International Journal of Research in Engineering, Science and Management
Volume-2, Issue-4, April-2019
www.ijresm.com | ISSN (Online): 2581-5792

Three Factor Graphical Authentication Mechanism

Vivek Solvande[1], Jay Chokshi[2], Mandar Gharat[3], Aparna Patel[4], Namit Kadget[5]
[1]*Professor, Dept. of Information Technology, St. John College of Engineering and Management, Mumbai, India*
[2,3,4,5]*Student, Dept. of Information Technology, St. John College of Engg. and Management, Mumbai, India*

***Abstract*: Today computer as well as security of information is the most significant challenge. Authorized and genuine users should access the system or information. Authorization and verification can't occur without authentication. For this authentication various techniques are available. According to this method images (pictures) are used as a password instead of text. The Psychological study says that human can easily remember images than text. These graphical passwords are easy to remember and difficult to guess. But due to graphic nature, nearly all the graphical password techniques are vulnerable to shoulder surfing attack. In this project, a new graphical password authentication technique is proposed which is resistant to shoulder surfing and also other types of possible attacks to some extent. This is a combination of recognition and recall based approach.**

***Keywords*: authentication, verification, authorization, graphical password.**

1. Introduction

These days computer as well as information security is the most significant challenge. Genuine and authorized users should access the system or information. Authorization and validation cannot occur without doing authentication. Hence to attain authentication different techniques are available. Among all of them the most popular and easy is the password technique. Password always ensures that computer or information can be accessed by those who have been granted right to view or access them. Traditional and commonly known password technique is a textual password. But these alphanumeric passwords are easy to crack through various types of attack. Hence to overcome these vulnerabilities, technique of graphical password is been developed. According to the name it suggests in this technique images (pictures) are used as a password rather than text. Also psychological study says that human can easily remember images instead of text. So as per this fact, graphical passwords are easy to remember and difficult to guess and attack. But due to graphic nature, almost all the graphical password techniques are vulnerable to shoulder surfing attack. Hence here, a new graphical password authentication technique is proposed which is resistant to shoulder surfing and also other types of possible attacks to some extent. It's a combination of recognition and recall based approach.

The human brains cells can process images easily. Due to this human characteristic, image based passwords are superior to alphanumeric passwords. As images are used it is therefore resistant to dictionary attacks, key loggers, etc. There exist two types of image based password techniques: Recognition based and Recall based. In Recognition based, multiple images are presented to the user and from that user has to recognize the right images in a correct sequence. In Recall based, user has to regenerate something that he/she has been created or selected during the registration process. Hence, as images are used in image based password it is easy to remember and difficult to guess and attack and it is best alternative for alphanumeric password. But it is observed that there are also some drawbacks of image based password techniques and the major drawback observed is that, it is endangered by shoulder surfing attack as pictures are used as a password. Shoulder surfing is watching over the person's shoulder to see the password. When a user enters password using keyboard, mouse, touch screen or other traditional input devices, an attacker may be able to see the user's password. This proposed technique is resistant to shoulder surfing over an extent and also to other possible attacks. It's a combination of recognition and recall based approach.

2. Literature survey

In this part, we will look at several same systems that are been researched and implemented by other researchers for further understanding on their methods and technique, refer to the reference page at the end of this report to search or text or even websites published.

In the year 2017, Smruthi Nanukuttan and Sruthi Nanukuttan [11] had proposed PCCP (Persuasive Cued Click Points) which was been designed to reduce the patterns and reduce usefulness of hotspots for attackers. Instead of five click-points sequence on one image, PCCP makes use of one click-point on five distinct images displayed in a sequence. The coming image shown is based on the previously entered click-point. Creating passwords with different click-points results in a distinct image sequences. Hence the main advantage of the PCCP is that to attack on the system is very difficult because even though the attacker tries the sequence of the click point he does not know about the registered sequence of images as it would not give any alert about the wrong sequence of images. Remembering the sequence of the click-points is no more a requirement on users,

since the system shows the pictures one at a time. PCCP also provides indirect feedback which is useful only to authorize the users. While logging on if the order of the click points goes wrong then also the wrong images will be shown one after other and after the final click point, SMS alert will be sent to the authorized user (alert: someone is fidgeting with your system.). Image security has become a critical issue. Hence to secure the image based password AES algorithm is used, where the click points entered by the user is encrypted and decrypted by using AES algorithm.

In the year 2017 Mrs. Mane Shruthi Nathuram and Dr. A.W. Kivelekar [9] had proposed a system in which password can be of any type; but most probably there are text based password. Alphanumeric passwords are the one which are commonly used, it's a string of alphanumeric characters. Alphanumeric passwords are easy to be memorized by users but it is also easy to hack by attackers. To provide more security, users use strong systems, use passwords which are are not easy for users to remember. Biometrics and tokens are used as an alternative to alphanumeric passwords but, it has it's own limitations as it will need extra system to get going. Image based passwords are of 3 types: Choice based Graphical Passwords, click based Graphical Passwords and Draw based Graphical Passwords. In the proposed system for registration of new users, users can select 3-5 images from database and select different point on the image. The selected viewport by a user is saved in database server and the order(sequence) of viewports is set as password of that particular user. When user wants to access the account, they need to enter the username and then the system will send binary number to user's registered mobile or mail-id. If the binary number is zero (0) user has to select wrong position and when the number is one (1) user has to select the right position of the image. Based on the binary number the password will be verified. When the user fails to select the exact wrong or right specified location on image, he/she would not able to access the account.

In 2018, Mr. V. Sunilanandh [12] discovered that there has been a great demand for Graphical Passwords since two decades as the traditional methods suffered from a large number of attacks which could be imposed easily. To begin with, the most common computer authentication method that makes use of alphanumeric passwords is focused. Ignoring the vulnerabilities, it is the user's natural behaviour that they would always prefer to go with short passwords for the ease of memorizing and also lack of awareness that how the attackers are likely to attack. These kind of passwords are broken mercilessly by attackers by many simple methods such as eaves dropping, masquerading, and other means like dictionary attack, shoulder surfing attacks, etc. To reduce the problems with primitive methods, latest methods have been proposed using graphical points as passwords. Thus, many other graphical password systems have been developed. The desirable quality associated with graphical passwords is that, psychologically humans can memorize graphical passwords way to better than text and hence is the best alternative which is proposed in this paper. There is a fast and growing interest in image based passwords since they are infinite in number, thus providing more security to any attack launched by intruders. The major aim of this work is to reduce the guessing attacks as well as encouraging the users to select random and difficult passwords that cannot be guessed.

In 2015, Mr. Amit Sawant and Mr. Jamdade Maruti [8] represented this research paper focuses on the integrated evaluation of the Persuasive Cued Click Points graphical password authentication mechanism, which includes usability and security. An important goal for this authentication system is to help users in selecting strong passwords, thereby increasing security. We had proposed the work to test usability of Cued Click Point using supportive sound signature w.r.t. CCP's of all images. In this mechanism a password consists of a sequence of some (e.g. images=5) images in which user can select one click point per image, we use sound signature. Here we suggest that the CCP provides greater security than pass points because number of images increase the workload for attackers. Users tend to use CCP instead of Pass Points, because selecting and memorizing only one point per image was easier and sound signature helps considerably in recalling the click points. The mechanism shows very good performance in terms of accuracy, speed and easy to use. This paper brings focus on the integrated evaluation of the Persuasive Cued Click Points image based password authentication system with sound signature, which includes security and usability

In 2012, Elizabeth Stobert and Sonia Chiasson [10] have represented an integrated evaluation of the Persuasive Cued Click-Points Image based password system, including usability and security evaluations, and implementation. The main focus for the authentication systems is to allow the users in selecting passwords of higher security, in the sense of being from an expanded effective security space. Here we are using persuasion in order to influence user choice in click-based graphical passwords, allowing users to select more random, and more difficult to guess, click-points or passwords.

3. Problem statement

The main challenge when implementing visual password schemes is finding an efficient solution to what is defined as the "password problem". This problem, as formulated in Wiedenbeck, arises because passwords are expected to comply with two conflicting requirements. Firstly, passwords must be easy to remember and the authentication process must be such that humans can execute it quickly and easily. The second requirement speaks to the security of the passwords. The passwords should look random and be hard to guess; it should not be necessary to write the passwords down or store them, since that would pose a security risk. The answer to these problems requires a scheme that offers a good trade-off between the usability and the security strength of the password scheme.

So we designed a system “Three factor graphical authentication mechanism” by using graphical passwords.

4. Proposed architecture

The proposed system is a modified and upgraded version of existing system to overcome the limitations of it. It has also two phases.

A. Registration Phase

1. The user enters the name, contact number and email address.
2. From grid of images selects any 4 image and remember sequence of images.
3. Select click points from two images and remember click points for the login.

B. Login Phase

1. Enter email of user.
2. Select 4 images in sequence which was selected at the time of registration.
3. Select click points from two images
4. From grid of images select 1st and 4th image position and enter it in textbox.
5. If user enters wrong password for 3 times then automatically mail will be send to particular user and you need to reset the password.

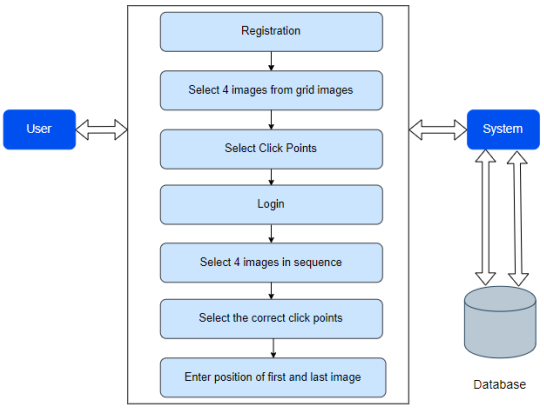

Fig. 1. Block diagram

5. Results

First the “Home Page” displays the basic use of the application developed that will request user to fill the details. The result is shown in Fig. 2. below,

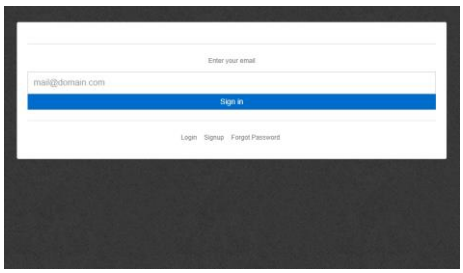

Fig. 2. Home Page

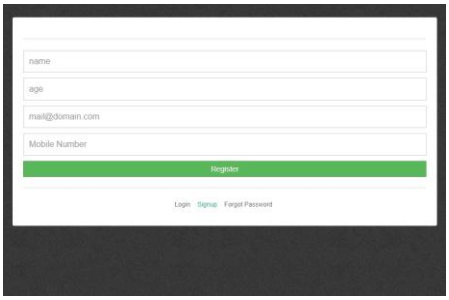

Fig. 3. Registration form

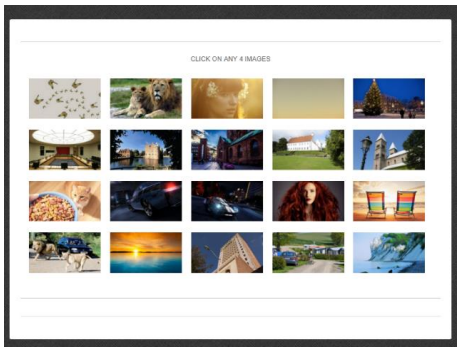

Fig. 4. Selecting 4 Images

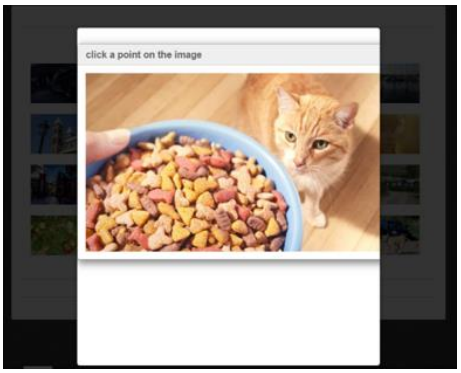

Fig. 5. Selecting a point on the image

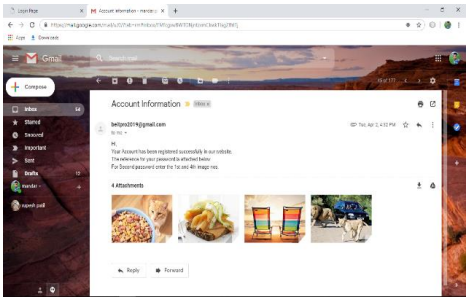

Fig. 6. Confirmation e-mail

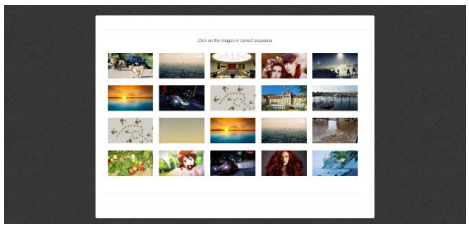

Fig. 7. Selecting 4 images in sequence (Login phase 1)

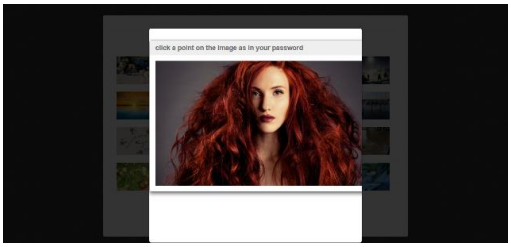

Fig. 8. selecting the same point on the image (Login phase 2)

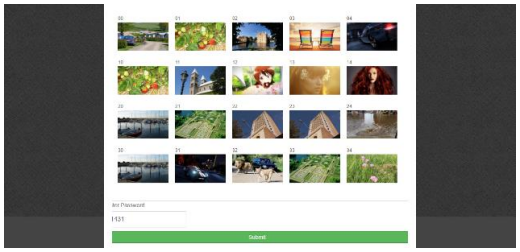
Fig. 9. Insert position of 1st and 4th image (Login phase 3)

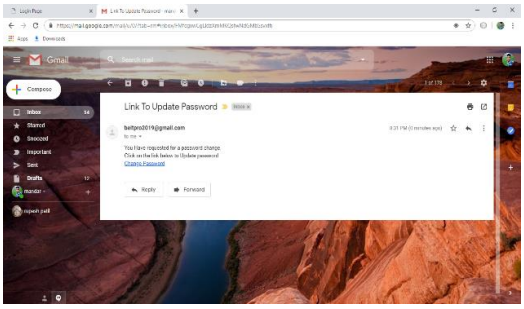

Fig. 10. Link to change password (Forgot password Phase)

6. Future scope

We are developing a project that would enable deaf people to get more involved in society. The idea of project is that, a camera-based sign language recognition system that would be in use for the deaf for converting sign language gesture to text and then speech. So, the objective is to design a solution that is intuitive and simple. Communication for majority of people will not be difficult.

This Sign Language Interpreter system will work as one of the futuristic of Artificial Intelligence and Computer Vision with user interface. It creates method to recognize hand gesture based on different parameters. And the main priority of this system is to be simple, easy and user friendly without making any special hardware. The further advanced version of the system might help the normal human being to convert their text into sign language which will build two-way communication. All computations will occur on single PC.

7. Conclusion

Mute people are isolated from the most common forms of communication in today's society such as warning, or any other form of oral communication between people in regular daily activities. Sign language is a primary means of communication. So, to communicate using sign language there is a glove-based system through which communication is possible. But it has to be recalibrated every time whenever a new user uses a system. The connecting wires restrict the freedom of moment.

So, the solution to this problem is image processing with deep learning. The project is implemented in such a way that it does not require gloves. The gesture has to be formed in front of the camera and the output is given in the form of text or audio. Thus, we can conclude that the system can interpret American Sign Language in real time environment and can act as a communication device between a signer and a non-signer person.

References

[1] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.
[2] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.
[3] 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 (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.
[4] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text" Journal of Computers, vol.5, no.5 May 2010.
[5] 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.
[6] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.
[7] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.
[8] Amit Sawant, Jamdade Maruti, "Persuasive cued click point authentication using Sound Signature", International journal of emerging technology in computer science and electronics, Volume 14 Issue 2 – April 2015.
[9] Shruti Nathuram Mane, A. W. Kiwelekar, "Cued Click Points Graphical Images with Binary based OTP Authentication", International journal of engineering science and computing, Volume 7 Issue No. 7, July 2017.
[10] Sonia Chiasson, Elizabeth Stobert, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism", IEEE transactions on dependable and secure computing, Volume 9 No. 2, 2012.
[11] Smruthi Nanukuttan, Sruthi Nanukuttan, Pooja. N. Patil, "Persuasive Cued Click Point (with E-mail and SMS services): Designing and Implementation", Imperial journal of interdisciplinary research, Volume 3 Issue 3, 2017.
[12] V. Sunil Anandh, "Graphical Password Authentication System Based On Persuasive Cued Click-Points", International journal of recent trends in engineering and research, March 2018.