And Rotating The Images Against OCRs‖ Third 2008 International Conference on Convergence and Hybrid Information Technology

[9] T. S. Ravi Kiran, and Y. Rama Krishna, Combining captcha and graphical passwords for user authentication‖ International Journal of Research in IT & Management, Volume 2, Issue 4 (April 2012).