ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.7

Cued Click Points Graphical Images with Binary Based OTP Authentication

Shruti Nathuram Mane[1], Dr. A. W. Kiwelekar[2]
M. Tech Student[1], HOD & Associate Professor[2]
Department of Computer Engineering
Dr. Babasaheb Ambedkar Technological University, Maharashtra, India

Abstract:
In Cued Click Points Graphical Images with binary based OTP Authentication, user clicks on sequence of five images. At the time of login phase images appear as per the random sequence. In the registration phase, user selects 5 images from the image pool or local drives. Based on the image selection server generate the signature during registration. While users coming to login phase, they enter username and then binary OTP number is send to user mobile or email id. If binary number is 1 user have to select correct position on the image and if binary number is 0 then they have to click on wrong position. Otherwise the user is aborted. Signature values of all five clickable images will be used for calculating binary OTP. This proposed system provides two-way authentication and also provides higher security than other techniques.

Keywords: Authentication, Cued Click-Points (CCP), Graphical password, Hotspot, OTP, Persuasive Cued Click-Points (PCCP), Viewport.

I. INTRODUCTION

Password can be of any type but most probably there are text based password. Text password are the one which are commonly used, it is a string of alphanumeric characters. Text passwords are easy to remember by users but it is also easy to hack by software hackers. For more security, users use strong systems assign passwords which are difficult for users to remember. Biometric and token are used as alternative to text passwords but, it has its own drawbacks as it will require extra system to work. Graphical passwords are of three types: Click based graphical password, Choice based graphical password and Draw based graphical password. In proposed work for registration of new user, user can select three or five number of images from file log and select different location on the image. The viewport selected by a user is saved in database server and the sequence of viewport is set as password of that particular registered user. When user wants to access account, they should enter username then the system will send binary number to user mobile or mail-id. When the binary number is 0 user need to select wrong position and when the number is 1 user need to select correct position of the image. On the bases of binary number password will be verified. If user failed to select the exact wrong or right specified location on image, they would not able to access the account.

II. RELATED WORK

Cued-Click point is a leading technology for creating graphical passwords. Previously there are various papers on the topic of graphical password; we are now going to discuss various techniques of these papers. S.Wiedenbeck and J.Waters (2005) had proposed pass points with little flexibility as the allowed to choose the images by user for creating graphical passwords. In Pass-point technique user choose an image and click on different location of image to set password. While login user should remember the location of clicks and click correctly on the image [1]. S. Chiasson (2007) came across with Cued Click Point (CCP) technique. Authors took advantage of user's ability of recognizing images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. Being cued as each image is shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image [2]. Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle and P. C. van Oorschot (2011). Persuasive Cued Click Points (PCCP) technique is presented by this paper in which password creation phase consist of visible hotspots and shuffle button, but in login phase it is invisible. PCCP reduce the problem of HOTSPOT and image pattern creation [3].A.Abuthaheer, N.S.Jeya Karthikka and T.M.Thiyagu (2014) they used to create CCP technique along with OTP authentication. In this paper after password login successfully, OTP verification is the next level security. This technique provides two way authentications [4]. Atish Nayak and Rajesh Bansode (2016) have paper on PCCP with advance technique. This paper compares registration profile vector with login profile vector to authenticate the user while login. If the user registration and login vector does not match then the server block the IP address of the computer for one day [5]. Ankit Aggarwal, Darshil Doshi, Vijay Gore and Jignesh Sisodia (2015) here three way authentication is described; first is text based password , second is PCCP graphical image password and the third is OTP authentication [6]. Shrikala, M. Deshmukh and P. R. Devale in this paper features of D´ej`a Vu, Cued Click Points, Secret Drawing and Text passwords are combined for secure authentication. In D´ej`a Vu system sequence of images are identified from database, if the user click is incorrect message of

authentication failure is given after last click, next step is secret drawing and the last step is text password [7]. Lavanya Reddy L and K.Alluraiah they wrote paper on enhanced cued click points. In which there are various steps for graphical password authentication. First, Create Phase in which graphical password is created. Second, Confirm Phase in this phase graphical password is re-entered. The first image of password is allotted by the server. They also carried out trial test [8]. Prof. Anil Kulkarni and Sangameshwar (2013) these people work on Persuasive Cued Click- Points (PCCP) but the viewport is saved in database using color feature of image. The next image displayed is based on the color feature of clicked viewport [9]. Suresh Pagidala and C. Shoba Bindu (2013) they proposed Improved Persuasive Cued Click Point (IPCCP) technique. This paper consists of various phases for creating graphical password [10]. Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot and Robert Biddle (2009). This paper proposed multiple texts for creating password and the viewport is not visible for on any phases. If user fail to login correctly then the user again have to start from the create password [11].

III. BACKGROUND

There are several methods available to set graphical password which are important part of this paper. Text passwords are most popular for user authentication method, but have security and usability problems.

A. Pass-points

In previous papers graphical password authentication was done with the technique called pass-points. In this technique only single image is used and the image consist of various viewports, user have to select this click-points within the system tolerance square and have to remember the sequence of view-port for further login. The two drawback of this method is the view-port as user cannot remember the sequence of click-points and the second drawback is attackers can easily guess the password as user performs certain patterns in order to remember the secret code.

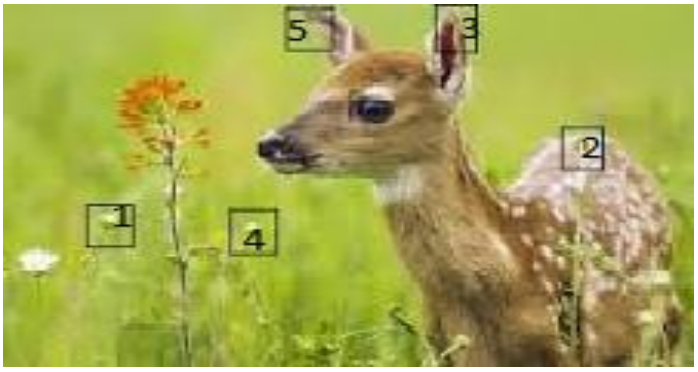

Figure.1. Pass-Point System

B. Cued Click Points (CCP)

Cued click points (CCP) technology was design to overcome the problems of design patterns and reduce hotspots of Pass-points which is previous technology. CCP uses one click on different images whereas five click on one single image in pass-points technology. The next image displayed is dependent on previously clicked Click-point image, the click-points displayed creates a path through an image set. The important feature of Cued Click Point is the authentication failure of unauthorized user is only provided after completing all the images Click-Points and not immediately after the wrong clicked image. But along with advantage CCP method also has drawbacks that it accepts wrong Click-points in the System and it also rejects the correct click-points after the wrong clicked images. This method solves the problem of design pattern recognition, but could not solve the problem of hotspot as users are selecting their own click-point.

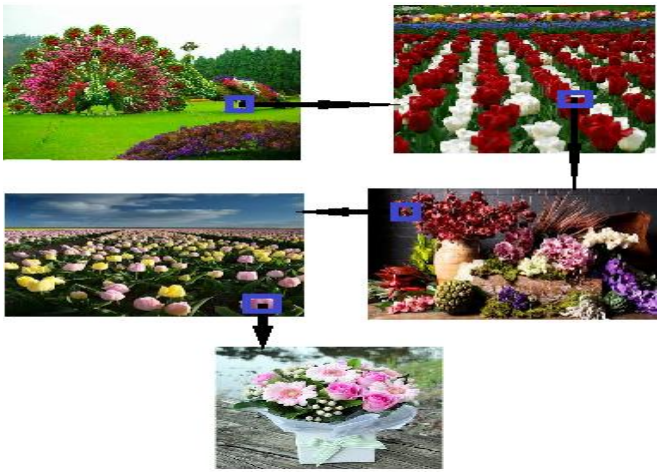

Figure .2. Cued Click Points System

C. Persuasive Cued Click-Points (PCCP)

Persuasive Cued Click-Points technique was invented to overcome the problem of lack of security in Cued Click-Points (CCP) technique. Attackers can easily find password of graphical image as users are most likely prone to select repeatedly specific viewports of image.

Viewports and pattern reduce the security of CCP technique; if users are allowed to select viewport as password on image it is possible that many users can select the same area of image and attackers can prioritize the probability password for more successful guessing attack. To overcome these problems PCCP is used, persuasive feature is added to the CCP and PCCP is generated.

While creating password images are slightly shaded to allow the visibility of hotspots. The viewport is positioned randomly to avoid the known position of hotspots as this will help attackers to improve guessing and also help to generate new position of hotspot. User must select the click-point within the highlighted viewport and must not click outside the viewport, when user wants to change the position of the viewport they need to press the shuffle button and select their own viewport position on respective image as password. At the time of password creation user may shuffle the viewport position as often as they require, but this leads to slowdown the password creation process.

During this password generation process only the viewport and shuffle button is displayed. After the completion of password generation process, the generated image password is saved in the server database and while login user have to select the exact

password position as images are displayed without viewport and shuffle button. PCCP is known for its best technology as it also has security problems; by using PCCP technology HOTSPOT problem is reduced. Hotspots and patterns reduce the security of click-based graphical passwords, as attackers can use skewed password distributions to predict and prioritize higher probability passwords for more successful guessing attacks. Research proved that various people are attracted towards same restricted area of image while password generation, this creates hotspot issue if users are allowed to select their own graphical password without guidance.

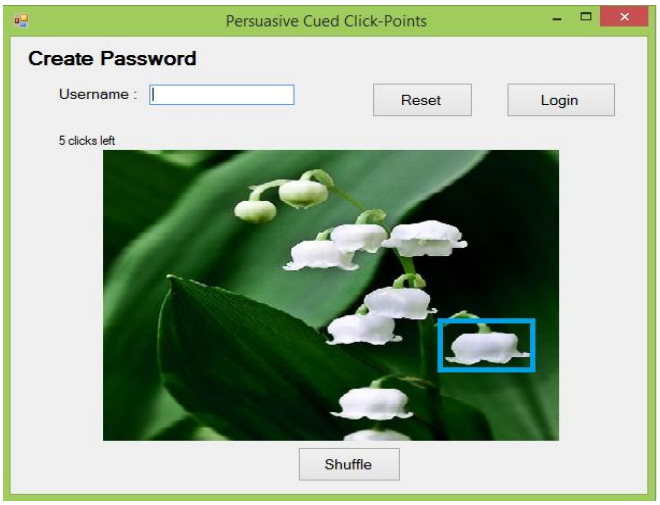

Figure.3. Persuasive Cued Click Points System

IV. SYSTEM ARCHITECHER

In Cued Click Points with binary based OTP authentication system, first registration is done by user. User selects images from their image pool and click on a particular location on image for creating passwords. User will have to click once on a single image.

The five clicked points of password are stored in the database and while login into the system after entering username the user will get a binary OTP number in the mobile or by email. In the sequence of binary number if bit is 1 user has to click the correct position on image and if the bit is 0 they have to click incorrect position on the image.

For e.g. 10100 is the OTP received by user, the first and third images should be correctly clicked on that particular registered location because the binary number is 1 for respective location and binary number 0 is there for second, fourth and fifth position hence user should click on the incorrect position for that sequence of image. If user fails to follow the instruction properly then they are aborted from the system.

Graphical password was first invented by Blonder. Graphical passwords are remembered easily then text based passwords and they are attractive by which they are not forgotten easily. As attackers are becoming clever, so there is a need to improve the security of system. By using Click based Graphical passwords hackers cannot guess the location of passwords from the image. With the help of this system it will be very difficult for attackers to guess the passwords.

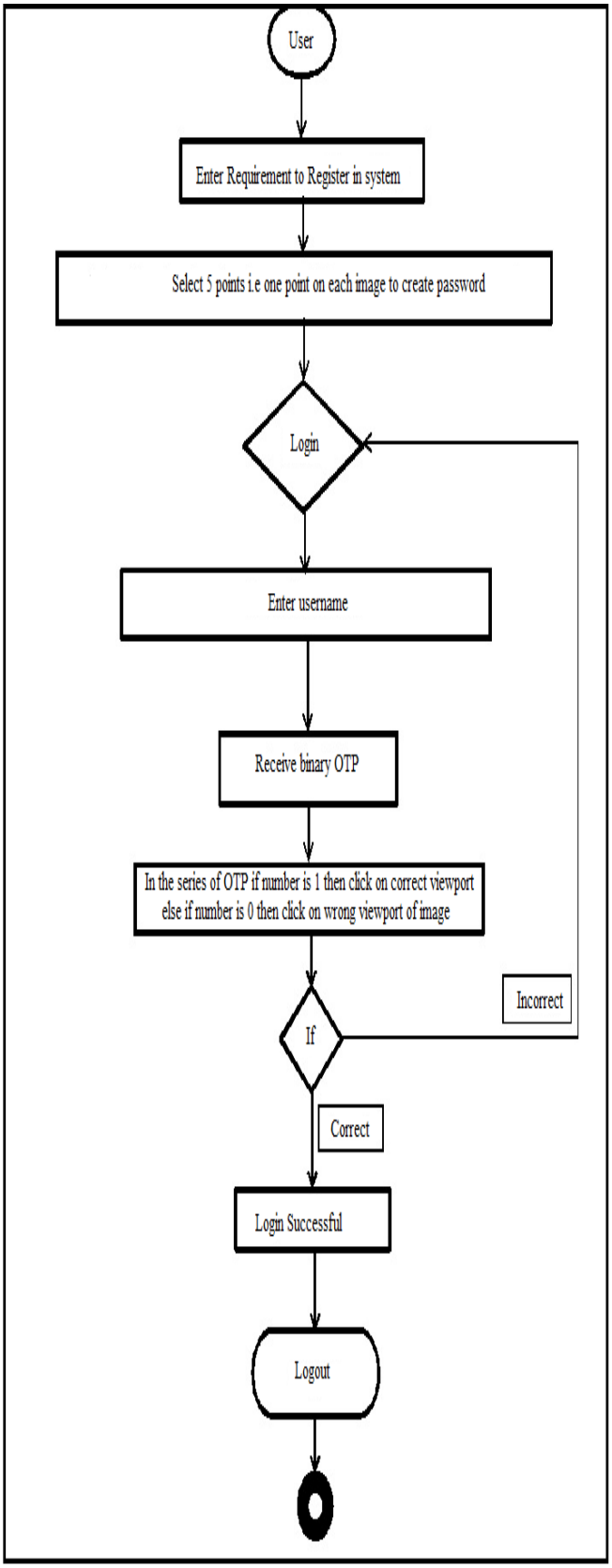

Figure. 4. Data Flow Diagram

V. CONCLUSION AND FUTURE SCOPE

In this paper we have shown our initial exploring experiments towards creating a Cued Click Point system with binary based OTP authentication. Click based graphical passwords are secure

and does not cost more as compare to token based passwords. This system will first register users with their username, password and IMEI number. Password creation will be based on Cued Click Point (CCP) system. User will have to browse the images from the image pool of their own database and click on the specific locations of the images. User will have to click once on a single image. The Click Passwords are stored in the server database and with this registration will get completed. In the login phase user will have to enter the username first and should click on the "Get OTP" button. Now the server will generate the binary OTP number for the user and will send to user's mobile or email. They should click on wrong location of image when binary OTP number is "0" and click on correct location when binary number is "1". This system will avoid Shoulder-Surfing, Guessing attack and Capture attack. The future scope of this paper will be creating a system with multi-level security, having greater security level.

VI. REFERENCES

[1]. S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005

[2]. 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

[3]. 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" Member, IEEE

[4]. A.Abuthaheer, N.S.Jeya Karthikka and T.M.Thiyagu "Cued Click Points Graphical Images and Text Password along with Pixel based OTP Authentication" International Journal of Computer Applications, February 2014

[5]. Atish Nayak and Rajesh Bansode "Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points", 7th International Conference on Communication, Computing and Virtualization 2016

[6]. Ankit Aggarwal, Darshil Doshi, Vijay Gore and Jignesh Sisodia, Three Level Security Using Cued Click Points in Image Based Authentication Information Technology Dept., Sardar Patel Institute of Technology, Andheri (W), Mumbai, India 2015.

[7] Shrikala M. Deshmukh and P. R. Devale, An efficient mechanism for secure Authentication" Research Scholar, College of Engineering, Bharati Vidyapeeth University, Pune, India

[8]. Lavanya Reddy L, K.Alluraiah, ECCP: Enhanced Cued Click Point Method for Graphical Password Authentication" Department of CSE Sri Venkateswara College of Engineering, India

[9]. Prof. Anil Kulkarni and Sangameshwar, "Design, Implementation and Evaluation of Knowledge-Based Authentication Mechanism Using Persuasive Cued Click-Points" Department of Computer Science and Engineering Department of Computer Science and Engineering Guru Nanak Dev Engineering College, India

[10]. Suresh Pagidala and C. Shoba Bindu M.Tech (CS) and Associate professor "Improved Persuasive Cued Click Points for Knowledge-Based Authentication", CSE Department, JNTUA, Anantapur (515002), Andhra Pradesh, India

[11]. Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, Robert Biddle "Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords" School of Computer Science, Department of Psychology Carleton University, Ottawa, Canada