ISSN:0975-9646

Securing Image Password by using Persuasive Cued Click Points with AES Algorithm

Smita Chaturvedi[#], Rekha Sharma[*]

[#]*Student ME-Computer Engineering, TCET, Mumbai University*
Thakur College of engineering & technology, India

[*]*Associate Professor, HOD Computer Engineering, TCET, Mumbai University*
Thakur College of engineering & technology, India

***Abstract*— In Digital environment authentication plays a major role. For authentication purpose the graphical based technique is used. The purpose of this paper is increasing the security space and avoiding the weakness of conventional password. The most common computer authentication method is to use alphanumeric user name and passwords. User often creates passwords that are memorable which is easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods where in graphical picture are used as a password. By using graphical password scheme shoulder surfing attack, masquerading and eavesdropping can be minimized. In this paper, we have changed the way of clicking on the images and to make the password more secure Advanced Encryption Standard (AES) technique is used so that authentication can become more secure and password can be generated, authenticated & protected easily. This paper presents the idea of new graphical idea for authentication. This system can be used for any online/offline system.**

***Keywords*— Authentication, graphical passwords, usable security, Persuasive cued click points, Advanced Encryption Standard**

I. INTRODUCTION

Usable Security has unique usability challenges because the need for security often means that Standard human-computer-interaction approaches cannot be directly applied.. The most common computer authentication method is use alphanumeric user name and passwords .User often creates memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. Security in transmission of digital images has its importance in today's image communications due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access, Image security has become a critical issue. So to secure the image password AES algorithm is used in which the click points entered by the user is encrypted and decrypted by using AES algorithm.

The following figure 1 shows a System Architecture of PCCP and AES method.

As shown in the figure 1 above there are basically three modules user registration module, picture selection process, and system login process. Here we will first make the application which we will use for entering our login id and image password. Here we will use Persuasive Cued Click Points for generating the password and user has to click on the images for their passwords. The PCCP technique in which we will divide the image into 4*4 grids that means each image will divide into 16 different unique grids. At the place where user will click the image that particular pixel's value will be fetch as X and Y coordinate's value and then calculated using AES algorithm.

After fetching the value of X & Y coordinate AES encryption is perform on X & Y coordinate's value and then securely stored the password into the database. The problems of knowledge-based authentication, typically text-based passwords, are well known.

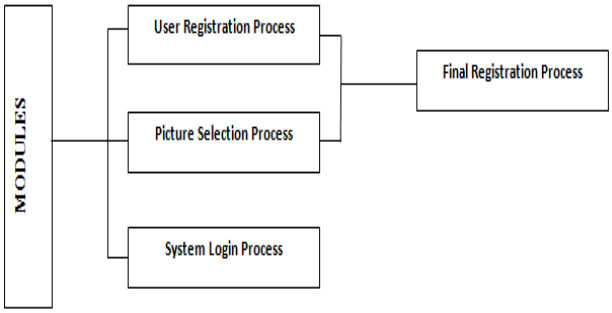


Figure 1: System Architecture of PCCP & AES algorithm

Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. A password authentication system should encourage strong passwords while maintaining reputation. We propose that authentication schemes allow user choice while influencing users towards stronger passwords. In our system, the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes choosing a more secure password the path-of-least-blocking.

II. BACKGROUND

Graphical passwords have been proposed as alternatives to text passwords to improve both usability and security issues. Text passwords are the most popular user authentication method, but have security and usability problems. Alternatives such as tokens and biometric systems have their own drawbacks [8]–[10]. In this system

to mitigate the problems with traditional methods, advanced methods have been proposed using graphical passwords. Greg Blonder first described the idea of graphical password in the year 1996. For Blonder, graphical passwords are nothing but the predetermined image that the sequence and the tap regions selected are interpreted as the graphical password. The major goal of this method is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess.

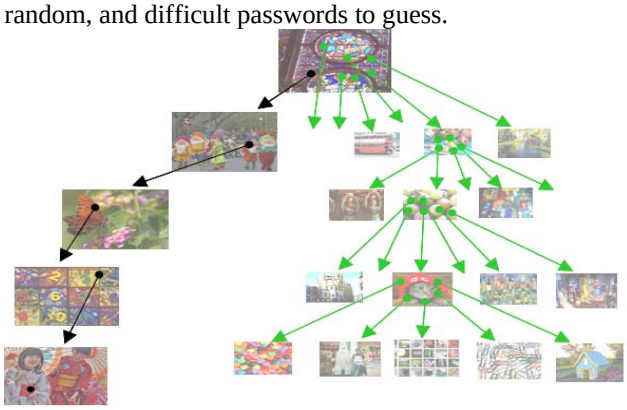


Figure 2. A user navigates through images to form a CCP password. Each click determines the next image [1]

Click-based graphical passwords: Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information of graphical passwords is available elsewhere Of interest herein are cued-recall click-based graphical passwords. In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues to aid recall. Example systems include PassPoints and Cued Click-Points.

A. Pass Points

In PassPoints, passwords consist of a sequence of five click points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. Although PassPoints is relatively usable, security weaknesses make passwords easier for attackers to predict. Hotspots are areas of the image that have higher likelihood of being selected by users as password click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess PassPoints passwords. Users also tend to select their click-points in predictable patterns [5] (e.g., straight lines), which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against PassPoints based on image processing techniques and spatial patterns are a threat.

B. Cued Click-Points

A precursor to PCCP, Cued Click-Points (CCP) [7] was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click-point on five different images shown in sequence. The next image displayed is based on the location of the previously entered click-point (Figure 2), creating a path through an image set.

Creating a new password with different click-points will result in a different image sequence. The claimed advantages are that password entry becomes a true cued-recall scenario, wherein each image triggers the memory of corresponding click-points. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. Although attackers must perform proportionally more work to exploit hotspots, results showed that hotspots remained a problem [2].

C. Persuasive Cued Click-Points

Persuasive Technology was first articulated by Fogg [6] as using technology to motivate and influence people to behave in a desired manner. An verification system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be adequate, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed below, PCCP achieves this by making the task of selecting a weak password more monotonous and time consuming.

The issue remain with the PCCP was shoulder surfing attack. This attack was not removed from the persuasive cued click points. The next issue remains with the persuasive cued click points, it was difficult for the user to remember the different images. It was difficult for the users to remember many images for the login. As we know that human can remember limited number of images

D. Persuasive Cued Click-Points with Advanced Encryption Standard (PCCP AES)

To remove the shoulder surfing attack and to provide the security on the click points of the user's password, AES algorithm is applied on the click points and in PCCP technique the system divide the images into 16 different grids on which users will click, after clicking on the image first time that particular grid will be expanded and displayed in the front of the user like this the image will be divided till the third click by the user. After selecting an image the user can upload the image for further process. PCCP uses one click point on three different images shown in sequence. Place where the user will click the x and y coordinate of the image is taken by the system and on value of x and y the advanced encryption Standard algorithm is applied and after encryption whatever the value of the x and y coordinate is coming that information is stored in to the database for authentication purpose.

III DESCRIPTION OF PERSUASIVE CUED CLICK-POINTS WITH ADVANCED ENCRYPTION STANDARD

A. Persuasive Technology

Persuasive technology used to motivate and influence people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide

and encourage users to select stronger passwords, but not promulgate system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed below, PCCP accomplishes this by making the task of selecting a weak password more tedious 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).

By adding a persuasive feature to CCP [7], PCCP [2] encourages users to select less predictable passwords, and makes it more difficult to select passwords where all five click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a viewport. The viewport is positioned randomly, rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots.

B. Advanced Encryption Standard

Cryptography: It is the practice and study of techniques for secure communication in the presence of third parties. AES is one of the popular and mostly used encryption techniques. It was officially announced as the new encryption standard in 2001 which has block size of 128 bits and key length 128, 192, 256 bits using 9, 11, 13 cycles respectively. Each cycle consist of four steps Byte substitution, shift row, mix column, add sub key. Less chances of attacks on AES because of key length is more in AES. This is how the system will work, at the time of the registration process the user has to enter his/her name, email id, phone no etc. after filling all the information user has to click on the login button after that page will redirect to other page like login.

At login page the browse option is provided, the user should browse for the image. In this system we have given the option of both user and system based images. User can upload the image from his/her system or the user can upload the images from the server. After uploading the image user has to click at one point on the image, after level 1 of the image the image on which user has clicked that image will be expanded at level 2 and again user has to click on that level and after second click the user has to click on the third level click on the image at the end. At all the level of click the user's click information is stored like the particular x and y coordinate where user had clicked on that coordinate AES is applied and then the value of click point is stored in to the database, this was the process of registration.

C. Hotspot

Hotspots are areas of the image that have higher likelihood of being selected by users as password click-points. Users also tend to select their click-points in predictable patterns [5], [2] (e.g., straight lines), which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against PassPoints based on image processing techniques and spatial patterns are a threat [2]. Specifically, when users create a password, the images are slightly shaded except for a viewport (see Figure 2). Users must select a click-point within this highlighted viewport and cannot click outside of the viewport, unless they press the shuffle button to randomly reposition the viewport. While users may shuffle as often as desired, this significantly slows password creation. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images.

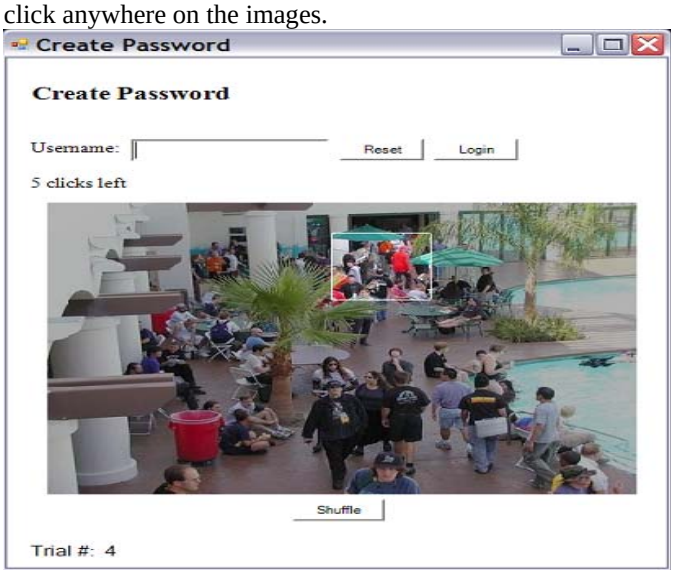


Figure 3. The pool Image [1]

IV PCCP AND AES TECHNIQUE

By using the combination of Persuasive Cued Click Points (PCCP) and advanced encryption standard (AES), we are getting the advantages of both the PCCP and AES technique. In this technique user has to click at three click points for authenticate themselves. If user is successfully authenticating them then he/she is able to get then notes of JAVA pdf. In the system, it provides both the text as well as graphical password so it is highly secure .By using the AES technique the password of the user is encrypted by using AES algorithm and so that user's password is securely stored in the database. So by providing the combination of both the PCCP and AES technique together we can securely provide the graphical password for the user and stored to the database.

Following are the images of our system in which the registration page, login page and the system architecture is given.

Registration:

As shown in the figure 4 before accessing the JAVA pdf user has to register them. In registration process the user has to fill the registration form and he/she has to enter id and text password and after that he/she to choose image password by clicking on the image thrice user can registered themselves.

Login:

In login process, the user has to enter their login id and text password which they have entered at the time of registration and after that they have to click on the selected image at three places one after the other.

In figure 5 the screen shot of registration process is shown in which the image is divided into 16 unique grids and the some part of the image is visible to the user If he/ she want to click on the different area of the image then they have to click on the shuffle button until the view port reached to that particular area. By providing the concept of view port it is less likely for attackers to attack on the image.

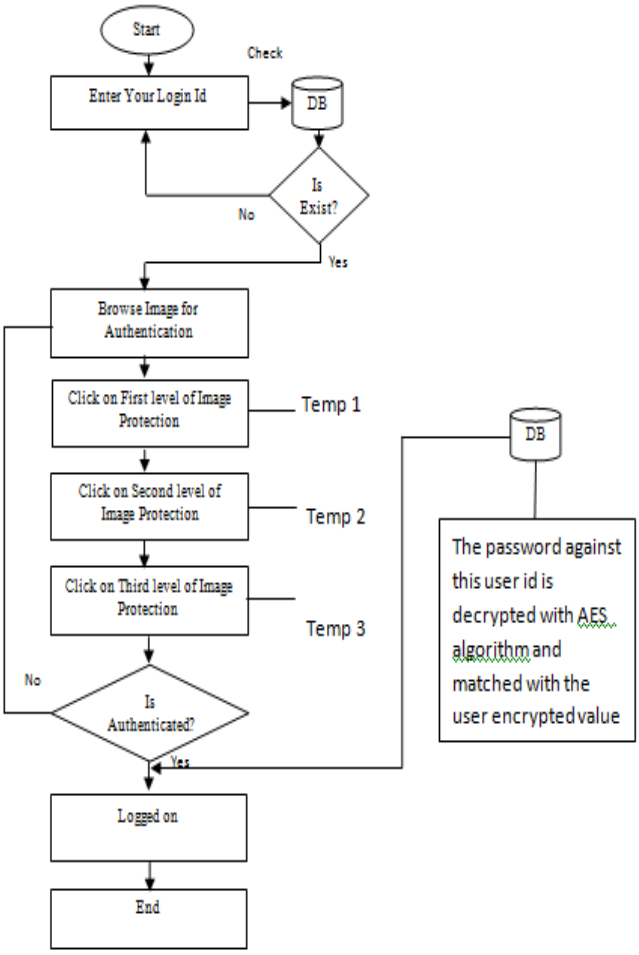


Figure 4. Registration in PCCPAES technique

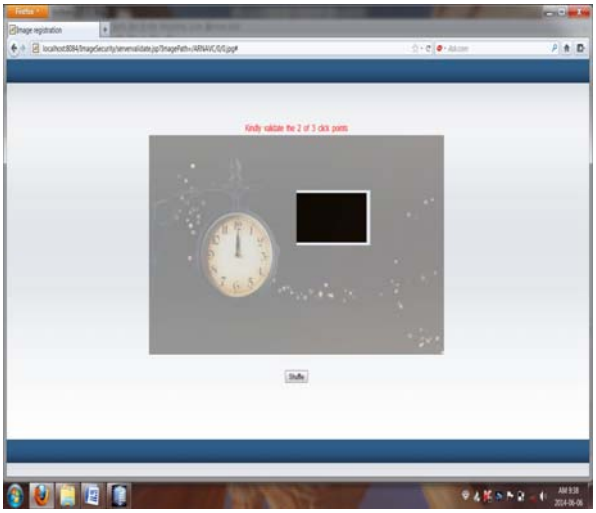


Figure 5. The watch image of PCCPAES

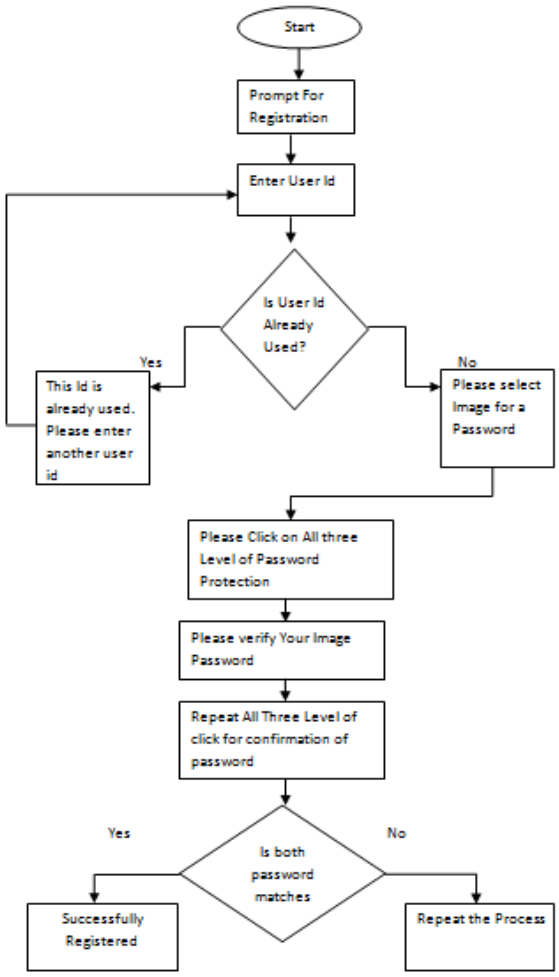


Figure 6. Login in PCCPAES technique

V SECURITY

A. Guessing Attacks

Against PCCP the most basic guessing attack is a brute-force attack, with expected success after examining half of the password space. However, asymmetrical password *distributions could allow attackers to improve on this attack model.*

B. Capture Attacks

Password capture attacks occur when attackers directly obtain passwords by blocking user-entered data, or by tricking users into disclose their passwords. For systems like PCCP, CCP, and PassPoints (and many other knowledge based authentication schemes), capturing one login instance allows deceitful access by a simple replay attack.

Shoulder-surfing: All three cued-recall schemes discussed (PCCP, CCP, PassPoints) are endangered to shoulder-surfing although no published experiential study to-date has examined the extent of the threat. Observing the approximate location of click-points may reduce the number of guesses necessary to determine the user's password. A considerably more complicated substitute is to make user input invisible to cameras, for example by using eye-tracking as an input mechanism many images from the server instead of only one. Malware: Malware is a major interest for text and graphical passwords, since keylogger,

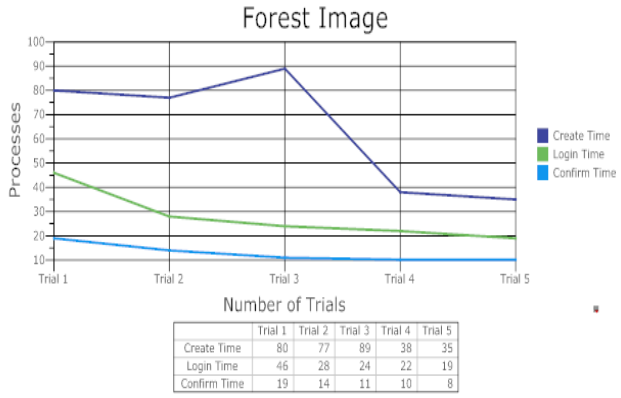
mouse-logger, and screen scraper malware could send captured data remotely or otherwise make it available to an attacker.

VI RESULTS & DISCUSSIONS

A. *Study on PCCP & AES technique*

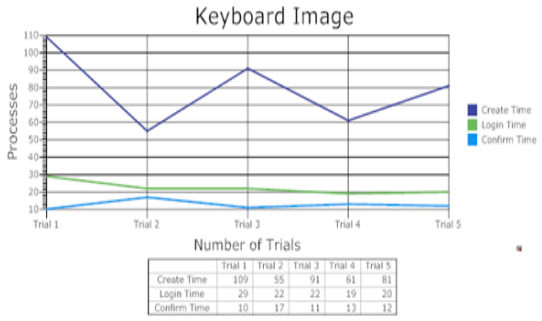
Students from undergraduate Engineering College are participated in this study. The study is performed in one week. Initially the students registered themselves to the PCCPAES technique and after one week time they are again called to login. Total Thirty One (31) images are kept on the server and Eleven (11) images are taken from the system. At the time of survey it is said that they have to imagine that they are registered they for the bank account websites.

In study it is found that as the number of trials is increasing the less time is taken for registration and login process.
In this section the system mentioned that after registration process, user has to click on the login button if he/ she is an already user. After clicking on the login button user has to enter his/her name and then text password.



	Trial 1	Trial 2	Trial 3	Trial 4	Trial 5
Create Time	80	77	89	38	35
Login Time	46	28	24	22	19
Confirm Time	19	14	11	10	8

Figure 7. Study on the Forest image



	Trial 1	Trial 2	Trial 3	Trial 4	Trial 5
Create Time	109	55	91	61	81
Login Time	29	22	22	19	20
Confirm Time	10	17	11	13	12

Figure 8. Study on the Keyboard image

After clicking on next button one image will displayed in front of user and user has to click on the image thrice. If the login is successful then message will prompt as “Done” and if click point is wrong then the message will prompt as “Image Clicks miss matched Please Retry Kindly validate the 3 level click points”. Following login flowchart will explain how exactly this system will work.

Figure 9. Forest Image

Figure 10. Keyboard Image

B. *Survey on PCCP & AES technique*

The survey is taken of Thirty (30) participants and results are collected on the basis of 10 likert scale questions. The range of answers are divided into five (5) parts from strongly disagree to strongly agree.

TABLE 1 LIKERT SCALE

Strongly Disagree	[1-2]
Mildly Disagree	[3-4]
Neutral	[5-6]
Mildly Agree	[7-8]
Strongly Agree	[9-10]

TABLE 2 RATING OF QUESTIONS FILLED BY PARTICIPANTS

Question	Mean	Median
1. I could easily create a graphical password	7.53	8.0
2. * Someone who knows me would be better at guessing my graphical password than a stranger (i.e. ,When reversed: “Someone who knows me would not be any more likely to guess my password than a stranger”)	6.16	6.0
3. Logging on using a graphical password was easy	7.6	8.0
4. Graphical passwords are easy to remember	7.67	8.0
5. * I prefer text passwords to graphical passwords (i.e., when reversed: “I like graphical passwords at least as much as text passwords”)	5.73	6.0
6. * Text passwords are more secure than graphical passwords (i.e., when reversed: “Graphical passwords are at least as secure as text passwords”)	5.7	6.0
7. I think that other people would choose different points than me for a graphical password	7.56	8.0
8. With practice, I could quickly enter my graphical password	7.9	8.0
9. “How easy was it to create a password on this image?”	7.73	8.0
10. “How difficult will it be to remember your password in one week?”	4.53	4.0

After successfully confirming their password, the Ten (10) point-likert scale questions are asked to the participants & the results are collected. The following figure 11 shows the results collected from the participants.

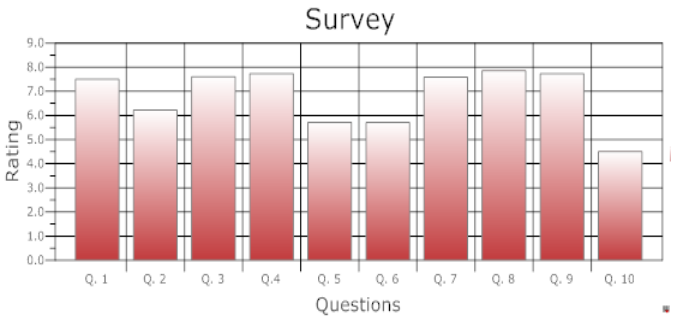


Figure 11. Study on PCCP with AES

VII CONCLUSION & FUTURE WORK

The combination of persuasive cued click points & advanced encryption standard provide the better results in authentication system. Graphical authentication scheme is better to remember for the user. As we are providing the only one image for the authentication purpose it is easier for the user to remember and difficult for the attacker to attack because it is difficult for the attacker to see at click points area of the image. In future we can provide the feature of asking from the user to enter their number of click points for their authentication system and likewise variable click points can be provided for the user.

REFERENCES

[1] S. Chiasson, Member, IEEE, Elizabeth Stobert, Alian Forget, Robert Biddle, Member, IEEE, and P.C. van Oorschot, Member, IEEE Oct 2011.

[2] S. Chiasson, R. Biddle, and P. van Oorschot, "A second look at the usability of click-based graphical passwords," in ACM Symposium on Usable Privacy and Security (SOUPS), July 2007.

[3] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing users towards better passwords Persuasive Cued Click-Points," in Human Computer Interaction (HCI), The British Computer Society, September 2008.

[4] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle,"Multiple password interference in text and click-based graphical passwords." in ACM Computer and Communications Security (CCS), November 2009.

[5] Davis, D., Monrose, F., and Reiter, M.K. On User Choice in Graphical Password Schemes. USENIX Security 2004.

[6] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring usability effects of increasing security in click-based graphical passwords," in Annual Computer Security Applications Conference (ACSAC), 2010.

[7] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," International Journal of Information Security, Springer, vol. 8, no. 6, pp. 387–398, 2009.

[8] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The memorability and security of passwords," in Security and Usability:Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 7, pp. 129–142.

[9] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.

[10] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol. 91, no. 12, December 2003.

[11] PD Photo. http://pdphoto.org Accessed Feb. 2007.