Literature Review: Cued Click Point based Authentication

Suvarna Pansambal[1], Pranali Chaudhari[2], Kirti Khonde[3], Tanvee Mantri[4]
[1,2,3,4] Computer Engineering Department, Atharva College of Engineering,
University of Mumbai, Mumbai-400095, India.

***Abstract* - Knowledge-based authentication and text-based authentication system have some drawbacks which are renowned. Users mostly choose easy to remember passwords which are easy for hackers to guess, and password generated by system are difficult for users to remember. This paper focuses on the implementation of Cued Click Points graphical password authentication system, which includes usability and security. A main goal of authentication systems is to protect users by allowing selecting passwords which are better than other password schemes, thus expands the effectual password space. In click-based graphical passwords, poorly chosen passwords lead to the emergence of hotspots. We use persuasion to influence user choice to use click-based graphical passwords, encouraging users to select more random and difficult to guess, click-points.**

Keywords- Authentication, Graphical Password, Cued Click Point (CCP), Security.

I. INTRODUCTION

The traditional alphanumeric passwords used for authentication purpose have some drawbacks with respect to security and usability. The problem occurs due to passwords should have two fundamentally conflicting requirements; the passwords has to secure and easy to remember. To satisfy these requirements is virtually impossible for users [12]. For this purpose authentication schemes makes use of more secure password with least resistance path. Rather than burdening on users, it is easier to follow the system's suggestions for a secure password - a feature absent in most schemes. Research and experience shown that text based passwords are less human friendly. According to psychology studies human brain better at recognizes images than text [9]

We focus primarily on click based graphical authentication [10]. Cued Click Point [2] is a click based graphical image password technique which is successor of pass point technique [1]. CCP is nothing but clicking one image on each of the five images. It helps to enhance the graphical strength of the password. It offers excellent surroundings for suggesting strategies that help users to select better passwords since graphical password scheme produce more secure passwords and hence prevent users from resorting to unsafe practices in order to cope. Indeed, we also mention how our approach might be adapted to text-based passwords. Rather than five click points on single image, CCP uses single click point in each of the images coming up in a sequence of five images.

II. LITERATURE REVIEW

Suvarana Pansambal (Shirke) and et al [12], summarizes the concept of graphical password system. in each of the images coming up in a sequence of five images. In the next stage user select number of images and click points on images. In the registration user gets one system generated text password on his e-mail based on the RGB values of the selected click points of the image. While logging in user has to enter text password and this text password is highly secured on second level by this cued click point method.

Sruthi P V [8] had been done work on graphical password authentication. In registration phase user enters all details and selects point on images. The system will send a random dynamic string/word to the user by email. Then in the next page, an images set, each with different meaningful word will be displayed. Now, user will click on the image with the same string/ word that he received by email.

Tara H R and et al [10] primarily focus on click-based graphical passwords. During password creation, user has to select the images alongwith its click points. At the time of authentication, user has to select the correct click point on each of the images. During authentication, system decides the first image to be displayed. User has to enter click point on the image as images are displayed one after the other on the screen. Click point on each image decides the next image.

Ansari Ahmed and et al [9] designed click point based technique. During the registration phase user has to enter all details. Then user has select images on the client machine storage or at the server side. To protect the integrity of the system, they had introduced BOGUS-POINTS and password fields. When the user is asked to enter the points for authentication he may enter n number of points on the images, in any sequence. But during login process the user must enter the points in same sequence as clicked in the registration process.

Atish Nayak and Rajesh Bansode [11], targets on the integral evaluation of the Persuasive Cued Click Points graphical password system which includes usability and security evaluation on three different levels. This paper used persuasive to impact user choice is used in click-based graphical passwords for motivating users to select more random, and hence more difficult to guess, click-points. Nikhil Bomanwar and Neha Singh [7], this paper briefly describes the different Graphical Authentication Schemes. Pass points, passwords consist of a sequence of

five click points on a given image CCP consists of password creation, wherein the user has to select the images, sequence of the images and a click point for each image. This paper also brings to notice the Persuasive Technology which guides and encourages users to select robust passwords, but not force system generated passwords.

Uma D. Yadav and Prakash S. Mohod [6], focuses on adding more features in existing graphical password schemes. The improvements are brought about by adding the concept of modules wherein the first module deals with setting the seed value or unique and the latter deals with offering tolerance. In short this paper comprises the improvements in the existing system.

III. METHODOLOGY

Authentication starts with registration process, which includes both registration phase and picture selection phase. After this next phase is login process in which user is authenticated. The proposed system reduces the brute force attack as well as allows the user to select more difficult password to guess.

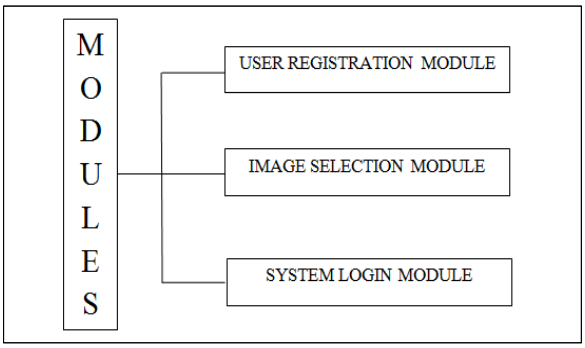

Fig.1 System Module

The modules are as follows:

A. Registration Phase

In registration process, the user will require to fill all the fields such as name, user id, email id, phone number etc. Then in the next page, user should choose the category of images and tolerance level as hard, medium, easy. User can upload own images stored on his/her machine. Then a set of images in the specified category will be displayed. User must select five images from that collection. The selected image will be displayed with a descretization grid overlaid on it. User has to select click point. User repeats this process for selected five images. This process is called as CCP Creation. Then the selected click point's x and y co- ordinates values are encrypted using AES algorithm and alphanumeric value is generated using Random Value Generator. This value is send to user by email which has to enter during login phase. After done with all these above procedure, user profile vector will be created. This user profile vector stored the user details, user selected images, encrypted x, y coordinates for each image, one alphanumeric value. This user profile vector is use for authentication by system.

B. Login Phase

In login phase, user first enters the unique user ID as same as entered during registration and alphanumeric value which is generated by system and mailed to the user. System will fetch the stored user profile vector. Then the system will display the preselected sequence of images on the screen, without shading or the viewport. User clicks the points on the images that he previously selected in the registration phase. All this details stored in the temporary vector called login vector. System compares the login vector and previously defined user profile vector. If all the click points are correct, the login will be successful. User has three failed attempts, after that login session will be expired.

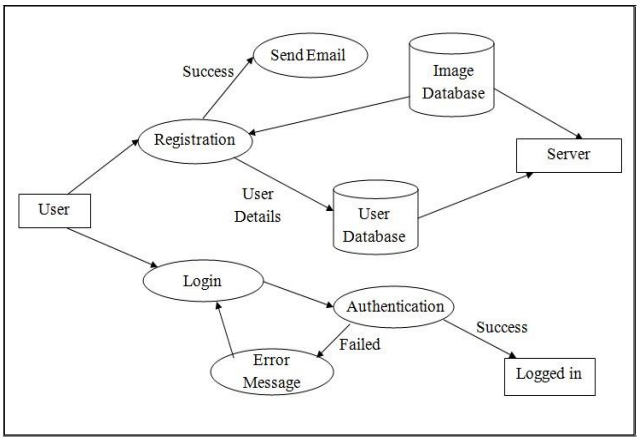

Fig.2 Block Diagram

IV. DISCUSSION

The system will be working in two phases: Registration and login phase. The distinctive feature of registration is the randomization of viewport so as to avoid selection of known hotspots and the descretization grid which helps the user select the click point. The user is also given a facility to shuffle the viewport. AES algorithm encrypts the co-ordinates of these click points and Random Value Generator generates an alphanumeric value. During login phase the user gets three attempts to select the appropriate click point failing which the session terminates.

The noticeable advantage will be that the lower tolerance value will lead to increased login security rates. This system will not face any limitations as those occurring in other authentication schemes like machinery requirement for biometrics thus leading to higher cost. Also hacking will become a difficult task as the proposed system makes Brute Force attack infeasible. Owing to the advantages mentioned above the few disadvantages like time consuming registration process and increased graphical password storage are negligible.

V. CONCLUSION

The proposed system aims at providing less predictable passwords to users as it targets on the major advantage of human psychology of remembering graphics

rather than text. Also it discourages the selection of known hotspots. Thus the effectual password space is increased. This system looks forward to providing a convenient user interface to the users thus providing flexible utility. The discretization grid adds to the higher security than that provided by other expensive authentication system (e.g. biometrics) hence reducing the effectual cost.

CCP offers a highly secure alternative to existing systems. CCP increases workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images.

VI. FUTURE SCOPE

In future development we can also add challenges response interaction. In challenges response interaction, server will present a challenge to the client and the client need to give response according to the condition. If the response is correct then access to the user is granted. Also we can give time limit to the user for selecting the points. We can increase the security of this system by increasing the security levels, the number of tolerance squares and images used.

REFERENCES

[1] S. Chiasson, A. Forget, O. Biddle, P.C. van Oorschot "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," published in IEEE transactions on dependable and secure computing, vol. 9, no. 2, pp.222- 235, Apr. 2012.

[2] Vaibhav Moraskar, Sagar Jaikalyani, Mujib Saiyyed, Jaykumar Gurnani, Kalyani Pendke, "Cued Click Point techniques for graphical password authentication,"International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1,

[3] Ian Jermyn, Alain Mayer, Fabin Monrose, Michael K. Reither, Aviel D. Rubin "The design and analysis of graphical passwords", Proceeding of the 8th UNISEX Security Symposium, 1999.

[4] Suo, Ying Zhu, G. Scott, Owen Xiaoyuan, "Graphical passwords: a survey", (Department of Computer Scince Georgia State University).

[5] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "Pass Points: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, 2007.

[6] U. D. Yadav, P. S. Mohod "Adding Persuasive features in Graphical Password to increase the capacity of KBAM," Published in IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, vol.2, Mar.2013, pp.513-517.

[7] Neha Singh, Nikhil Bomanwar "Improves Authentication Scheme Using Password Enables Persuasive Cued Click Points", Published in IEEE International Conference on Green Computing and Internet of Things (ICGCIoT),, vol. 00, Oct 2015, pp. 1394-1398,2015,

[8] Sruthi P V, "CRASH-Cued Recall Authentication Resistance to Shoulder Surfing attack", Published in IEEE International Conference on Green Engineering and Technologies(IC-GET 2015), Nov 2015

[9] Ansari Sana Nafees Ahmed, Shaikh Mohammed Sadique " Cued Click As An Authentication Mechanism For An Application", International Journal of Engineering research and Technology,vol.3, Mar 2014.

[10] Tara H R, Usha T Published in International Journal of Engineering Research & Technology (IJERT) ISSN: 2278- 0181 Vol. 2 Issue 6, June – 2013.0

[11] Aatish Nayak, Rajesh Bansode "Analysis Of Knowledge Based Authentication System Using Persuasive Cued Cllick Points" Published by Elsevier B.V, Mar 2016.

[12] Suvarna Pansambal (Shirke) and et al "Enhancement of Password Authentication System Using Graphical Images" Published in International Conference on Information Processing (ICIP), Dec 2015.