Volume 6, Issue 6, June 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Web Security and Authentication with Graphical Password Using Cued Click Point Technique

Deepak Shrivastava[*], Vimal Shukla (Asst. Professor)
Cyber Security/Cyber Forensic, KNP College of Science & Technology, RGPV,
Bhopal, India

Abstract— ***Graphical password consists of some actions that the user performs on an image. A click-based graphical password scheme is a one type of graphical password technique. In click based approach, users click on image or a sequence of images to create passwords. Graphical methods have advantages over biometric and token based passwords. Being click points on images is shown and having to easy to remember, also since they are not typed they cannot be retrieved from key tabs or caches as in case of text passwords. The major problem of user registration, mostly text base password, is well known. If the login user be inclined to select simple passwords which are frequently in his mind it becomes straightforward for attackers to guess. If the password is machine generated it is mostly complicated for user to keep in mind. User authenticated password using cued click points graphical password scheme includes usability and security evaluations.***

Keywords— ***CCP, PCC,***

I. INTRODUCTION

Security has been an issue from the inception of computer systems. Secured systems must be usable to maintain proposed security. Password Authentication Systems have either been usable and insecure and not usable. Increasing either tends to complicate the other. Today, authentication is the principal method to guarantee information security and the most common and convenient method is password authentication .Traditional alphanumeric passwords are strings of letters and digits, which are easy and familiar to basically all users. Texts created passwords are nothing but string of characters. For text passwords, peoples always creates password which is easy to remember but these passwords are easy for attackers to break. Due to the inadequacy of human retention, most users incline to choose short or simple passwords which are easy to remember. In mainly cases, these passwords are easy to guess and vulnerable to dictionary attack. Users have many passwords for personal computers, social networks, E-mail, and more. They may decide to use one password for all systems to decrease the memory burden, which reduces security. Moreover, Text based passwords are vulnerable to shoulder surfing attack, spyware attack and social engineering attack etc. Biometric and tokens are used as an alternative to text based passwords but has its own drawbacks such as it requires extra hardware so these methods are costly. Like alphanumeric passwords, graphical passwords are knowledge-based authentication mechanisms. The main goal of graphical passwords is to use images or shapes to replace text, since numerous cognitive and psychological studies demonstrated that people perform far better when remembering pictures than words. Graphical passwords are an alternative to existing alphanumeric passwords. In graphical password, user clicks on images. Prior to the graphical passwords, the most common authentication technique used is a ‘Password’, which is an alphanumeric word known to the computer and the user. The most widely accepted theory explaining this difference is the dual-coding theory suggesting that verbal and non-verbal memory (i.e., word-based or image-based) are processed and represented differently in the mind. Images are mentally represented in way that retains the perceptual features being observed and are assigned perceived meaning based on what is being straight observed. Text is a form of knowledge depiction. Text is represented metaphorically, where symbols are given arbitrary meaning that describes the object represented by the text, as different to observed meaning. For example, `X' may represent the Roman numeral 10 or the multiplication symbol. The exact meaning is assigned based on some deeper conception. Furthermore, images may be determined double, perceptually and metaphorically, if meaning is allotted to the image. Graphical passwords are proposed to exploit on this human characteristic draw in that by reducing the memory burden on the user, more secure (e.g., longer or more complex) passwords can be produced and users will not resort to unsafe practices in order to cope. The results of a recent survey shows that 93% of large businesses in United Kingdom still use passwords to authenticate users. But users have many problems with the alphanumeric passwords like difficulty in remembering complex, pseudo-random passwords over time. Generally, a ‘good’ password has some characteristics like including numbers, alphabets (both capital and small) and special symbols, words not present in dictionary and not only that it must be long enough to stand against different attacks. As a general rule of thumb, a strong password should have no less than eight characters. Such pseudorandom passwords not have meaningful content and can be learned only by rote memorization, which is a pathetic to remember. Studies have shown that users tend to pick short passwords or passwords that are easy to remember, like alphabetic-only passwords consisting of personal names of family or friends, names of pets etc. Such passwords are easy to discover using dictionary attacks or attacks based on the knowledge of the user. According to Computerworld news article, a team of security engineers ran a password cracker in a network and within 30 seconds, they broken 80% of the passwords .Graphical passwords can be created during user register or after register, and be distorted any time after creation. Graphical password policies, which may be set by the site operator or the user, influence its presentation and defense. Example procedure attributes are:

a. Number of rounds of verification.
b. Display layout, e.g., 6×6.
c. Defining how images are presented to the user and the total number of images displayed in each round.
d. Number of images to be selected in each round.
e. Ordered or unordered image collection, defining whether order of image selection matters.

People often forget their passwords. If a password is not used frequently it will be even more susceptible to forgetting. If the password is hard to guess, it is hard to remember. Psychological theories have recognized decompose over time and interference with other information in long term recollection as necessary reasons for forget. Another complex issue is that users have many passwords for computers, network and e-mails. Detection a complex and long password is difficult. But Studies shows that human brain can better recall images than text.

II. METHOD

Project Design: - Given that text passwords are easy to deploy and to use. In this Proposed System, propose to hybrid text password, image password and video captcha. Proposed system is alternative to PassPoint, Persuasive Click Point scheme and Click Point. From literature review, in CCP, PassPoint and PCCP there were some limitations related to different issues viz. security and usability. Proposed system offers three-factor authentication to the user. User has to use text password, image click point and video frame text for authentication. In proposed method, multi-object images are provided to user .Our proposed system has provided images of size 400x300 pixels and tolerance square is 20x20 pixel size. Images has grid like structure to provide wide better password space. The basic use-case diagram is shown in Fig 2.

Use case Diagram: - Use-cases model the system from the end user's point of view. According to proposed system, use-case diagram provide a clear and definite description of how the end user and the system interact and to define the functional and operational requirements of the system (product). Modules of proposed system:-

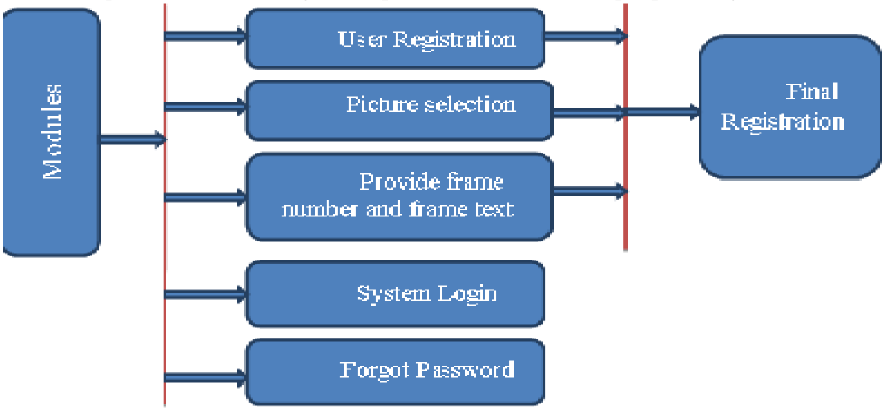

Fig1. Modules of Proposed System

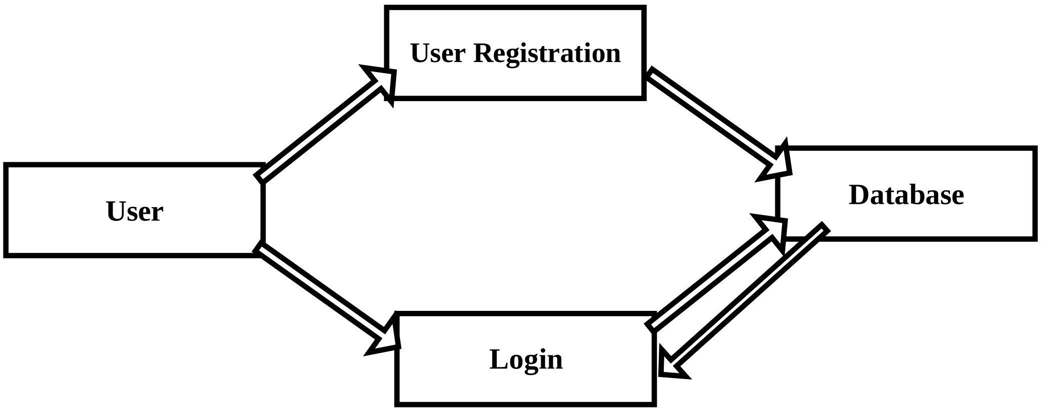

Fig 2. Basic Use-Case diagram

In this system, first module is user registration. User needs to register first with his /her basic information and create his/her user name and text password. After creating username and text password, then user asked to click point on images to store image password. User has given of freedom of choosing more than one image for password. After creating the image password, user has to select particular frame number and the frame text which is observed in the frame and that text and frame number will assign to the particular user. And finally user registered with system by the above procedure.

Then user can move to the login process. Cued Click Points (CCP) is a proposed alternative to PassPoints. It can be viewed as a combination of PassPoints, Passfaces, and Story graphical method. A password consists of one click-point per image for a sequence of images. The next image has shown which is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. The prototype system did not hash the passwords or use a discretization method as would a actual system, but actually stored the particular pixel coordinates so that the users choice of click-points and their accuracy on re-entry could be examined. The system also implemented an improvised image selection process to reduce the size of the required image set since with several unique trials per participant, we would have needed several thousand images to implement this technique. The first time a user clicked on a point, a new image was associated through that point. If a user clicked within the imaginary boundary of that point again, either to re-entering or to reset a password, the same image was shown.

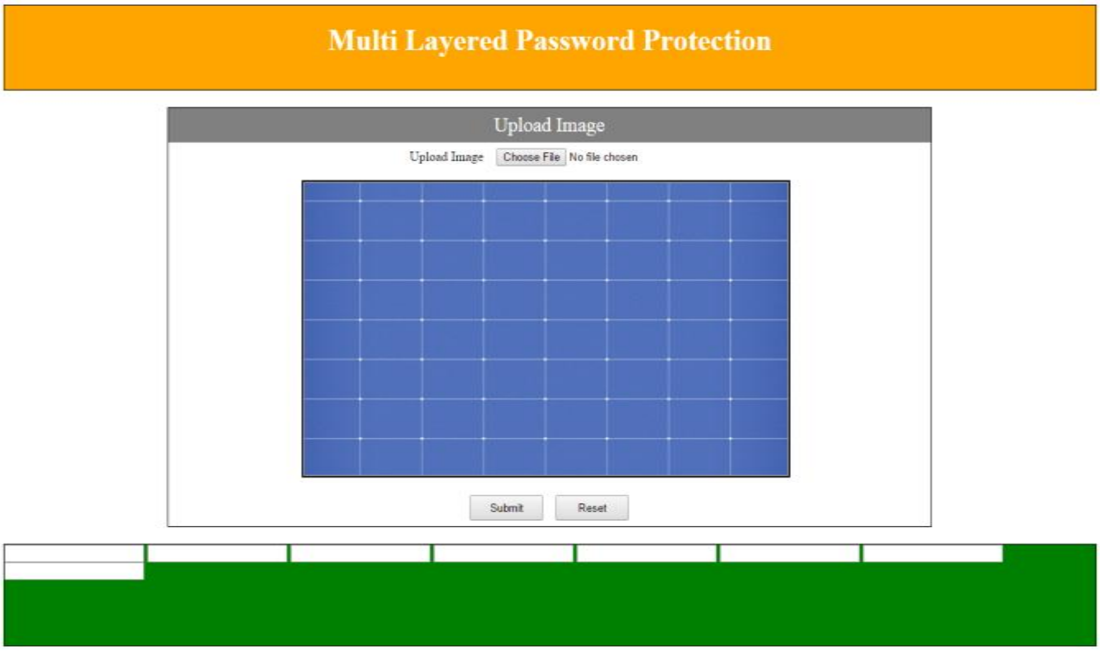

Fig. 3: Main User Interface

Registration form: - As shown in Fig.4It is basically a registration form provided to user. User will register her/his basic information with creation of alphanumeric or text password. Next for more enhancement of this method, security questions have been provided to user. Security question id user defined means user can create his own question which he likes. After given basic information, the user will move towards image password creation form for creation of image based password. In case of image based password, images are provided to user. Images contain a number of object images which are provided here for password creation. User has to create image password using click point on images. User can choose multiple images to create his/her image password. Images password is store in form of pixel form as row and column values.

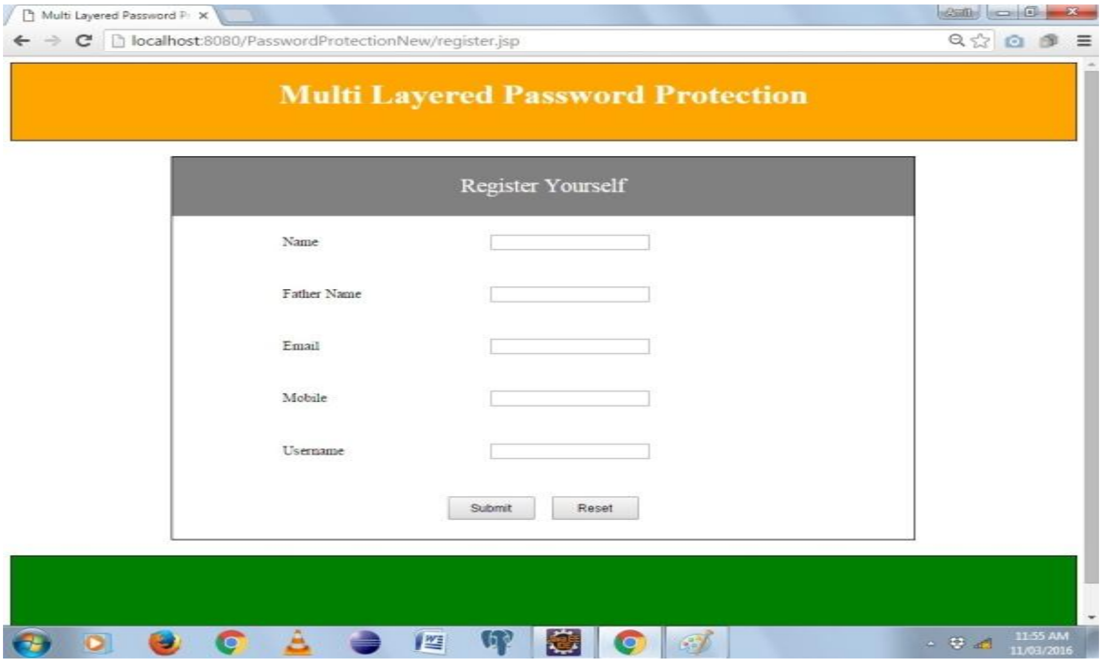

Fig. 4. User Registration

After create text password and user name, for creating image password, user has provided images with grid like structure .Framework like structure make easier to select their click point on given images. User has to select click points given area with grid like structure as shown in Fig. 5. After generating the click points user interface will show the message such that pattern saved with 3 points as shown in fig.6

Once generated the click points as per the user requirement user can another image for click points as a password. After that user come to third or final phase of registration process in which user has to select a particular frame number and frame text as a password as shown in fig.6 and all the information are stored in the database.

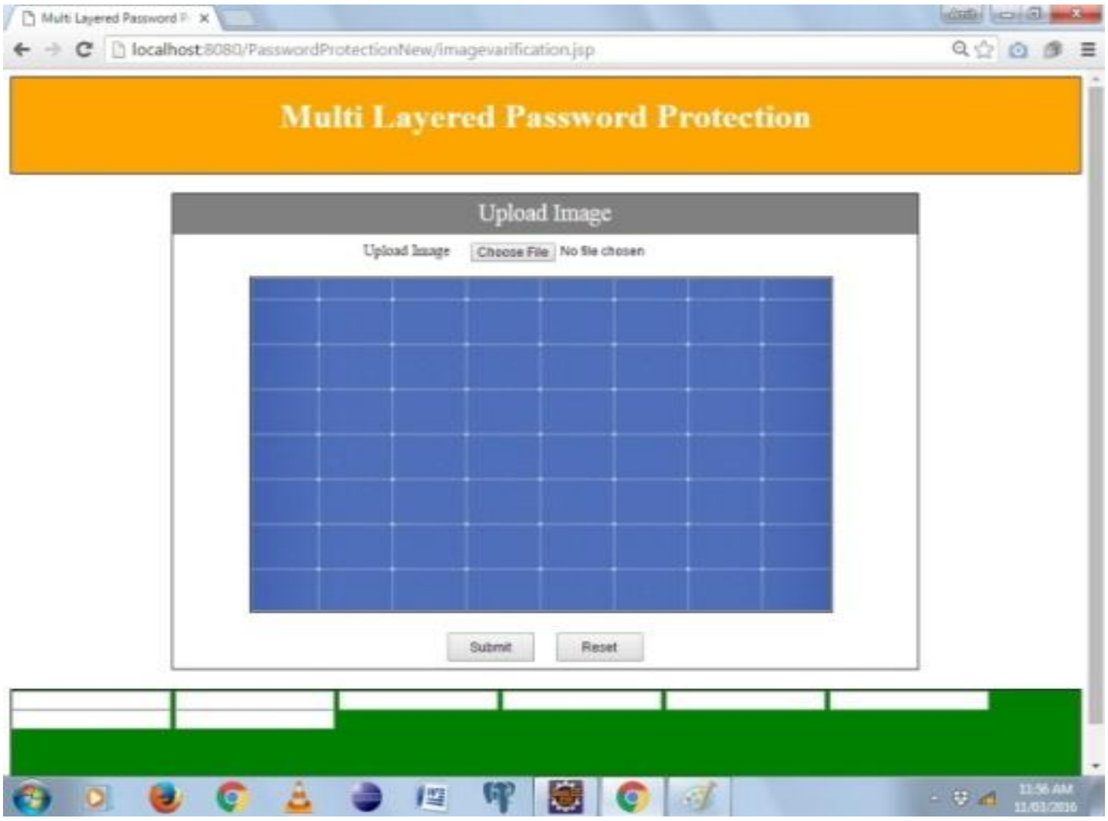
Multi Layered Password Pr ×
localhost:8080/PasswordProtectionNew/imagevarification.jsp
Multi Layered Password Protection
Upload Image
Upload Image
Choose File
No file chosen
Submit
Reset
11:56 AM
11/03/2016

Fig. 5 Second phase of User Registration

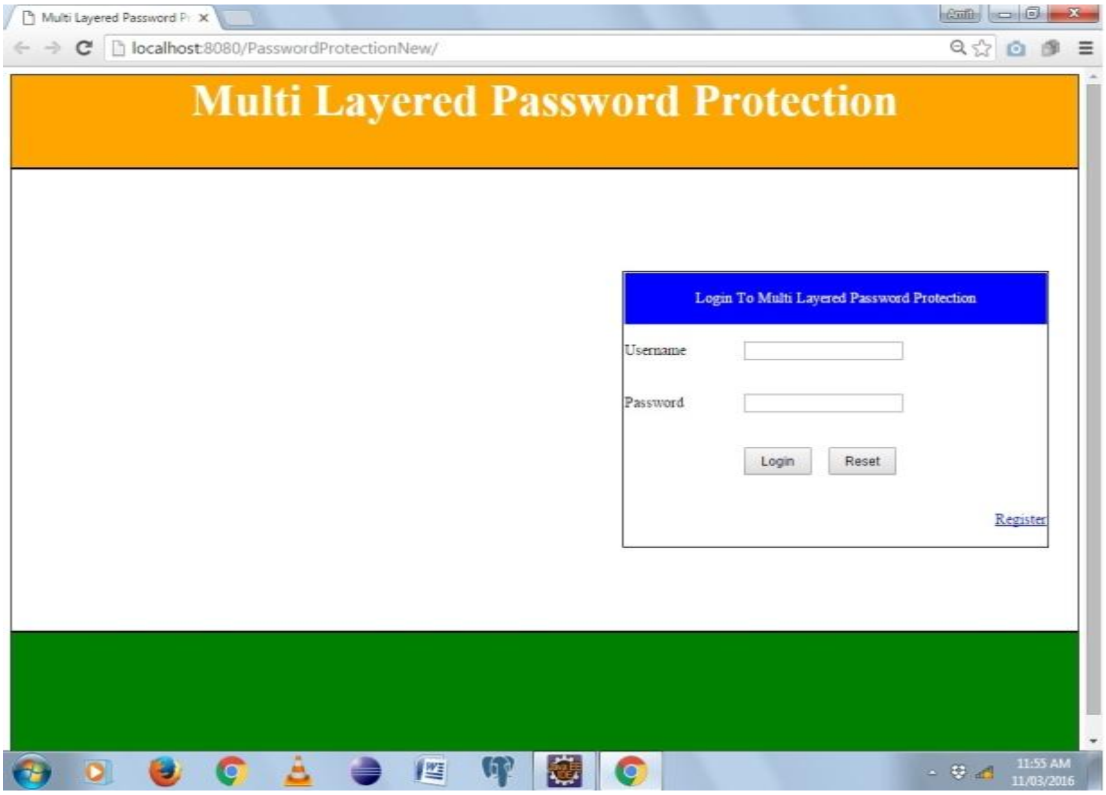
Multi Layered Password Pr ×
localhost:8080/PasswordProtectionNew/
Multi Layered Password Protection
Login To Multi Layered Password Protection
Username
Password
Login
Reset
Register
11:55 AM
11/03/2016

Fig. 6 second phase of user Registration

III. CONCLUSION AND FUTURE WORK

3.1 Conclusion

The proposed 3-factor proposed method scheme shows secure as a usable and memorable certification method. By delightful benefit of clients capability to recognize images and the memory trigger associated with text password. The proposed method has advantages over PassPoints, Cued Click Point, and Persuasive Cued Click Point in terms of usability and also security. Being click point as on images shown and having to remember click-point on given image appears easier than having to remember an ordered series of clicks.

3.2 Future work

In future development, proposed authentication techniques based on text and images will propose for online applications. These techniques will generate session passwords and are resistant to different attacks. However this schemes completely new to the users.

REFERENCES

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu- Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems- IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6,pp-891-904, JUNE 2014.

[2] SmitaChaturvedi, Rekha Sharma-Securing Image Password by using Persuasive Cued Click Points with AES Algorithm- International Journal of Computer Science and Information Technologies, Vol. 5 (4) ,pp-5210-5215, 2014.

[3] Md. Asraful Haque, Babbar Imam- A New Graphical Password: Combination of Recall & Recognition Based Approach- World Academy of Science, Engineering and Technology International Journal of Computer, Control, Quantum and Information Engineering Vol:8, No:2, pp-310-315,2014

[4] Ms. Shilpa Veerasekaran , Prof. Alka Khade , Prof. V.B Gaikwad-Using Persuasive Technology in Click Based Graphical Passwords-International Journal of Emerging Trends & Technology in Computer Science -Volume 3, Issue 2,pp-32-36, March – April 2014.

[5] A.Abuthaheer, N.S.Jeya Karthikka, T.M.Thiyagu- Cued Click Points Graphical Images and Text Password along with Pixel based OTP Authentication-International Journal of Computer Applications (0975 – 8887) Volume 87 ,pp-45-48, February 2014.

[6] V.Prasath, R.Buvanesvari, P.Nithin, S.Banu, K.Rajeswari -Graphical Password Authentication Using Persuasive Cued Click-Points Mechanism- International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-6,pp-142-145, January 2014

[7] Vaibhav Moraskar, Sagar Jaikalyani- Cued Click Point Technique for Graphical Password Authentication-International Journal of Computer Science And mobile Computing-Vol. 3, Issue. 1, pp-166-172, January 2014.

[8] Lavanya Reddy L,K.Alluraiah-Enhanced Cued Click Point Method for Graphical Password Authentication-international journal of advanced research in computer science and software engineering- Volume 3, Issue 8,pp-321-326, August 2013.

[9] Haichang Gao, Wei Jia, Fei Ye and Licheng Ma-A Survey on the Use of Graphical Passwords in Security-JOURNAL OF SOFTWARE,-VOL. 8, pp-1678-1698, JULY 2013.

[10] Binitha .V.M,Persuasive cued click based graphical password with scrambling for knowledge based authentication technique with image scrambling,IOSR journal of computer engineering,vol.13,issue 2,pp.14-24,July-Aug 2013

[11] Iranna A M1,Pankaja Patil2; Graphical Password Authentication using Persuasive Cued Click Point;International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, pp-2963-29,July 2013.

[12] Ms. Shilpa. L. Dhapade-Implementation of Persuasive Cued Click-Points Techniques for Folder Security-International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 6, pp-2005-2012,June – 2013.

[13] Devi Srinivas1, M.L.Prasanthi- Implementation of Knowledge Based Authentication System Using Persuasive Cued Click Points- IOSR Journal of Computer Engineering (IOSR-JCE)- Volume 12, Issue 2, PP 39-46,may-june. 2013.

[14] Priti Jadhao, Lalit Dole- Survey on Authentication Password Techniques, (IJSCE) International Journal of Soft Computing and Engineering, Volume-3, Issue-2, pp.67-68, May 2013.

[15] P. R. Devale Shrikala M. Deshmukh, Anil B. Pawar- Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme , (IJSCE) International Journal of Soft Computing and Engineering , Volume-3, Issue-2, pp.280-283,May 2013.

[16] P. R. Devale Shrikala M. Deshmukh, Anil B. Pawar- Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme-International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2,pp-280-283, May 2013.

[17] Alankrita Ladage, Swapnil Gaikwad Prof. A. B.Chougule-Graphical Based Password Authentication,(IJERT) International Journal of Engineering Research & Technology, Vol. 2 Issue 4, pp.626-630,April – 2013.

[18] Harsh Kumar Sarohi1, FarhatUllah Khan-Graphical Password Authentication Schemes: Current Status and Key Issues, (IJCSI) International Journal of Computer Science Issues, Vol. _10, Issue_ 2,pp-437-443, March 2013

[19] K. Semmangaiselvi, T.Vamsidhar ,KothaHariChandana, B. Krishna Priya and E. Nalina-An Effective Secure Environment Using Graphical Password Authentication Scheme-International Journal Of Engineering And Computer Science-Volume 2 Issue 2,pp-383-490, Feb 2013.

[20] Baljit Singh Saini, 2Anju Bala, A Review of Bot Protection using CAPTCHA for Web Security, IOSR Journal of Computer Engineering, Volume 8, Issue 6,PP 36-42,(Jan. - Feb. 2013).

[21] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. van Oorschot,- Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2,pp.222-235, MARCH/APRIL 2012.

[22] Priti C. Golhar, Dr. D.S. Adane- Graphical Knowledge Based Authentication Mechanism, International Journal Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp.48-54,October 2012.