Graphical Password Authentication using a Fake Cursor Approach

Pratik P. Jog
M.E. Student,
Department of Computer Science,
Thadomal Shahani Engineering College,
University of Mumbai, Mumbai-50.

Archana B. Patankar, PhD
Associate Prof.
Department of Computer Science,
Thadomal Shahani Engineering College,
University of Mumbai,
Mumbai-50.

ABSTRACT
This paper presents a novel method for solving the shoulder surfing problem commonly found in the graphical password authentication system. Authentication of a user is the critical aspect required to gain access to secure and confidential data. Most of the current systems are using alphanumeric password for authentication purpose, however alphanumeric passwords have some disadvantages for example in terms of memorability. So a substitute to alphanumeric passwords, graphical passwords have been recommended. Graphical passwords have been planned to make passwords more unforgettable and effortless for the people to use. During a graphical password authentication, end users click on particular points on images rather than submitting alphanumeric characters. Graphical password schemes can be grouped into two general categories based on the type of cognitive activity required to remember the specific password: recognition and recall. Recognition is the easiest for human memory where on the other hand pure recall is most difficult since the information must be accessed from memory with no triggers. This paper focuses on Cued recall which falls somewhere between these two as it offers a cue which must establish a context and trigger the stored memory. Graphical passwords generally suffer from shoulder surfing problem. The problem of shoulder surfing is solved using a fake cursor approach. This is a new approach in which two cursors are displayed during the login phase and only the authorized user is aware which is the original cursor and which one is the fake cursor.

Keywords
Fake cursor, Graphical Password, Security, Authentication

1. INTRODUCTION
For any application, Security is the main principal element to consider [11].In digital and modern environment, authentication plays a major role [5]. A good authentication system should encourage robust passwords while preserving memorability [10]. An excellent password authentication system should boost less anticipated passwords along with preserving memorability and security [3]. In day-to-day life passwords are widely used for –

a) Authentication (A process to establish that the user are indeed who they say they are).

b) Authorization (The procedure used to determine if the authenticated person has access to specific information or functions).

Mostly people select passwords that is predictable in nature. Users normally have the tendency to choose memorable password, sadly it means that the passwords follow expected motif that are easier for raider to guess. While the motif problem can be resolved by not allowing user choice and accrediting system generated passwords to end users, this normally drives to usability issues since users are unable to remember and recall such randomly generated passwords. It is assumed that the human brain is exceptional at recognizing and recalling pictures than text. Graphical passwords exploit this basic human characteristic [1].

Alphanumeric passwords were first introduced to the world in the late 1960s.Today computer systems and all net-based projects use this technique to authenticate and authorize their users. Sadly, these passwords are broken ruthlessly by intruders by simple means [6]. Dictionary attack is the common method used by hackers to crack the alphanumeric password, such attack is very efficient mechanism because it only needs a little time to discover the user's password. The main problem/issue with the traditional alphanumeric passwords is that once a password has been selected the user must be able to evoke it to log into a particular system. If the password is not frequently used it will be even more prone to forgetting. Usually people choose understandable passwords that are guessed easily, for example, names of their family and office members, place of birth, date of birth etc. [15]. As studied by Gilhooly, the good and hard to guess or break passwords basically are difficult to memorize. Graphical password techniques have been proposed as a substitute to alphanumeric based techniques. It has been proposed to overcome the known weakness of traditional alphanumeric password. It is also designed to make the passwords more significant, easier for crowd to use and therefore more protected [14]. Based on the two assumptions; first, human beings can remember and recollect pictures better than alphanumeric characters and second, an image worth a thousand passwords; graphical password prove to be a better alternative to alphanumeric passwords [6].

The rest of the paper is systematized as follows: Section 2 describes the literature survey of this work. Section 3 describes proposed method for solving shoulder surfing problem in more detail. Section 4 gives an insight of the experimental results. We conclude the paper in section 5 and list out Future scope in section 6.

2. LITERATURE SURVEY
Present authentication methods can be bifurcated into three main regions:

1. Token based authentication

2. Biometric based authentication

3. Knowledge based authentication

Token based techniques, such as ATM cards and smart cards are used all over the world from the late 1980s [4]. Countless

token based authentication systems also include knowledge based techniques to enhance security. For example, ATM cards are used along with a Personal Identification number. The major flaw of this approach is that such systems can be overpriced, and the recognition procedure might be sluggish and unreliable, however, they provide the topmost level of protection. Biometric based authentication checks on the unique biological characteristics of individuals to verify identity for guarded access to systems. Knowledge based techniques are the most widely used authentication technique and include both text based and image-based passwords. The image based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques which will be studied in detail in the next sections [2].

2.1 Recognition Based Techniques

Sobrado and Birget designed and developed graphical password technique that tackled to some extent with the shoulder surfing problem. In this scheme, the system will show a number of pass-objects (pre-selected by user) among many other objects. To gain access in to the system, an end user needs to identify passobjects and click inside the convex hull formed by all the pass-objects. In order to make the password difficult to predict, Sobrado and Birget suggested using 1000 objects, which makes the display very congested and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space[2].

Fig 1 Sobrado and Birget graphical password scheme [2]

Brostoff and sasse carried out a study of pass faces, which illustrates well how a graphical password recognition system typically operates [8]. A user clicks on several previously chosen locations in a single image to log in. As implemented by Pass logix Corporation, the end user chooses various predefined regions in an image as his or her password. To log in the end user has to click on the identical regions in effect, cued click points (ccp) is a proposed alternative to pass points. In cued click points, users click one point on each of 5 images rather than on five points on one image [13].

Fig 2 Passface method [2]

2.2. Recall Based Authentication

In this method, a user is asked to emulate something that he or she created or selected earlier during registration phase. This method can also be referred as Click Based Graphical Password technique. These are classified into two types:-

2.2.1 Pure Recall Based Technique

In this method/technique, a user needs to reproduce their passwords without being given any kind of reminder, hints or gesture. Although this category is easy and convenient but it seems that users hardly can remember their passwords. Draw A Secret as shown if Figure 3 is one of the scheme which falls under this category [6].

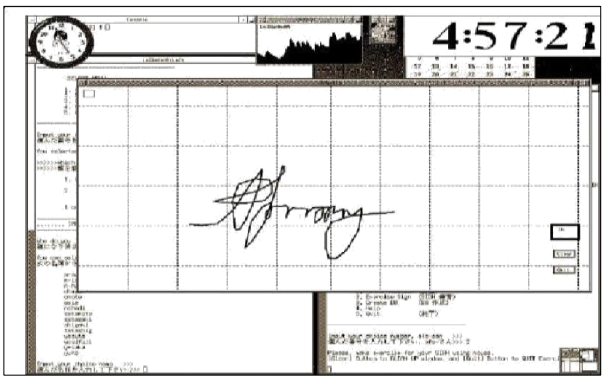

Fig 3 Draw a Secret method [2]

2.2.2 Cued Recall Based Technique

The two main categories are explained as follows:

2.2.2.1 Pass Point (PP)

This is click-based graphical password authentication where a user randomly clicks on five points on an image during the registration phase [12]. While logging in, the user has to click on the same exact points as selected during registration process [14].

Fig 4 Passpoint Method [2]

2.2.2.2 Cued Click Point (CCP)

In this method instead of selecting five points on an image, user selects one point per image for five images [13]. The user is shown only one image at a time; the image is replaced by the next image as soon as a user selects a click point as shown in Fig.5 [6].

Graphical passwords are not widely used in practice. However there are some advantages of graphical password as described below.

1) Dictionary Attacks

This is the major problem with the text based passwords. Graphical Passwords based on recognition involve the user toinput using mouse instead of keyboard; it is unrealistic to execute dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, a dictionary attack can be performed but an automated dictionary attack will be much more difficult than a text based dictionary attack [7].

2) Guessing

This is the serious problem usually associated with the text based passwords. Graphical Passwords are likely to predict. It is found that people often choose weak and predictable graphical passwords. Analogous predictability is generally observed among the graphical passwords created with the DAS technique [7].

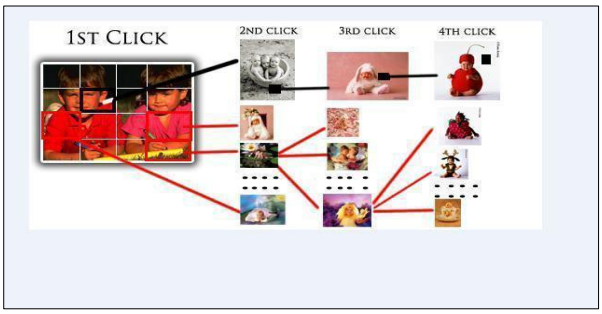

Fig 5 Cued Click Point Method [2]

3. PROPOSED SYSTEM

The proposed system is based on Cued click point as Users preferred CCP to PassPoints, saying that selecting and remembering only a single point per image was easier, and that seeing each image triggered their memory of where the corresponding point was located. It is also suggested that CCP provides greater security than PassPoints because the number of images increases the workload for attackers [9].The proposed system consists of two phase's viz.Registration Phase and Authentication phase. Let us see the two phases in detail.

3.1 Registration Phase

The first phase is Registration phase. During the first phase, the user has to first register his account by entering his personal details such as email id, First name, Last name and mobile number. Then if the Email id is not registered before, then only the user is asked to select three images of his choice. After selecting the three images the user has to click on a specific point in every image. After successfully clicking on those three points the registration phase is completed.

1) Algorithm: Registration

1) Enter Email id (Ur) (If exists Enter New Email id)
2) Now user enters the personal information such as First name and last name and Mobile Number
3) The user is requested to choose three images of his choice
4) User selects the images from the various categories of Images for cued recall based password.
5) User chooses a click point on these three images.
6) Registration complete.

3.2. Authentication Phase

During the second phase i.e. Authentication phase, the user has to give his Email id, after entering his Email id the user will be displayed the three images which he chose during the registration phase. If the user correctly chooses the click point's authentication is complete or else he is considered as imposter.

1) Algorithm: Authentication

a. Enter Email id (Used during the registration phase)
b. Three images will be displayed
c. User clicks on the click points which he chose during registration phase
d. If Successful then
e. e). Authentication is complete

The concept is quite well secure and advanced as compared to the current passface scheme, Sobrado and Birgit scheme, etc. This project will deal with using the property of cued click points. The click points of the user during the registration phase are saved as the password for the user. The user needs to provide three such passwords i.e. the user needs to submit three images during the registration phase and three click points for the respective images. The sequence of the images during the registration phase will be as it is provided in the login phase.

Since a single graphical image can contain thousands of pixels, clicking on the same pixel during the login process will be a tedious job and so will prove inconvenient for the users. Hence a small tolerance level around the pixel will be set up which will be clicked during the registration phase. The area of tolerance will be displayed by a red window but only during the registration phase(s). Following is the detailed structure of the loopholes found during implementation, of which solutions have been found.

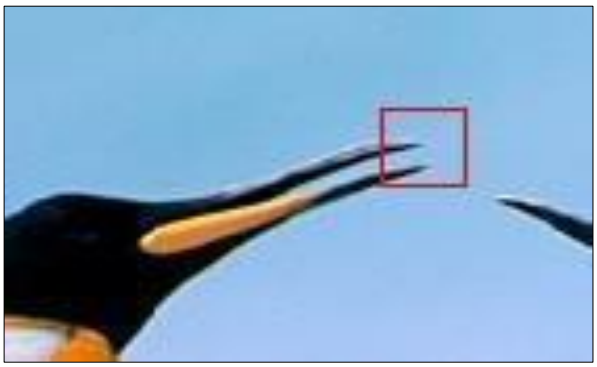

Fig 6 Tolerance value

1) SHOULDER SURFING: Shoulder surfing was the major drawback of the system. A camera recording a screen of a public computer will also record the CCP of a user which can be dangerous.

Solution: A fake cursor will be implemented in the system in order to confuse the masquerading person. During the authentication process the user will provided with two cursors, one will be original cursor which will be visible at a distance of only 60-70 centimetres and a fake cursor which will be visible from a quite long distance. The masquerade will consider the fake cursor as the correct one and will get a wrong password. As it can be seen from the figure 8 the screen has two cursors from which only one is the original cursor and the other one is the fake cursor and only the authorized user will know the difference. The cursor encircled in white border (cursor 1) is a fake cursor whereas the cursor encircled in black border (cursor 2) is the original one. Since in day to day life most of the system consider cursor 1 as the active cursor this will confuse the masquerader and hence the masquerader will be under wrong impression and will get incorrect result.

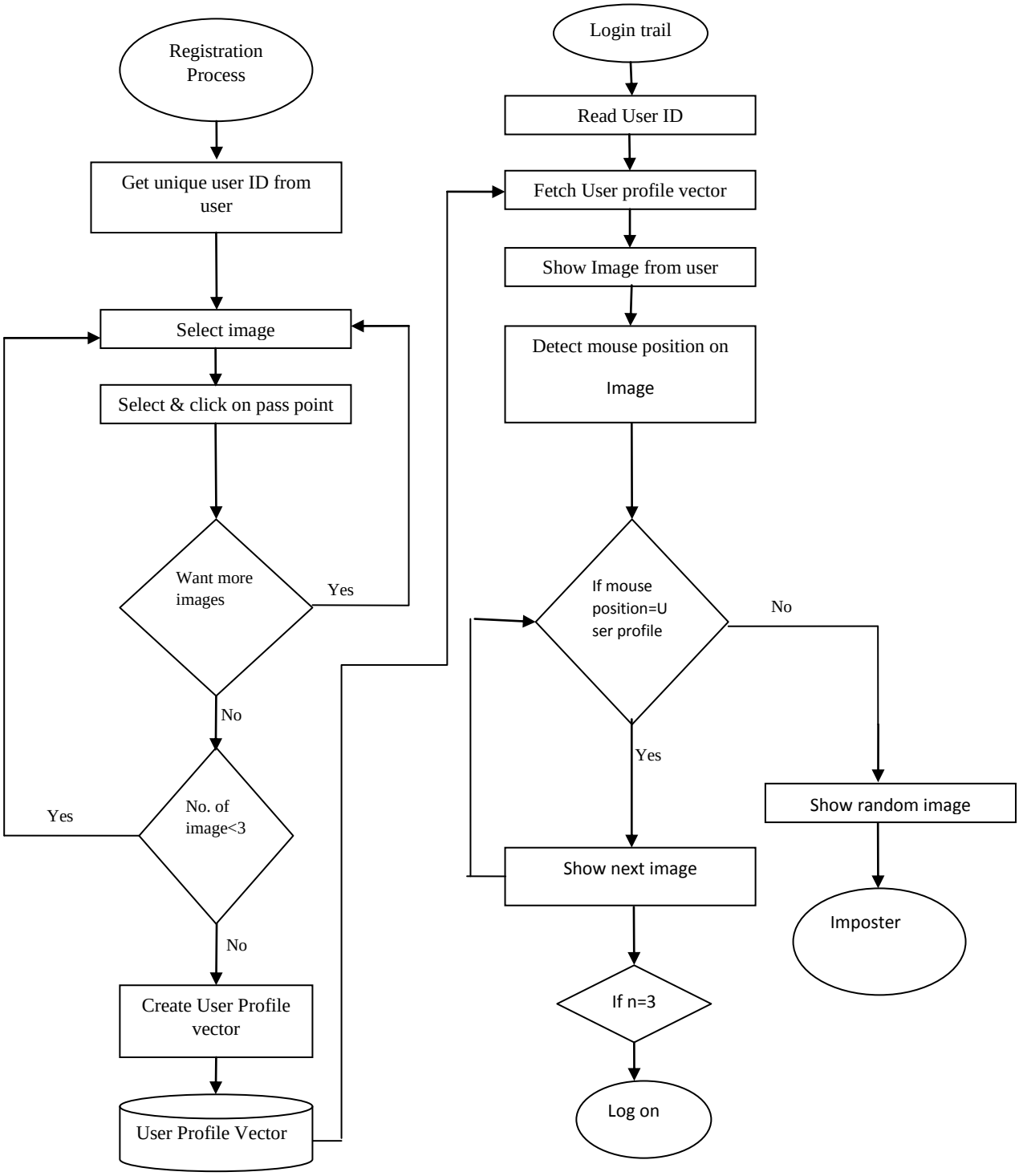

Fig.7 Flow Chart

2) FIXED DISTANCE: If the distance between the original cursor and the fake cursor is constant the masquerader can easily find out the correct password if he attempts for shoulder surfing.

Solution: The distance between the two cursors will be variable. After the specific time intervals the distance between the two cursors will change so that even if the masquerader attempts to login by taking the fake cursor at the same position where he saw it while shoulder surfing, he won't be able to successfully login as the location of the original cursor must have changed. The result is quite clear from figure 8 and figure 9, the distance between both the cursors have changed for the same image, this is achieved by using a Math.random function which randomly calculates the distance between the two cursors and hence the output is variable distance.

Fig 8 Fake cursor approach

Fig 9 Variable distance between two cursors

3) UNSUCCESSFUL LOGIN: To let the user know if the user has entered correct password or not was a big issue as it can be helpful for a valid user but at the same time could also get misused by a malicious user.

Solution: The user has to enter 3 passwords for three images. Based on the study of research papers the project will be designed with such a concept which has proved helpful and convenient for the valid user to get the location where he entered a wrong password whereas the malicious one would never be able to find it out. Here the concept of random images will be implemented. According to this concept, if the user clicks on a wrong password at any step in the login process, the user won't be restricted there to move forward, instead he would be allowed to continue with his login process but the next image after the wrong click would be a random image from the database. By seeing at the random image, the valid user will understand the step or image where he clicked wrong password and will correct it next time, whereas the masquerader won't be able to understand where exactly did the masquerader went wrong.

4) USE OF BACK BUTTON: As the proposed project will provide the user with a random image on wrong click, if suppose a malicious user knows the valid images and the sequence, the malicious user can easily trace the image where a wrong password was entered and by using back button the malicious user can try the same image n number of times.

Solution: In order to prevent the project from this type of attack, the back button will be disabled of the browser so that the masquerader won't be able to go back and re-enter the password on a wrong click.

5) URL REWRITTING: URL REWRITTING is another technique to crack the system without getting the user blocked. A malicious user may re-enter the URL of the previous page if the malicious user gets to know that the password entered was a wrong one.

Solution: In order to prevent the system from such an attack, the URL's will be hidden during the login phase. Due to this technique, the user won't be able to know the URL of the previous page.

6) BRUTE FORCE: Using a Brute force attack, a hacker may easily find out the combination of right passwords within a few minutes.

Solution: The user will be given only three chances to login and enter the password. If the user is unsuccessful in entering the password three times, his account will be blocked and an email, IP address of the machine from which the last attempt was done to login, the time, date, geo locations and a new password for login will be sent. The user can login into his account only by using the emailed password.

7) SMS ALERT: People generally do not check emails regularly, so in case if the account is compromised the authorized person will not be able to take action immediately

Solution: An SMS alert will be sent to all the telephone number the user will register during the registration phase, so as soon as the account is compromised, the user will receive an immediate SMS and after reading the message the user can take proper actions.

4. EXPERIMENTAL RESULTS

Cued Click points with fake cursor approach was tested with 34 participants. Participants ranged in age from 24 to 57. All participants were regular computer users who were comfortable with passwords and using a mouse. Participants were first introduced to the system and communicated that they would be creating graphical passwords. They were further instructed to pretend these passwords were safeguarding their bank information, and thus should select passwords that were memorable but difficult for others to guess. Along with the graphical password, participants were also told to select three alphanumeric passwords which were a combination of lowercase, uppercase numeric and special characters. All the participants were made to reproduce the graphical passwords and alphanumeric passwords in a week's time. Out of the 34 Participants only 67% people could remember their alphanumeric passwords on the other hand 82% people were able to login to the system using graphical password. In the next step of the experiment the same set of participants were asked to remember 3 points on a single image and 3 points on three different images. The participants were asked to recall the points, 74% people were able to remember 3 different points on a single image whereas 88% people correctly recalled 3 points they selected on 3 different images before a week time. In the last step of the experiment out of the 34 participants a user was randomly chosen and the other remaining participants were made to stand behind the randomly selected user at random distances. The main objective was to shoulder surf and obtain the user's co-ordinates to reproduce them, 94% people failed to reproduce the random user's click points thus giving the system a success rate of 94%.The experimental results can be seen in detail from the below tables.

Table 1.1 Comparison between alphanumeric password and Graphical password in terms of memorability

	Total No. of Participants	Passed	Failed	Success rate
Alphanumeric password	34	20	14	67%
Graphical Password	34	28	6	82%

Table 1.2 Comparison between Passpoint and cued click points

	Total No. of Participants	Passed	Failed	Success rate
PassPoint	34	25	9	74%
Cued Click Points	34	30	4	88%

Table 1.3 to check the resistance of the proposed system to shoulder surfing

	Total No. of Participants	Passed in reproducing User co-ordinates	Failed in reproducing User co-ordinates	Success Rate in not able to reproduce User co-ordinates
Resistance to Shoulder Surfing	34	2	32	94%

5. CONCLUSION

A novel approach which uses images and click points on images to authenticate the user is proposed. No previously developed system used this method, this system is helpful in providing a safe, secure and comfortable authentication systems to websites and web applications. The graphical password techniques evolved before do not provide a solution over shoulder surfing. This system uses a fake cursor technique to provide solution over shoulder surfing.

6. FUTURE SCOPE

The graphical password authentication system can be used as a safe and secure password authentication technique for web applications such as military website or banking systems etc. This system provides a solution over shoulder surfing and thus is a secure, quick and comfortable authentication system to provide secure authentication for websites in future. Following are the few examples where the proposed system can be used:

- Web log-in application.
- System login and logout process
- ATM machine.
- Folder locking.
- Mobile device.
- Hard disk locking

7. REFERENCES

[1] Saurabh Singh and Gaurav Agarwal, Integration of Sound Signature in Graphical Password Authentication System, International Journal of Computer Applications (0975 – 8887) Volume 12– No.9, January 2011.

[2] Dr.C.Kumar, Overcome Password Hacking through Graphical Password Authentication, International Journal on Engineering Technology and Sciences – IJETS™ ISSN (P): 2349-3968, ISSN (O): 2349-3976 Volume 2 Issue 2, February 2015.

[3] Vaibhav Moraskar et al. Cued Click Point Technique for Graphical Password Authentication, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 166-172.

[4] Devi Srinivas and M.L.Prasanthi, Implementation of Knowledge Based Authentication System Using Persuasive

Cued Click Points, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 12, Issue 2 (May. - Jun. 2013), PP 39-46.

[5] Smita Chaturvedi et al, Securing Image Password by using Persuasive Cued Click Points with AES Algorithm, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4), 2014, 5210-5215.

[6] Ankita R Karia et al, Image Based Authentication Using Persuasive Cued Click Points Int. Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 4, Issue 5(Version 6), May 2014, pp.179-185.

[7] Sunil et al, Cued Click Points: Graphical Password Authentication Technique for Security / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1073-1075.

[8] Anu Singh et al, Graphical Password Authentication System with Integrated Sound Signature, International Journal of Computational Engineering Research||Vol, 03||Issue, 4||, pg 230-234.

[9] Iranna A M, Graphical Password Authentication using Persuasive Cued Click Point, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013, ISSN (Print) : 2320 – 3765.

[10] Sonia Chiasson, P.C van Oorschot and Robert Biddle, "Graphical Password Authentication Using Cued Click Points," Springer-Verlag Berlin Heidelberg, LNCS 4734, p.359-374, 2007.

[11] Smita Chaturvedi et al, Securing Text & Image Password Using the Combinations of Persuasive Cued Click Points with Improved Advanced Encryption, Procedia Computer Science 45(2015) 418-427.

[12] Lavanya Reddy L, Enhanced Cued Click Point Method for Graphical Password Authentication, International Journal of Advanced Research in Computer Science and Software Engineering Volume 3 Issue 8 August 2013.

[13] Ms. Aarti Thakur et al, Integration of Sound Signature with Captcha as a Graphical Password , IJSRD - International Journal for Scientific Research & Development | Sp. Issue – Computer Networking | ISSN (online): 2321 – 0613.

[14] Roshni Rajavat et al, Textual and Graphical Password Authentication Scheme Resistant to Shoulder Surfing, International Journal of Computer Applications (0975 – 8887) Volume 114 – No. 19, March 2015.

[15] G. Agarwal et al, Security Analysis of Graphical Passwords over the Alphanumeric Passwords, International Journal of Pure and Applied Sciences and Technology.