International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 2, Issue 1, pp: (19-26), Month: April 2015 – September 2015, Available at: www.paperpublications.org

Folder Security Using Graphical Password Authentication Scheme

[1]Madhuri Akhand, [2]Ankita Bijwe, [3] Kajal Zade, [4]Karuna Borkar

Abstract: **Now a day most of the user are facing problem for providing the security to the folder, so that it will not be accesses by the unauthorized user. Taking in action all these problems I have designed a model which will provide a best security to your folders using graphical password authentication model. Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. We have developed one such system, called Pass Points, and evaluated it with human users. Beginning around 1999, a multitude of graphical based password scheme which have been proposed as alternative to text based password scheme, motivated by the promise of improved password memorability and thus usability. This paper presents a detailed evaluation of the Pass Points and pattern matching password scheme which provides high level of security and provides security to your folder.**

Keywords: **Authentication, Cued Click Points, Draw-A-Secret, Graphical password authentication, pass faces pass points, pass-objects.**

I. INTRODUCTION

Traditional authentication systems use text passwords which includes username and password. These passwords fail to provide the desired level of security. Text passwords, once chosen and learned, the user must able to recall it at the time of login, which makes them hard to remember. However if we keep changing our password frequently it is more vulnerable to be forgotten. To reduce brute force attacks the user should select long passwords which include characters as well as numbers. This makes them all the more difficult to remember. Text passwords include risks of shoulder surfing, hidden cameras and spyware attacks. Also they are prone to dictionary attacks and keyboard sniffers. Thus they are not much reliable and hence for greater security we can use graphical passwords. Numbers of graphical password systems have been developed. Studies shows that text based password suffer with both security and usability problems.graphical passwords are passwords that are based on images instead of alphanumeric strings. Graphical Passwords are brought into use for greater memorability and to reduce the tendency of choosing insecure passwords. Its is expected that using images as passwords should increase overall password security. Graphical password is the picture as a password. Human remember picture immediately and longtime rather than words, it is also difficult to break. The memorability of the image is because of its nature and specific sequence of click locations, undertake to retrieve the password. Image with meaningful content will supports the user’s memorability.

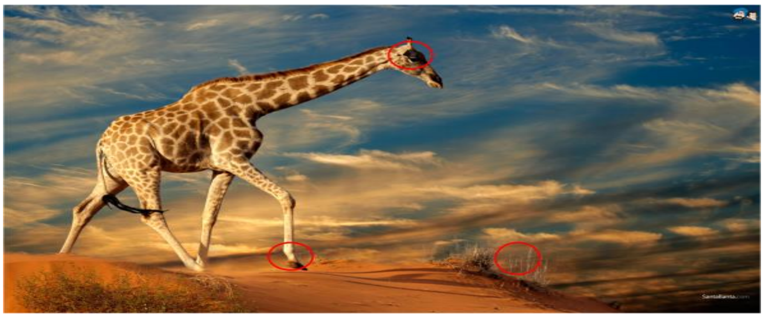


Fig 1. An Example for Graphical Password

II. LITERATURE SURVEY

In the survey people are in the favor to use image as a password to protect their account. It is always proved that human brain is better in recognition and recalling by graphical password. Graphical password should not write down orstored in plain text. According to psychological research human brain is very good recognizing the image. Graphical password was first described by blonder in 1996.

“Passface” is a technique developed by Real User Corporation [1,6]. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures. Comparative studies by Brostoff and Sasse showed that Passfaces had only a third of the login failure rate of text-based passwords, despite having about a third the frequency of use.

Fig: 2. An example of Passfaces

Sobrado and Birget [8] developed a graphical password technique that deals with the shouldersurfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two passobjects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating.

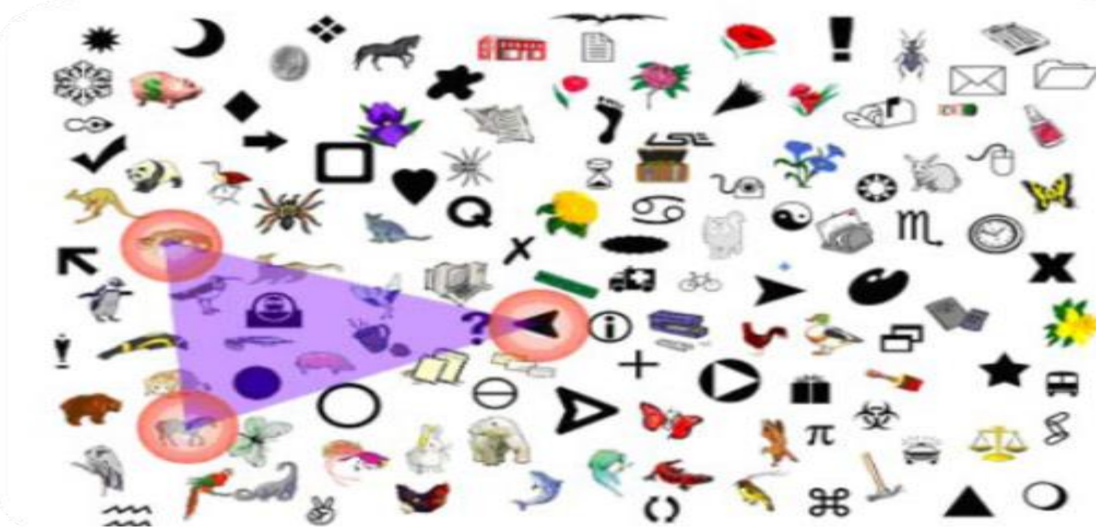


Fig: 3. An example of Pass-Objects

Dhamija and Perrig [7] proposed a graphical authentication scheme based on the Hash Visualization technique . In their 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. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

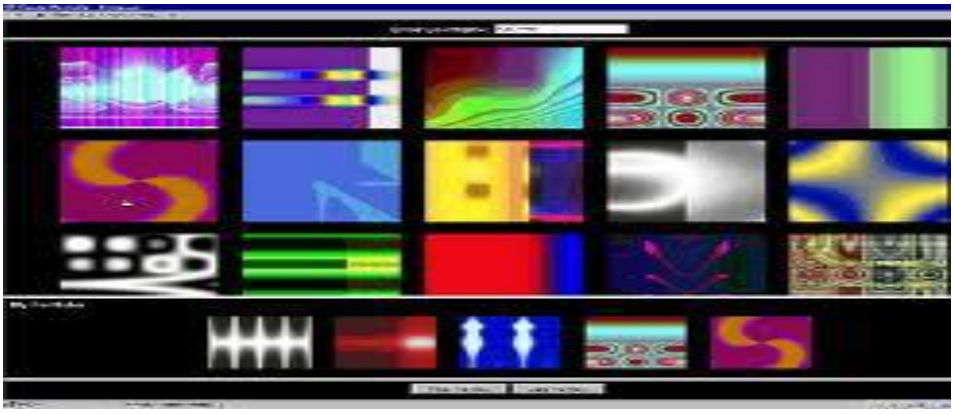


Fig 4: A Sample of single image pass click method

Akula and Devisetty's algorithm [9] is similar to the technique proposed by Dhamija and Perrig [7]. The difference is that by using hash function SHA-1, which produces a 20 byte output, the authentication is secure and require less memory. The authors suggested a possible future improvement by providing persistent storage and this could be deployed on the Internet, cell phones and PDA's.

Jansen et al. [10,11] proposed a graphical password mechanism for mobile devices. During the enrollment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password (figure 5). During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumbnail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size.

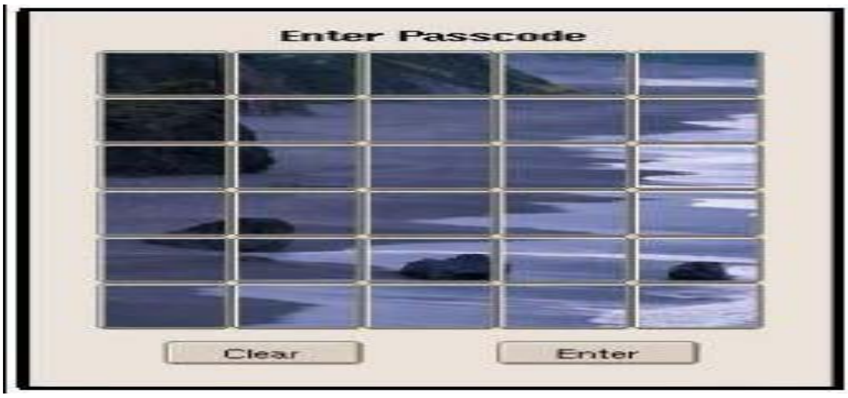


Fig: 5. A graphical password scheme proposed by Jansen

Takada and Koike discussed a similar graphical password technique for mobile devices. This technique allows users to use their favorite image for authentication [13]. The users first register their favorite images (pass-images) with the server. During authentication, a user has to go through several rounds of verification. At each round, the user either selects a pass-image among several decoy-images or chooses nothing if no pass-image is present. The program would authorize a user only if all verifications are successful. Allowing users to register their own images makes it easier for user to remember their pass-images. A notification mechanism is also implemented to notify users when new images are registered in order to prevent unauthorized image registration. This method does not necessarily make it a more secure authentication method than text-based passwords. As shown in the studies by Davis [12], users' choices of picture passwords are often predictable. Allowing users to use their own pictures would make the password even more predictable, especially if the attacker is familiar with the user.

III. METHODOLOGY USED

Generally, the graphical password techniques can be classified into two categories:-

A. Recognition-based graphical techniques

B. Recall-based graphical techniques

A. RECOGNITION BASED TECHNIQUES:

In recognition-based graphical password systems, users typically memorize a portfolio of images during password creation and then must recognize their images from among decoys to log in. Humans have exceptional ability to recognize images previously seen, even if those images were viewed very briefly. Several recognition-based graphical password schemes have been proposed in recent years.

1. Pass Faces
2. Pass-Object

B. RECALL BASED TECHNIQUES:

Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Graphical passwords requiring pure recall are most similar to text passwords because users must remember their password and reproduce it without any cues from the system. This is a difficult memory task and users sometimes devise ways of using the interface as a cue even though it is not intended as such. The typical recall-based authentication schemes is :

1. Draw-A-Secret (DAS)
2. Pass Clicks

IV. PROPOSED WORK

There are two previous techniques used in our project. That are Single image pass click, Multiple image single click point, Pattern Matching.

A. SINGLE IMAGE PASS CLICKS:

In this, user selects single image and choose number of click point on that image at the registration phase and the user has to provide the same at the login phase to get authenticate.

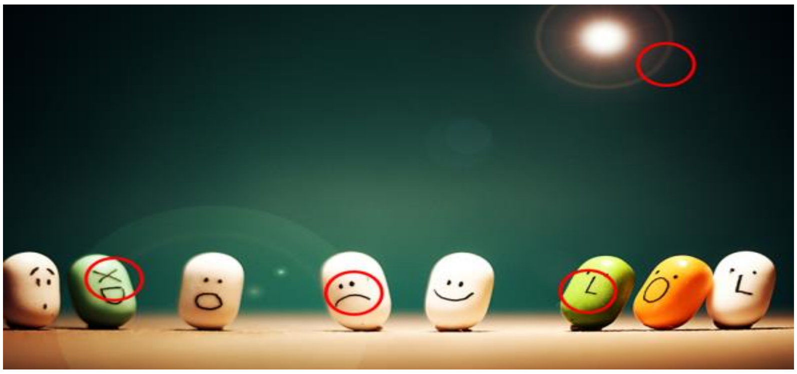


Fig 6: Single image pass clicks

B. MULTIPLE IMAGE PASS CLICKS:

In multiple image type, user will select multiple images and select one region on every region and follow every step same as in single image.In our proposed system, user can free to choose the image and select points on it and he can reset it and recover it in case of forgot the points on it. By giving the answer of security question correctly user can recover his password.

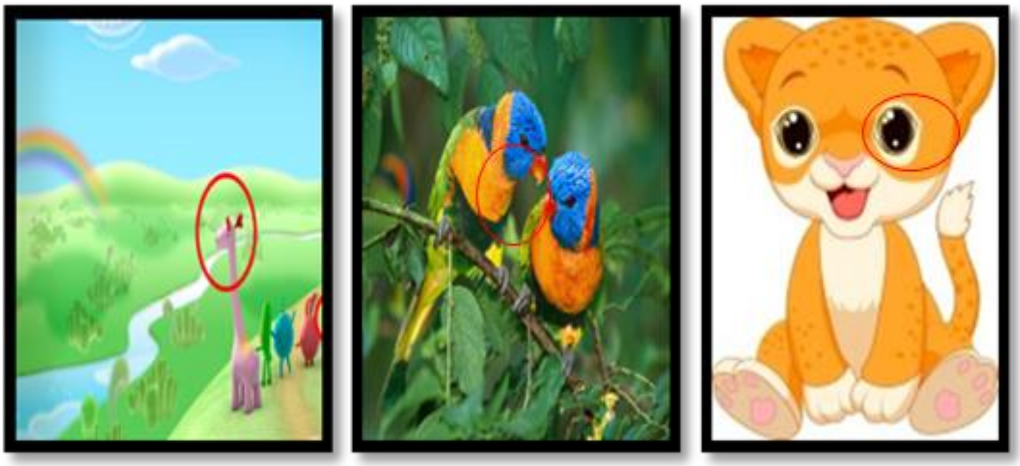


Fig 7: Multiple images pass clicks

C. PATTERN MATCHING:

With Pattern matching, users draw their password on a 2D grid using a stylus or mouse. The password is composed of the coordinates of the grid cells that the user passes through while drawing. A drawing can consist of one continuous pen stroke or several strokes. To log in, users repeat the same path through the grid cells. The theoretical password space is determined by the coarseness of the underlying 2D grid and the complexity of the images. A coarser grid helps with usability, while a finer grid increases the size of the password space.

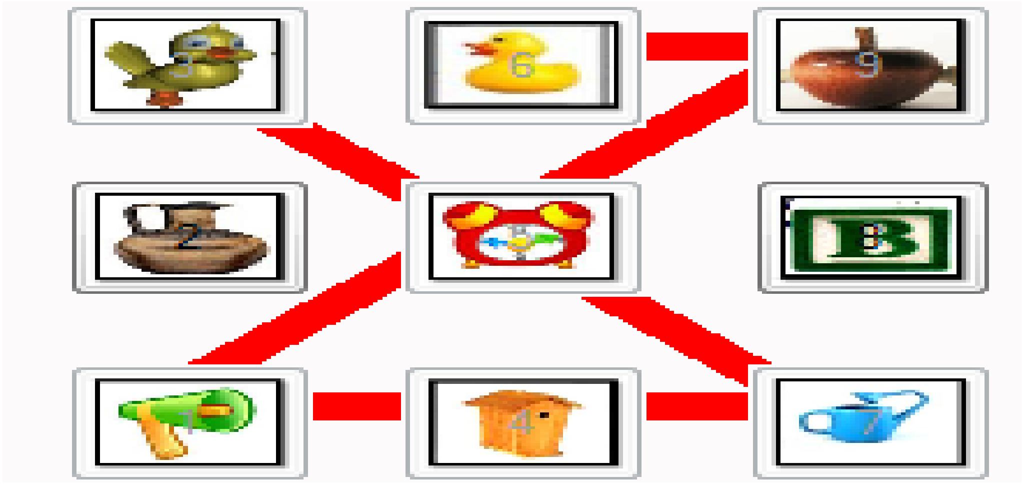


Fig 8: Pass-object graphical password system

V. SYSTEM ARCHITECTURE

In the proposed system, the user will be validated based on set of certain image along with the approximate pixel of the click made or pattern drawn by user. Now a day's most of the user are facing problem for providing the security to the folder, so that it will not be accesses by the unauthorized user. In our proposed system, we have proposed a model which will provide a best security to your folders using graphical password authentication scheme.

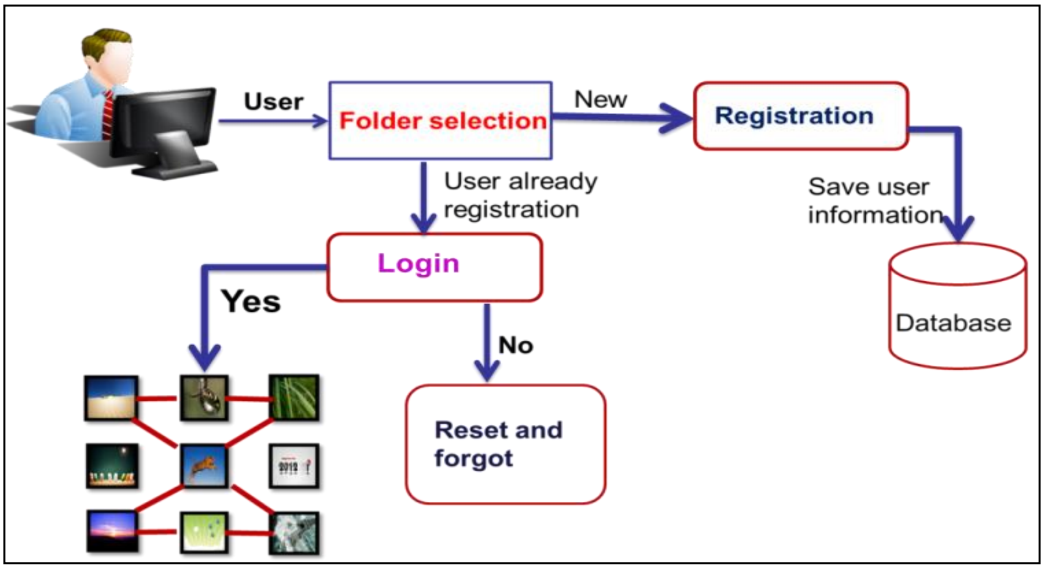


Fig 9: System Architecture

VI. MODULES

There are 5 modules in our project as follows:

1. FOLDER SELECTION MODULE:

In Folder selection module, first user browses the folder and selects the folder which user wants to lock. First user has to register them and if user is already register then user should be login to unlock that folder.

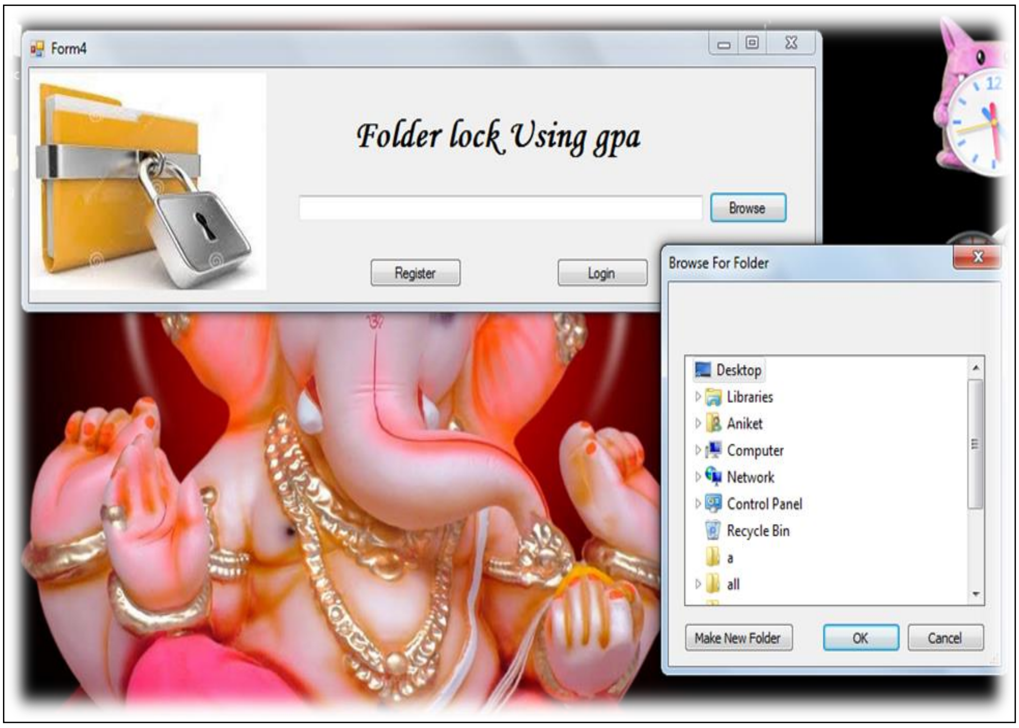
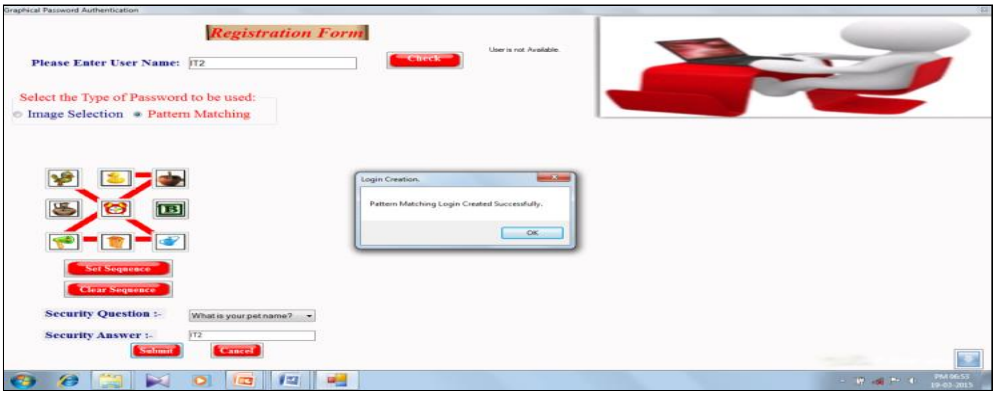


Fig 10: Folder Selection Module

2. REGISTRATION MODULE:

In Registration Process, first user provides necessary information & creates Graphical Password.



Graphical Password Authentication

Registration Form

Please Enter User Name: IT2

User is not Available.

Select the Type of Password to be used:
○ Image Selection ● Pattern Matching

Login Creation.

Pattern Matching Login Created Successfully.

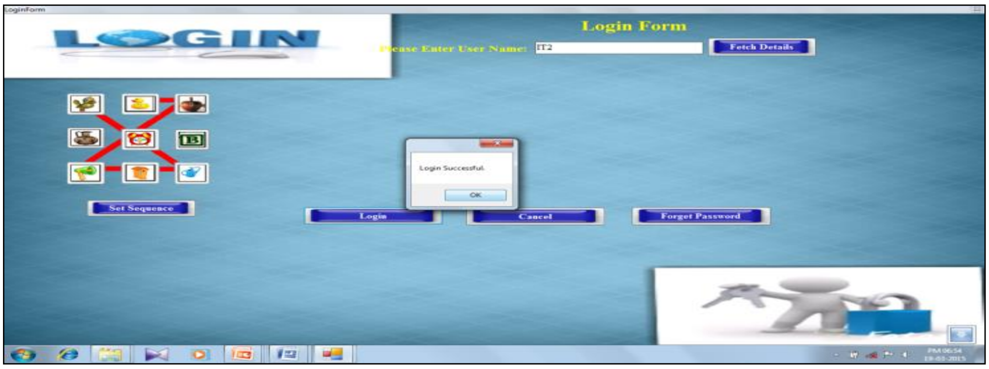
Security Question :- What is your pet name?

Security Answer :- IT2

Fig 11: Registration Module

3. LOGIN MODULE:

When user comes to Login phase, the first step is to enter the username and fetch details. Then user draws the pattern or click on images to get authenticated.



LoginForm

Login Form

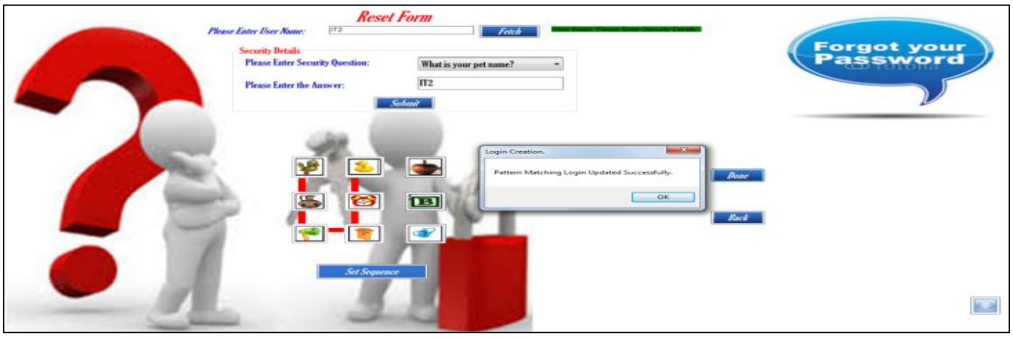
Please Enter User Name: IT2

Login Successful.

Fig 12: Login Module

4. RESET PASSWORD MODULE:

When user comes in forget reset phase first step is that user enter the username and security question if its username and security question are available in database user can recover its password.



Reset Form

Please Enter User Name: IT2

Security Details

Please Enter Security Question: What is your pet name?

Please Enter the Answer: IT2

Login Creation.

Pattern Matching Login Updated Successfully.

Fig 13: Login Module

5. SERVER MODULE:

In our proposed system, we have used SQL Server 2005 to store data. The data includes user information such as username, security question and answers and Password details(images).The password details includes pixel's coordinates of the click points of drawn pattern.

In SQL Server database, we have created 3 tables i.e cordInfo, LoginInfo, PathInfo. The cordInfo table stores the username along with coordinates of the selected pixels of the password.The LoginInfo table fetches and stores the data of cordInfo table temporarily and verify the user’s authentication by comparing the information in cordInfo with LoginInfo in order to get authenticate (if the data matches). The PathInfo table stores the Folder’s path selected during folder selection phase by the user.

VII. CONCLUSION

Taking in action all the security attack, viruses, malwares, the designed module will provide security to the folder preventing unauthorized access of your folder. It is clear from the above descriptive modules that, it will almost not possible to crack or guess the password by unauthorized users. The Pattern matching technique provides an environment in which the folder will be in safe condition. It will be one of the safe mechanisms for folder security. This result might allow other considerations to be taken into account when making modifications to the system, such as the size of the screen on a mobile device, which would favour the use of smaller images. Future work in this area might include a field study to investigate these modifications in a more ecologically valid situation and more investigation into how the cost to usability is similarly.

REFERENCES

[1] Xiaoyuan Suo et al, “Graphical Passwords: A Survey”, Department of Computer Science,Georgia State University, may 2013.

[2] Ms. Shilpa L. Dhapade,” Implementation of A Graphical Based Password For Folder Cryptography”,International journal of Engineering Research and Technology(IJERT) Volume. 2 Issue 7,July-2013.

[3] Abuthaheer, N.S.JeyaKarthikka, T.M.Thiyagu, “Cued Click Points Graphical Images and Text Password along with Pixel based OTP Authentication,” International Journal of Computer Applications (0975 – 8887) Volume 87 – No.2, February 2014.

[4] Ishwar Padade,” Graphical Password Authentication”, IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014 ISSN: 2348 – 6090.

[5] Ankesh Khandelwal1,”User Authentication by Secured Graphical Password Implementation “,International Journal of Computer Applications (0975 – 8887) Volume 1 – No 25.

[6] RealUser, "www.realuser.com," last accessed in June 2005.

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

[8] L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[9] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of MidwestInstruction and Computing Symposium, 2004.

[10] W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.

[11] W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.

[12] Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[13] T.Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User’s Favorite Images," in Human-Computer Interaction with Mobile Devices and Services, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 – 351.