ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Robust Authentication Scheme for Graphical Password

Snehal Tarkeshwar Ambade[1], Prof. Jagdish Pimple[2]

M. Tech Student, Department of Computer Science & Engineering, NIT College, Nagpur, Maharashtra, India [1]

Professor, Department of Computer Science & Engineering, NIT College, Nagpur, Maharashtra, India [2]

ABSTRACT: User authentication is an important subject in the field of information security. For apply security of information, passwords were introduced. Mostly in text based passwords, users usually create memorable passwords which are quite easy for hackers to figure out, but a strong system assigned passwords are harder for users to remember. Repeatedly using same passwords for various accounts help for memorability but decrease in security level. The text based passwords are the Traditional and most popular user authentication method, but have more security and usability problems. Alternatives like biometric systems and token based have their own drawbacks. Various existing graphical password techniques were studied and analysis. The existing Persuasive cued click point (PCCP) graphical password technique offer better security, but has accessibility problem and also system assign viewport in PCCP technique encourage users to select strong password but takes number of clicks to get desired portion which slows down the systems password creation process. This drawback of PCCP technique overcome in proposed system by providing better security while maintaining user accessibility.

KEYWORDS: Graphical password; Authentication; Security; Usability

I. INTRODUCTION

An authentication is a guarantee that the entity is one that demands to be. Authentication is any protocol or process that allows one entity to create the identity of another entity. The main function of authentication schemes is to permit system access only by legitimate users. Password authentication methods can be split into three main categories:Token based authentication, Biometric based authentication and Knowledge based authentication techniques [9].

Token based authentication technique is method in which tokens such as bank cards, key cards and smart cards are used to grant security. Lots of token-based Authentication systems can also use knowledge based techniques to increase security. For example, ATM cards are commonly used together with a PIN number.Biometric based authentication techniques, like iris scan, fingerprints and facial recognition etc. This scheme uses hardware which is costly. The main drawback of this technique is that such systems can be costly and also the identification process can be slow and often uncertain. Thus, this technique provides the highest level of security for authentication.

Knowledge based techniques are the most generally used authentication techniques. It includes both text based and image based passwords. The Graphical password systems are try to leverage the human memory for visual information which decrease memory burden that will help the selection and also use of more secure or less predictable passwords and discourage users from uncertain coping practices.

II. RELATED WORK

The main drawbacks of text based passwords are forgetting the password, stolen the password and weak password. Thus, an essential to have a strong authentication method is required to secure the information. Traditionally, ordinary passwords have been used for authentication but have security and usability problems. The Graphical password have been proposed as a substitute to the text-based password which inspired by the case that humans can remember pictures better than texts. Graphical passwords offer another alternative which is focus of this paper.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A. *Click Based Passwords:*

Graphical password systems are the knowledge based authenticationthat tries to leverage the human memory for visual information. A full review of graphical passwords is available elsewhere of interest, includes are cued recall click-based graphical passwords (also known as locimetric). In such systems, users identify and mark previously selected locations within single or more images. The images act as memory cues to help recall. Such systems include Pass Points and Cued Click- Points (CCP).

In cued- recall system, the user is provided with a clue to recall there password where they identify and target previously selected locations within single or more images. Here images itself act as memory cues to aid recall. This feature proposed to reduce the memory burden on users which is an easier memory task than pure recall.

Figure 1: Pass Point Technique

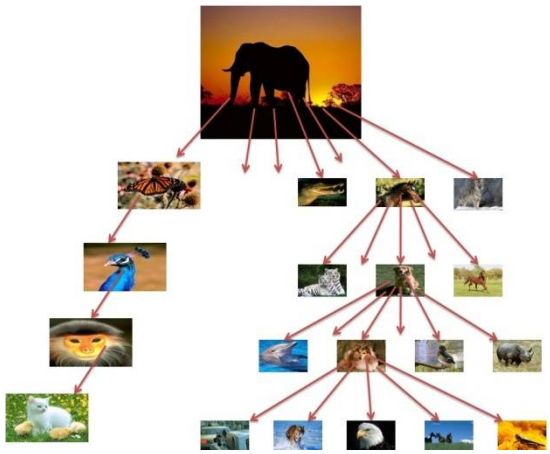

Figure 2: Cued Click-Point Technique

In pass point technique, a password contains sequence of click points on an image. The image is divided into tolerance squares. A user can select any points on the image as a password in any order during registration process. For login in system the user have to correctly click on the same points in the given image in correct order which is in the same tolerance squares as entered in the registration process. The main drawback of this technique is brute force attack and pattern attacks are possible [10].

In Cued Click Point (CCP) technique, users have to click on single point per image on five different images shown in order sequence. For making a different password, users have to click on different click points in different images. No evidence of patterns in CCP technique showed in user testing and analysis [12], thus pattern-based attacks look to be ineffective here. Attackers must do more work to exploit hotspots (most attractive part of an image),in CCP technique results showed that hotspots remained a problem.

B. *Persuasive Technology:*

Persuasive Technology was first express by Fogg [8] using technology to motivate and influence people to act in a desired way. An authentication system which uses Persuasive Technology should encourageand guide users to select stronger passwords, but didn'tforce system generated passwords. For more effective passwords, the users must not ignore the persuasive elements and the resulting passwords must be memorables. Thepersuasive cued-click point (PCCP) accomplishes this by making the task of selecting a weak password more boring and time consuming. The path of least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across users is minimized as the click points are more randomly distributed. PCCP's design follows Fogg's Principle of Reduction by making the desired task of selecting a stronger password more easily and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of selecting a password.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

III. PROPOSED WORK

The persuasive technology encourage user to select more difficult password for secure authentication scheme. PCCP is a good scheme but has accessibility problems, in password creation users may shuffle as often as desired but it slow down the process of password creation and it can take many clicks to shuffle viewport on user wanted area which can leads to increase in password creation time. In PCCP scheme system generated view port indicate very less attractive portion of an image, but if user want to choose his click on less attractive part or on their choose area, users may get disinterested by clicking on shuffle button several time to get that.

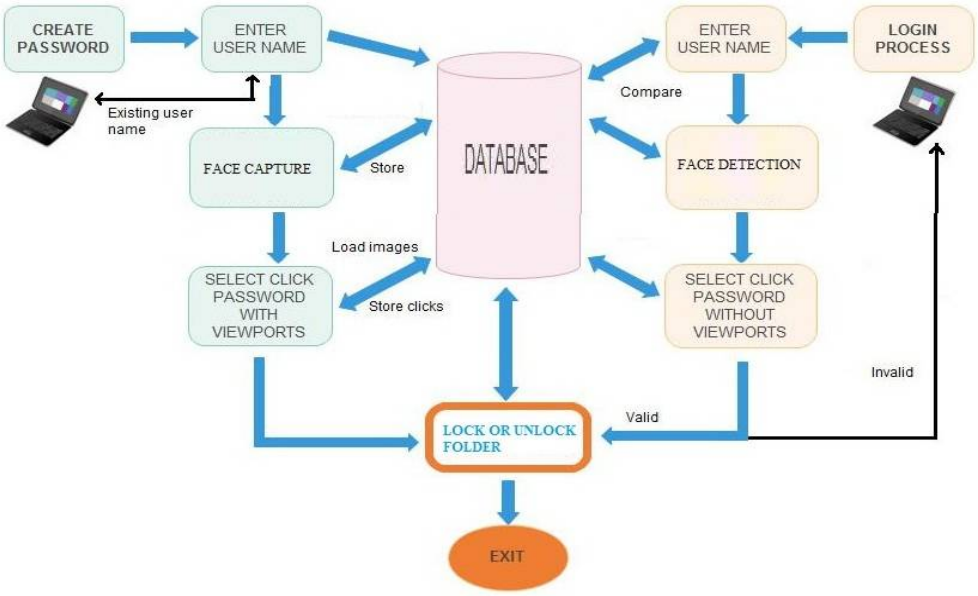

Figure 3: System Architecture for Proposed System

Proposed system is mainly the Persuasive Cued Click Points based graphical password scheme having user defined viewport. In this, the process of click points is done for 3 images by default in order to increase the security. User can increase the number of images to set password i.e. 3, 4 or 5 at creation. At the time of password creation user need to drag (as a viewport) the image in order to select as click point for next image to display. Dragging the portion of image will guide user to select strong and memorable password by recommendation message i.e. showing current and overall status of password strength. By providing user choice viewport on the image we try to maintain the usability. A User can now select at anywhere and any portion of image. While password creation, user's face detect using webcam in background, in order to increase the security. For login user have to click on portion of image which are selected at creation process. Dragging of viewport is disabled in login process. This propose scheme seem to like Cued-click point technique in which users can select password at any point on the image, But it differs with CCP because here we provide user defined viewport and suggest user to select strong password on image along with face detection. Thus by providing user choice viewport and face detection technique, we maintain the usability and security of graphical password.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

IV. MODULES DESCRIPTION

There are five modules in proposed system.

A. *GUI and Database:*

First have to design a graphic user interface (GUI) and database for proposed system, where all aspects and functionality is covered in this module a user-friendly GUI and Database can created. We use MySQL for database and JavaFX Scene Builder which is a design tool for the JavaFX platform. It allows for the simple drag and drop of graphical user interface components onto a JavaFX scene.

B. *Edge Detection:*

For Registration process, edge detection done so that system guide user for better password and reduce the Hotspot. We use canny edge detection algorithm whichaims to satisfy three main criteria as follows [15].

- Low error rate: Meaning a good detection of only existent edges.
- Good localization: Thereal edge pixels have to be minimized by detectingdistance between edge pixels.
- Minimal response: Only one detector response per edge.

The Process of Canny edge detection algorithm can be broken down to five different steps.

Step 1: Apply Gaussian filter to smooth the image in order to remove the noise.
Step 2: Find the intensity gradients of the image.
Step 3: Apply non-maximum suppression to get rid of spurious response to edge detection.
Step 4:Apply double threshold for determine potential edges.
Step 5: Track edge by hysteresis -Suppressing all the other edges that are weak and not connected to strong edges tofinalize the detection of edges.

C. *Face Detection:*

The human face is a dynamic object. The human face poses more problems than other objects as that comes in many coloursand forms. Facial detection and tracking provides many advantages when talking about security features.In proposed system we use Haar classifier for face detection. The core basis for Haar classifier object detection is the Haarlike features. These featuresuse the change in contrast values between adjacent rectangular groups of pixels rather than using the intensity values of a pixel [14]. Face detection in proposed system consist of following operations.

- For registration :
  Step 1: Start webcam of system and capture image.
  Step 2: Select image and make integral image with haar classifier features.
  Step 3: capture face, crop face and stored face with threshold value in database.

- For Login :
  Step 1: Start webcam of system and capture image.
  Step 2: Select image and make integral image with haar classifier features.
  Step 3: capture face, crop face and checking face with threshold value in database.

D. *Registration Process:*

User must enter the uncommon user name. The first image is always same. User can select password by using drag an area on image that user want to select as password and set a click point for next image (user choice viewport). The viewport is appears only at registration process. System guide user to select strong password. This process is repeated for

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

three numbers of images. Users face detection is also done while registration process. To increase the complexity, three images are to be selected and given a click point as password.

E. *Login Process:*

During login, the user must enter the user name first, if it present in database then only user can able to select the image. Viewports will not appear at login process. User must select the same sequence of images which he/she selected during registration process. If first click point is correct then only user can able to see the next image, if not he will get wrong image. With this sequence, the process is done for three numbers of images. Face detection is takes place here and check database about validity of profile, if its matches then only user get access.

V. TECHNIQUE USED

A. *Viewport:*

In proposed system there is a user choice viewport at the time of password creation user need to drag (as a viewport) the image in order to select as click point for next image to display (see figure 4). In existing system the image is slightly shaded except for viewport, but in proposed system image is clear. Viewport size is not fixed; user can drag a viewport up to whole image itself. As user select viewport on image the system suggest user about strength of password by status progress.

B. *Face Detection and Password Recovery:*

There is lots of attention gained by automatic human face recognition and identification in the last decades. In proposed pccp we use Haar Cascades classifier for face detection. At the time of password creation automatic face detection takes place and at time of logging system check database about validity of profile, if its matches then only user get access.

There is an option for reset password (see figure 5). User has to simply click on forgot password and put associate username and process for recovery of password, user face is captured and verify as it belong to same user or not. If verification is valid then user can recover or reset their password.

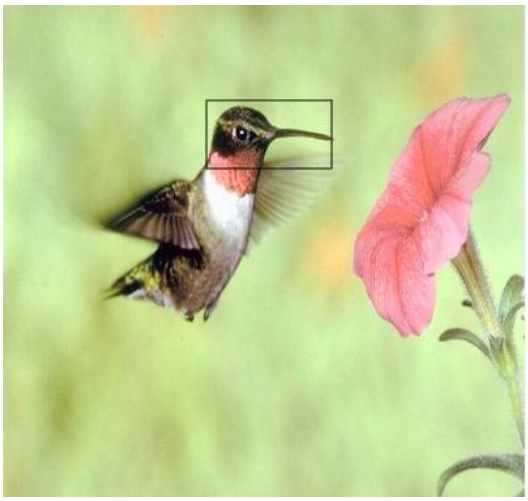

Figure 4: User choice viewport in proposed system

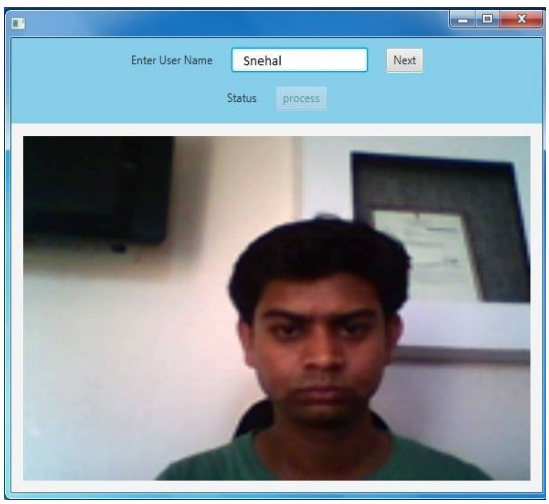

Figure 5: Password recovery in proposed system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

VI. RESULTS

Success rates are the number of trials completed without errors or restarts. Time required for password creation and login affects the success rate of system. We conducted 5 user studies for both PCCP and Proposed PCCP techniques for both password creation and login process. We gave basic training to understand both the techniques and gave two trial attempts each. We record third successful attempt for user study.

The empirical study was designed to explore ways of increasing the efficiency and also conducted study for the comparison of creation success rate and login success rate of existing PCCP's and proposed PCCP's. Success rates are reported at third attempt. Success on the attempt occurs when the password is entered correctly, without any error.

Users	Password Creation (time in second)	
	PCCP	Proposed PCCP
User 1	50	28
User 2	62	22
User 3	47	24
User 4	53	30
User 5	49	26

Table 1: Time for password Creation process

Users	Password Login (time in second)	
	PCCP	Proposed PCCP
User 1	26	16
User 2	28	15
User 3	31	17
User 4	24	19
User 5	22	17

Table 2: Time for password Login process

It clearly shows in Fig. 6 that the proposed PCCP system takes less password creation time as compares to existing PCCP and Fig. 7shows that it also takes less login time when compare to existing system. This user study (Table1 & Table2) shows that proposed scheme is more robust than existing one while maintaining the security. We found that existing system takes longer time as compare to proposed system. As per resultant graph shows the proposed PCCP have better success rate as compare to existing technique.

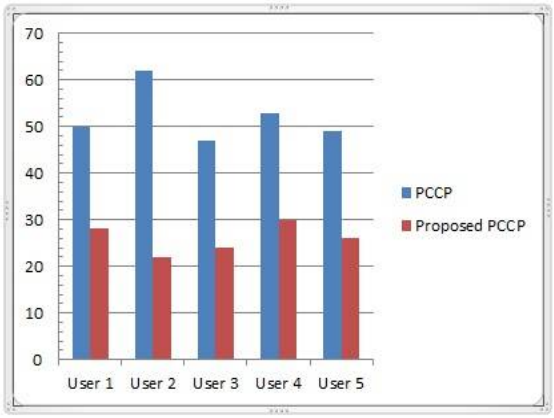

Figure 6: User study shows that proposed PCCP system takes less password creation time as compares to PCCP (from table1)

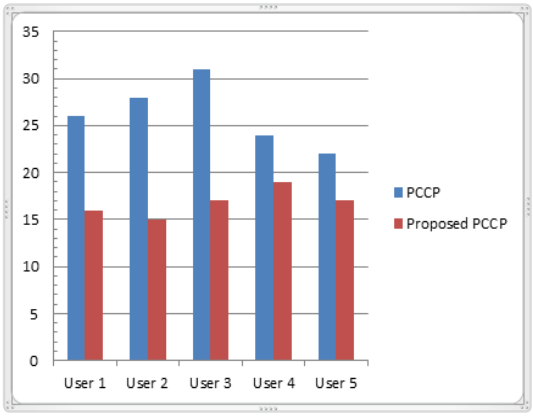

Figure 7: Comparison between login Success rate of existing PCCP and proposed PCCP (from table2)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

VII. CONCLUSION

This paper for graphical passwords mechanism shows that people are better at remembering picture passwords rather than text based passwords. Existing Persuasive cued-click point graphical password technique offers better security but have certain accessibility problem. The Proposed system overcomes the drawbacks of PCCP technique by providing new user choice viewport and provides more security by introducing face detection technique in it. Thus, proposed work provides better security while maintaining accessibility.

ACKNOWLEDGMENT

We would like to express our appreciation to our parents and all the professors who helped us to understand the importance of knowledge and show us the best way to gain it.

REFERENCES

1. PriyankaGunde, UjjwalaKokate , "Graphical Password Authentication by Using Persuasive Click Point Method", in International Journal of Science and Research (IJSR), Volume 5 Issue 2,pp. 2138-2140 ,February 2016.
2. G.Kalpana, G.Akshaya, "unpredictable password generation using graphical authentication and decentralized encryption", in International Journal of Scientific Engineering and Applied Science (IJSEAS), Volume-2 Issue-3, pp. 368-371, March 2016.
3. Y. Sravana Lakshmi, "Evaluation of a Knowledge Based Authentication Mechanism through Persuasive Cued Click Points", in International Journal of Computer Applications Technology and Research, Volume 4 Issue 9, pp. 633 - 639, 2015.
4. NileshChangune, Ganesh Shinde, SagarChaugule, SandeepHelkar, "graphical password authentication using pccp with sound signature", in IJRET: International Journal of Research in Engineering and Technology, Volume 4 Issue 1, pp. 46-49, Jan-2015.
5. AtishNayak, Rajesh Bansode, "Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points", in 7th International Conference on Communication, Computing and Virtualization,Procedia Computer Science 79, pp. 553-560,2016.
6. S. B. Sahu, A. Singh "Enhanced User Graphical Password Authentication with an Usability and Memorability," published in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5 Issue 6,pp. 477-484,June 2015.
7. R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM ComputingSurveys (to appear), vol. 44, no. 4, 2012.
8. Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and P. C. van Oorschot, "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism" in IEEE Transactions on Dependable and Secure Computing (TDSC) , volume 9, no.2,march/april 2012.
9. X. Suo, Y. Zhu, G. Owen, "Graphical Passwords: A Survey", in annual computer security conference (ACSAC), December 2005.
10. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud." Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", International Journal of Human-Computer Studies, volume 63, no. 1-2,pp. 128-152, 2005.
11. S. Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon."Pass Points: Design and longitude in an evaluation of a graphical password system". International Journal of Human-Computer Studies, volume 63, no.1-2, pp. 102-127, 2005.
12. S. Chiasson, P. C. van Oorschot, and R. Biddle."Graphical password authentication using Cued Click Points". In European Symposium on Research in Computer Security (ESORICS), LNCS 4734, pp. 359-374, September 2007.
13. Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot, "Influencing user toward better password:Persuasive Cued Click-Points" in Human computer interaction (HCI), The British computer society, September 2008.
14. Phillip Ian Wilson and Dr. John Fernandez, "Facial feature detection using haar classifiers", CCSC: South Central Conference, JCSC 21, 4, pp. 127-133, April 2006.
15. Jamil A. M. Saif, Mahgoub H. Hammad, and Ibrahim A. A. Alqubati, "Gradient Based Image Edge Detection", IACSIT International Journal of Engineering and Technology, Vol. 8, No. 3, pp. 153-156, June 2016.

BIOGRAPHY

Snehal Tarkeshwar Ambade is a M. Tech Student in Department of Computer Science and Engineering, Nagpur Institute of Technology, Nagpur, Maharashtra. He received Bachelor of Engineering (CSE) degree in 2014 from RTMNU, Nagpur, MS, India. His research interests are Image Processing, Computer Networks etc.

Jagdish Pimple is Assistant Professor in Department of Computer Science and Engineering, Nagpur Institute of Technology, Nagpur, Maharashtra. He received Master of Technology degree and has more than 10 years of teaching experience. His research interests are Computer Networks, Image Processing and Data Structure etc.