IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 13, PP 46-52

System For 3 Level Security Verification Using Image Based Authentication & OTP

Dr. Mamta Meena[1], Harshit Singh Lamba[2], Deepit Taterwal[3], Moiz Shaikh[4]

1, 2, 3, 4(Computer Engineering Department, Atharva College Of Engineering, Mumbai University, India)

Abstract : *This paper disucsses about improving authentication and authorization techniques which can be easily implemented and are user friendly Every individual has their own personal life. In a world with internet, the process of communication and personal life management has drastically changed from what it was few decades back. But for any internet user, the advantage of instant communication comes at a cost. The network infrastructure has loopholes which gives way to hackers to access any registered users entire data. The hacker can further exploit an individual for personal benefits. These loopholes can we covered by introducing a multiple authentication and authorization techniques in the process. We have designed a unique 3 Level Authentication and Authorization system while keeping in mind the key fundamentals of security which are Confidentiality, Integrity & Availability. We want each and every user to feel secure and safe from hackers.*

Keywords : *Authentication, Authorization, Availability, Confidentiality, Integrity, Security.*

I. Introduction

1.1 Overview

Traditionally, textual based passwords have always helped users to maintain & prove identity [1]. These passwords are generally alphanumeric passwords i.e. it is a combination of alphabets, digits and special symbols. But it has various flaws. To, remember easily, users tend to keep the passwords short and simple like personal names, pet names, phone no.'s, birth dates, family member names etc. & so it is exposed to several attacks such as easy to guess, dictionary attack, brute force, shoulder surfing, hidden camera, social engineering and malicious software's like key logger, spyware etc.

To overcome these limitations users can use the strong (complex) password. But it is difficult to remember. So to memorize easily users write the password on paper and so it is easily available to anyone. Also, the users nowadays tend to use the same password to access multiple accounts, thus reducing the security even more [2].

To solve the problems with textual passwords a new graphical password technique is introduced [3].

1.2 Graphical Password

Here different types of images or shapes are used as password. Also psychological research claims that images can be effortlessly be remembered by human than text [4 -7]. Studies have proven that images are easier to remember when compared to alphanumeric passwords. Because of the use of images, this technique is now resistant to several attacks such as dictionary attack, key logger, social engineering etc.

Generally, there are two types of graphical password technique, Recognition based and Recall based. In Recognition based, the user presents a random set of images and he/she is supposed to recognize the right images in correct order. In Recall based, the user has to reproduce something that he/she had selected or created during registration. So, when graphical password with the help of images is used it can easily be remembered. Also it will be difficult for the attacker to guess it through social engineering. It is the best alternative for textual password. But, it has limitations too. Shoulder surfing attack is a major threat for any user using graphical password. Shoulder surfing attack is a major threat for any user using graphical password. Shoulder surfing means watching over victims shoulder to get the credentials.

To overcome these issues, we have proposed a technique which is a combination of Recognition and Recall based approach. We have also focused on making the system such that it can provide resistance to shoulder surfing up to some extent and other possible attacks.

2. Related Work

Blonder originally introduced the graphical password technique in 1996. Since then a lot Research work has taken place on it. This section will further discuss about the existing technique for Recognition and Recall based approach.

2.1 Recognition Based techniques

Here, while registering the user is presented with a random set of images. The user then has to select a fixed number of images from the set as a password. During authentication, user has to recognize and select the images in the correct order which he/she had selected during registration.
Some examples:

2.1.1 Jensen et al. technique [8]

This technique was first introduced for PDAs and mobile phones. Here, the user has to choose a theme first (E.g. Buildings, Beaches, Cars etc.). Now the images based on the theme selected are displayed to the user in 5 x 6 grid in the form of thumbnails. The user has to select the images in a fixed sequence to set up the password. During Authentication, the user is required to recall the previously selected images and touch them with help of a stylus in the correct order. Here the size of password created is small as the number of images to select is limited to 30. A token number is assigned to each image and the order of selected images will form a numerical password for the user. It was observed that the numerical password is sometimes shorted than the textual password. To solve this issue the user can also select two images at a time on one click to increase the password size. But again this will confuse and increase the difficulty and complexity of the password for the user.

2.1.2 ImagePass technique [9]

In this technique, the user is presented with a grid of 30 images for registration. The user then has to select a predefined number of images and remember the order in which he had selected it. For Authentication, the user is now displayed a combination of real and decoy images in a grid format of 4x3. The user has to select the correct images in the right sequence to login.

This technique is also highly vulnerable to shoulder surfing as the password images are fixed and the grid is not that big. Which makes it really easy for the attacker to see and remember the images selected by the victim.

2.1.3 ColorLogin technique [10]

In this technique the login time is decreased with the help of background color. Several colors are used in the process which can be easily recognized by the authentic user but easily confuses the attackers. The password space here is small compared to text based password. This technique is clearly resistant to shoulder surfing attacks.

2.2 Recall Based Techniques

In Recall based, the user has to reproduce something that he/she had selected or created during registration, so as to successfully login.
It is further divided in two categories

2.2.1 Pure Recall Based Technique

In this technique the user is not provided with any hint to recollect the password.
For example:

2.2.1.1 Passdoodle technique [11]

In this technique, to login the user has to redraw the password in the exact order using a stylus onto a touch sensitive screen. The password could be a text, design or some sort of figure.

It was observed that the users can easily remember their password but sometimes the order in which they draw the doodle is not correct. Some users were fascinated by doodles drawn by another user and ended up using the same doodle as their password. This technique is various attacks such as guessing, spyware, shoulder surfing attacks.

2.2.1.2 Draw-a-Secret(DAS) technique [12]

In this approach, the user has to draw a picture on a 2-D grid of size G x G to register themselves. Each point on the grid is specified by discrete x, y coordinates. These coordinate values are stored in the order of the image drawn. During login phase, the user has to simply redraw the same picture by touching the same coordinates on the grid, in the same order as during registration. Here the users can keep the password as long as they want. Also, here the password space is much larger compared to textual passwords.

It was later observed that users would often forget the order of their stroke and sometimes it is rather easier to remember a text based password compared to DAS technique. At times the user would often choose weak passwords thus making it vulnerable for replay attack and dictionary attack.

2.2.1.3 Signature technique [13]

Here, the user has to authenticate oneself by drawing their signature with the help of mouse. The major advantage of this technique is that, here the passwords can easily be remembered and also signatures are hard to duplicate. But, it can become really difficult for the user to redraw the signature in the same perimeter as at the time of registration since not every user can be expected to be familiar with using mouse as a writing device. An alternative to solve this problem would be to use a stylus as a writing device. But adding another piece of hardware would further increase the cost of the system.

2.2.2 Cued Recall Based Technique
In this technique the user is provided with hint to recollect the password.
For example:

2.2.2.1 Blonder technique [14]

Blonder originally had first introduced the graphical password technique in 1996. Here, during registration the user is shown a fixed image with predetermined tap regions. The user has to click on the tap regions in a particular order. During login, the user has to click on the fairly accurate areas of those tap regions in the predefined sequence. Since the image actually helps the users in recalling their passwords, this technique is more suitable than text based password. But this technique lacks options as the user has to compulsorily click on fixed tap regions. Also it clearly vulnerable to shoulder surfing attack.

2.2.2.2 PassPoints Technique [15]

This technique was proposed to solve the issues faced in Blonder technique. Here, the user is a shown a random picture on which he/she can click on any place on the image to select click points. Unlike blonder technique, here the user does not have to select fixed click points in the predefined order. Each click point has a tolerance limit. During login, the user has to click inside the tolerances of selected click points in the correct order. Here, it was observed that users take longer time to remember their passwords than text based passwords. Many users would take multiple attempts to select click points within their tolerance limit to successfully login.

2.2.2.3 Passlogix V-Go Technique [16]

This technique was proposed by Passlogix Inc.. It is a private security firm located in "New York City, USA". This technique is commonly known as "Repeating a sequence of actions". Here the password is created by navigating through a random image such as bedroom, classroom, kitchen etc.. E.g. In the bedroom surrounding, the user can rest by lying on the bed, change clothes from the wardrobe, dress themselves up for any particular occasion. But the drawback here is that the size of password is really small. There are limited actions that can one can do in case they want to sleep. Hence these passwords can be easily predicted.

The above discussed techniques either lack user compatibility or are vulnerable to major shoulder surfing, spyware, key logger attacks. Our proposed technique is blend of recall based and recognition based technique. The system keeps a balance between security metrics and usability.

II. Existing System

The existing system [17] is a graphical password based approach. It is designed as a blend of Recognition and Recall based approach. The user authentication is done in two steps. It functions as follows:

3.1 Registration Phase:

1. The user has to make his/her profile by entering personal information and username.
2. A set of 25 images in a grid of 5 x 5 is displayed to the user. The images displayed here are common for everyone. Now, the user has to choose some number of images to set as a password. The user can select any image more than once. The selected images are now the password for step-I authentication.
3. Now the user is displayed only the selected images from the local memory/ stored image database. Out of which he/she has to select one.
4. The user is displayed the selected image along with a question set. He/she has to opt for any 3 questions out of the question set.
5. Individual click points are called as ROA (Region-Of-Answer). The user has to select 3 different ROAs on the image for the three different questions. Each ROA is saved in the memory with its x,y coordinates on the image.

Figure.1 Step-I Registration

Figure.2 Step-II Registration

3.2 Login Phase

1. The user will have to provide correct username and select the right images in the correct sequence for step-I authentication. The order of images within the grid will change at every login attempt.
2. Next, irrespective of whether or not it is correct, the preselected image and the preselected 3 questions are displayed to the user for step-II authentication.
3. The order of questions displayed is completely random. The user has to click on the correct ROAs as per the order of questions.
4. After entering correct details for both the steps, he/she is authorized to access the respective system.

Figure.3 Step-I Login

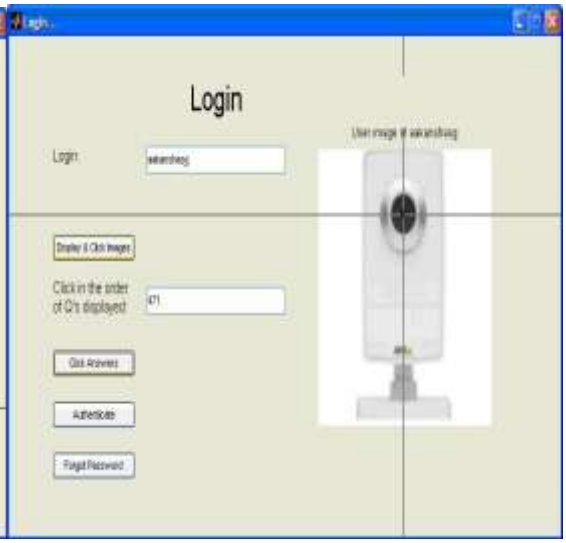

Figure.4 Step-II Login

4. Proposed System

Our proposed system is a 3 step authentication and authorization system which will overcome several vulnerabilities which we saw above. It is designed as a combination of Recognition and Recall based techniques.

4.1 System Architecture

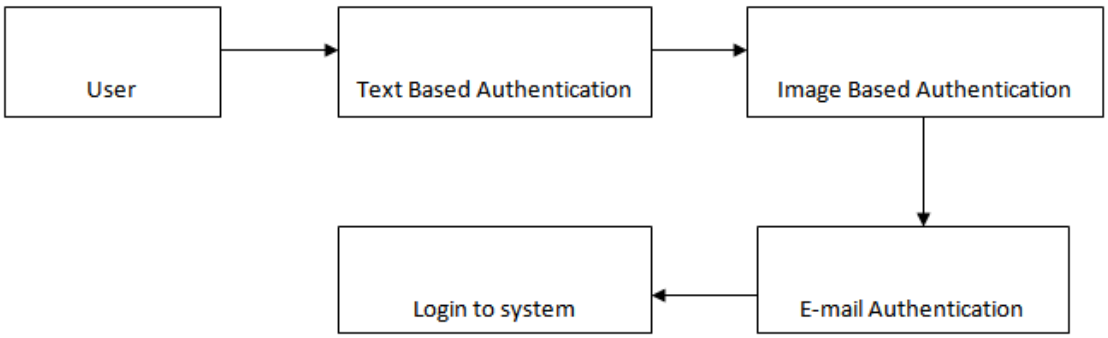

Figure.5 System Architecture

4.2 Registration Phase

1. The user will have to first provide their personal details and setup a username and standard alphanumeric password. This will secure the system against Brute-Force attack and Tempest attack. The set of 16 images will vary at every user registration and login.
2. Now a grid of 4 x 4 matrix with 16 images will appear. The user will now have to select any two image. Once the user selects any two images, the diagonal image of one selected image blink and it'll pop up. The user then has to set two click points on the displayed image. This technique will provide strong resistance against Shoulder Surfing and Spy Ware attack.
3. Once the above two steps are completed, an OTP will be sent on the users mobile number to authenticate it. The user has to simply enter the received OTP to successfully register oneself. .

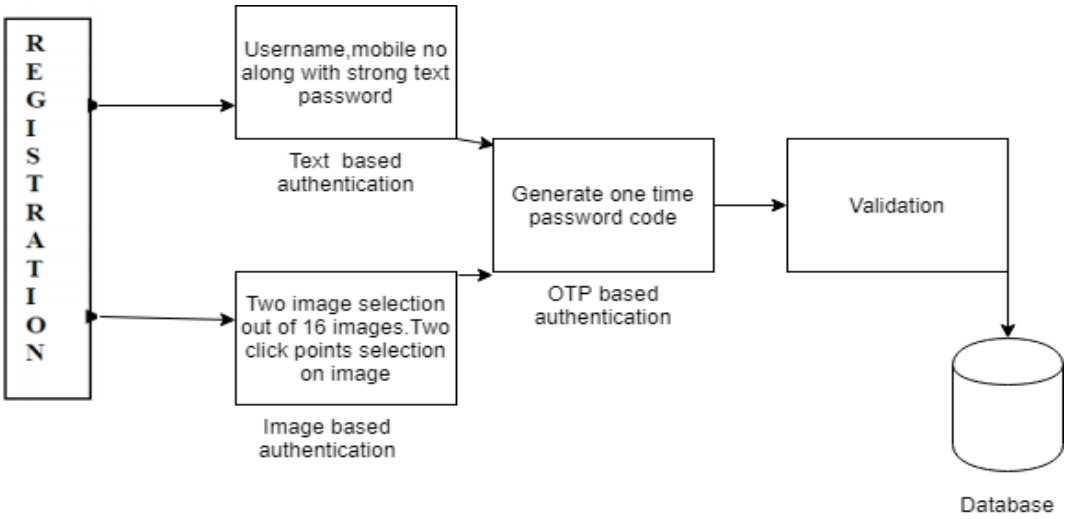

Figure.6 User Registration

4.3 Login Phase

1. Users will have to enter their user name and text password, which they had created during registration.
2. A grid of 4 x 4 matrix with random images will appear. The user will then have to correctly identify the image one he/she had set their click points on during registration phase.
3. If the above steps go correctly then the user will receive the OTP on the registered number. User can enter the OTP and complete the verification process.

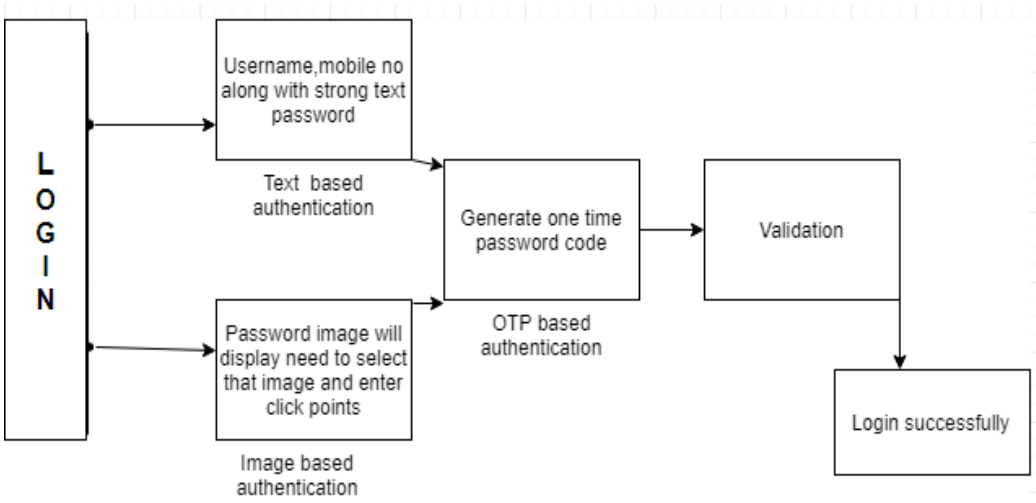

Figure.7 User Login

4.4 Flow Chart

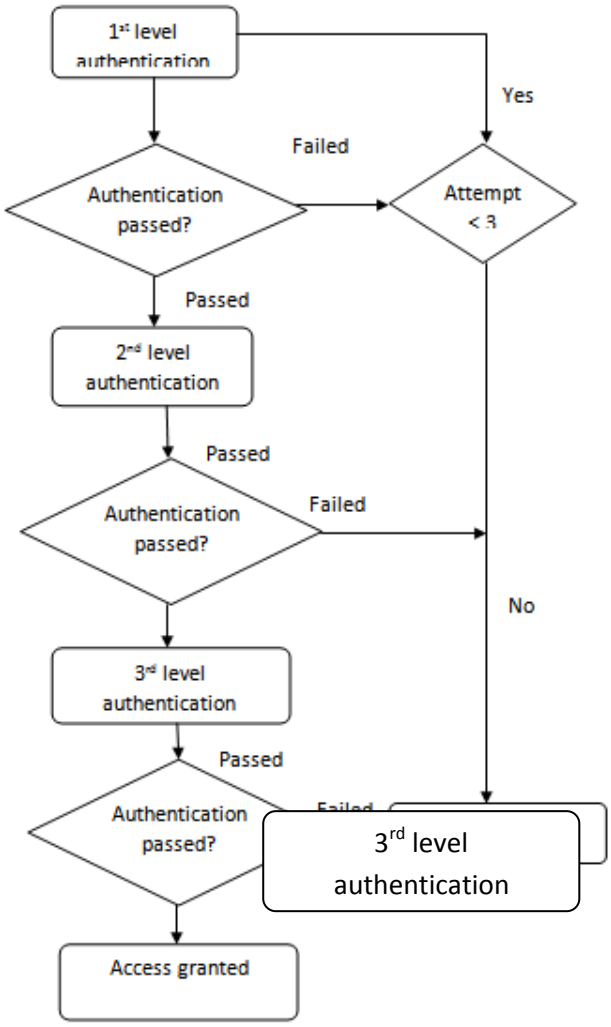

Figure.8 Flow Chart

III. Conclusion

Our designed system is a blend of Recognition based and Recall based approach. The system is easy for users to operate and more secure compared to the previous graphical based techniques. As the password space here is very large it provides strong resistance against brute force attack. The passwords created are easy to remember. Randomization during image selection for step-II authentication slves the vulnerability against shoulder surfing attacks. The system is resistant to all other possible attacks too. This system can be used in all kinds of business or personal enterprises to enhance their security. In future, we can add another feature to system that, if any user forgets their password then they can reset the password via a link which will be sent to the registered alternative email id of the user. In future our system can be made more easily accessible and more secure.

Acknowledgements

We would like to thank our project guide **Prof. Mamta Meena** for her enormous co-operation and guidance. We have no words to express our gratitude for a person who wholeheartedly supported the project and gave freely of his valuable time while making this project synopsis. All the inputs given by her have found a place in the project synopsis.

We are also thankful to our Principal **Dr. S.P. Kallurkar**, Our Project coordinators **Prof. Suvarna Pasambal**, **Prof. Deepali Maste**, **Prof Aruna Pavate**, **Prof Mamta Meena**, Our **Prof. Mahendra Patil H.O.D.** (Computer Engineering), and the entire staff and management of **Atharva College Of Engineering** who have provided us various facilities and guided us to develop a very good project idea.

References

[1] Renaud. "Evaluating authentication mechanisms". In L. Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pp.103-128. O'Reilly Media, 2005.

[2] D. Florencio and C. Herley. "A large-scale study of WWW password habits". In 16th ACM International World Wide Web Conference (WWW), May 2007.

[3] Xiaoyuan Suo, Ying Zhu, G.Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University.

[4] Kirkpatrick. "An experimental study of memory". *Psychological Review*, 1:602-609, 1894.

[5] S. Madigan. "Picture memory". In J. Yuille, editor, *I*magery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[6] A. Paivio, T. Rogers, and P. C. Smythe. "Why are pictures easier to recall than words?" *Psychonomic Science*, 11(4):137-138, 1968.

[7] R. Shepard. "Recognition memory for words, sentences,and pictures". *Journal of Verbal Learning and VerbalBehavior*, 6:156-163, 1967.

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

[9] "ImagePass - Designing Graphical Authentication for Security" Martin Mihajlov E- business Department Faculty of Economics Borka Jerman-Blazi Jožef Stefan Institute Ljubljana, Marko Ilievski Seavus Group 2011.

[10] Haichang Gao, Xiyang Liu, Ruyi Dai, "Design and Analysis of a Graphical Password Scheme", International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 675 – 678.

[11] Christopher Varenhorst" Passdoodles; a Lightweight Authentication Method ", Massachusetts Institute of Technology, Research Science Institute, July 27, 2004.

[12] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin," The design and analysis of graphical passwords", Proceedings of the Eighth USENIX Security Symposium. August 23-26 1999. USENIX Association 1–14, 1999.

[13] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[14] G. E. Blonder. Graphical passwords. United States Patent 5559961, 1996.

[15] Susan Wiedenbeck, Jim Waters, Jean - Camille Birget and Alex Brodskiy, Nasir Memon. PassPoints, "Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, 63(1-2): 102-127, July 2005.

[16] Passlogix,http://www.passlogix.com,Accessed on February 2007.

[17] "A New Graphical Password: Combination of Recall & Recognition Based Approach",Md. Asraful Haque, Babbar Imam World Academy of Science Engineering and Technology International Journal of Computer, Information, Systems and Control Engineering Vol: 8 No: 2, 2014.