AN EFFECTIVE AUTHENTICATION METHOD USING IMPROVED PERSUASIVE CUED CLICK POINTS

Dhanashree Kadu[1], Shanthi Therese[2], Anil Chaturvedi[3]

*[1]M.E. Computer Department, Shree L.R. Tiwari College of Engineering,
Mumbai University, MS, India
[2]Associate Professor, Thadomal Shahani College of Engineering,
Mumbai University, MS, India
[3]Assistant Professor, Shree L.R. Tiwari College of Engineering,
Mumbai University, MS, India*

---***---

ABSTRACT: *In today's digital environment security is very important. For that password protection is very much necessary. Various password protection techniques are available. For authentication text-based passwords are used commonly which is very much prone to attacks. so to overcome the disadvantage of text password, graphical passwords are used. Persuasive Cued Click Point is a click-based graphical password technique which is consist of numbers of images where users click on one point per image & generate one password. Graphical passwords are easy to memorize but difficult to crack by attackers. In this paper, we proposed a methodology of graphical password authentication system using Improved Persuasive Cued Click Points, including usability and security. Main goal of this system is to support the users in selecting better passwords, which will increases the security.*

Keywords—Cued Click Point (CCP); Graphical passwords; authentication; persuasive Cued Click Point.

1. INTRODUCTION

All our applications needed Strong authentication method. Text based password is a popular authentication method and they are very much prone to attacks. so to overcome the disadvantage of text password, graphical passwords are used. . Graphical authentication is best alternative solution to text-based authentication. Graphical passwords have two main issues as Shoulder surfing and hotspot, to reduce that we have proposed a graphical password authentication system which is best alternative for text password. In this paper we have proposed a graphical password authentication system which is best alternative for text password. The main objective of the project is to provide a two way authentication to the users by using Persuasive Cued Clicked point's technique and OTP.

2. OVERVIEW OF GRAPHICAL PASSWORD AUTHENTICATION SYSTEMS

Graphical password is an alternative to text based passwords in which users click on number of images to authenticate themselves rather than typing text as password [3]. Graphical passwords are more memorable compared to alphanumeric passwords, because it is easier to remember an image of flower than a set of alphabets and numbers.

Several psychological studies have recognized human brains have apparently superior memory to recognize, recall visual information like photos as opposed to verbal or text based information [4].One of the best password authentication systems was text based or alphanumerical based password has several problems. One of the main problem with text based password is it was ridicules to remember several text password for different account. Then introduction of biometric password [3] and token based password was considered as alternative of the text based password, but it again has several drawbacks like cost and unavailability issue. To overcome the disadvantages of text based password and token based password the invention of graphical password is introduced. Initially there were following graphical password authentication systems:

A. Pass point.
B. Cued Click Point (CCP).
C. Persuasive Cued Click Points (PCCP).

But this system had again disadvantage of hot spot problem and shoulder surfing attacks. To overcome the disadvantage of hot spot problem invention of Persuasive cued click point is made.

A. Pass Point: The pass point system for password authentication. Pass point was as simple as just clicking five point on single image and combination of this point as a password. In this user has to select five points from single image and at the time of password selecting and during the time of login user has to repeat the same sequence of the points from single image. But the main security problem with this was the HOTSPOT [1], the area where the user clicks. User choose the easy to memorable passwords to which can be easily guessed by hacker. To avoid this problem the next method is implemented.

B. Cued Click point: To overcome the disadvantage of the pass point authentication system the cued click point is invented. Cued click point [1][2] has the same concept as of the pass point but the main difference between them is passing five points on five different image one point per image.

C. Persuasive-cued click point (PCCP) The persuasive cued click point [1][2] is the addition of the persuasive feature to cued click point. It allows user to select less portable password. It has two more function as shuffle and viewport, when users make a secret word, the images are a little monochromic except for viewport for to avoid known hotspots the viewport. The most useful benefit PCCP is make complex system to hackers. Users have to choose clickable area within the area and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport. At the time of password creation users may shuffle many times as he want. Only during the password generation, the viewport & shuffle buttons are displayed. After secrete word generation process, graphical images are presented to users casually without viewport & shuffle or refresh button. Then user has to select particular clickable area on particular image.

3. PROPOSED SOLUTION & PROPOSED MODEL

The two way authentication needs to be developed for the users by using Persuasive Cued Clicked points technique and OTP, which can be effectively used for any system for secure login and but difficult to be guessed by attacker.

A. Registration Process:
B. Login Process:
Proposed model contains following points:

Proposed system provides a high range of security to the users by using Persuasive Cued Clicked point's technique and OTP. The user has to register him by entering his user name; mobile number and email ID. After successful registration user will have to select the five images with which he wants to generate the password by clicking one point on each image. After the five clicks unique password is generated and the registration process is completed. While selecting images user will get two options for selecting images as from system or user an select their favorite images to generate the graphical password. Now every time the user wants to login will have to enter the username and select the start button. After user selects login, user will receive the binary OTP containing 5 bit binary code on his mobile and email ID. Now user want to select the same points which he had selected at the time of registration for the images when the bit in the OTP is 1 and select any other point except the point select while registration for the image when the bit in the OTP is 0.After successful completion of this steps, he will get the access to the system using login.

4. SYSTEM ARCHITECTURE

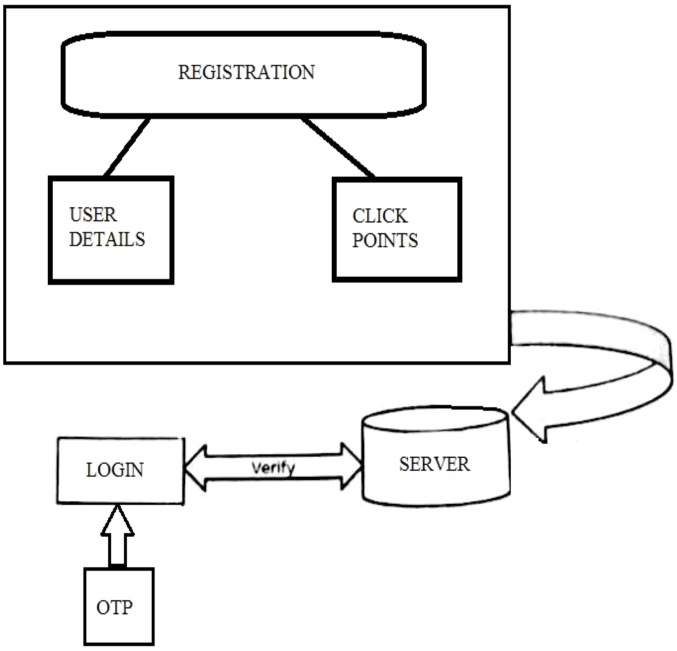

Fig 1.System architecture of proposed model

Registration module focuses on the registration of a new user who needs to register before logging on to the system.

a) User Details:

In this module for registration user needs to like username, name, address, mobile number and email ID, which gets stored in the database for authentication.

Figure 2 shows User Registration form where user needs to fill username, name, address, mobile number and email ID.

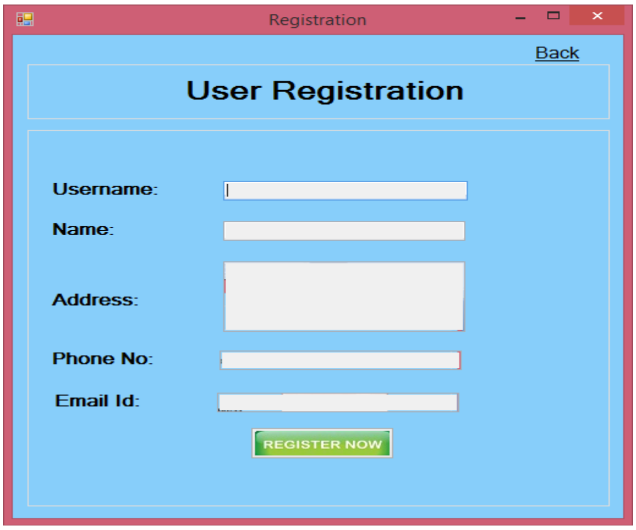

Fig 2.User Registration Form

b) Click Points:

Once the user fills details there is provision of load image which presents images to user after they fill user details .For each image assigned by system there appears a viewport which can be shuffle as per user requirement. A single point inside this viewport user need to select as click point.

Login Module

In this module the user authentication is verified by the system. User has to follow the same sequence of images and selects particular click points which is selected at the time of registration by the user.

User has to verify the username first. After that Image selection page will appear. User has to select one particular point inside this viewport. These procedure should be repeated for the five number of images. If all the images clicked point matches with the user then user allowed using the system.

Figure 3 shows Login form where registered user can login into the system with a valid username.

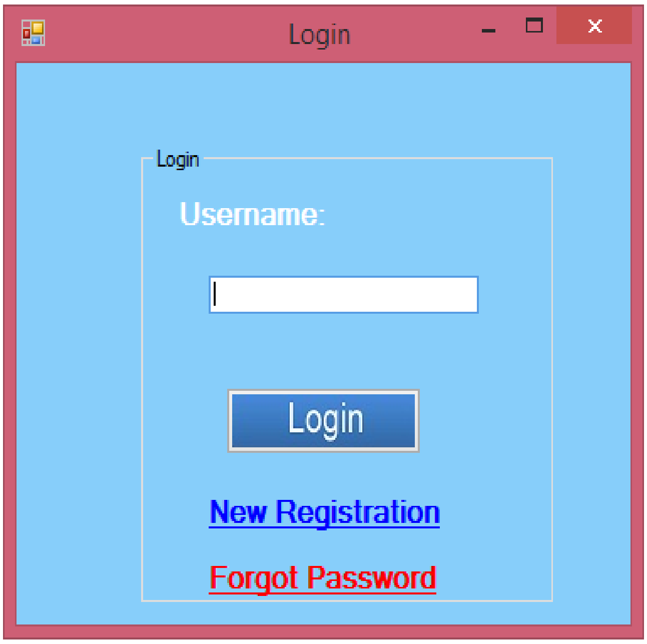

Fig 3.Login Form

Figure 3 shows Image selection form, After clicking on Login button Image selection form gets displayed

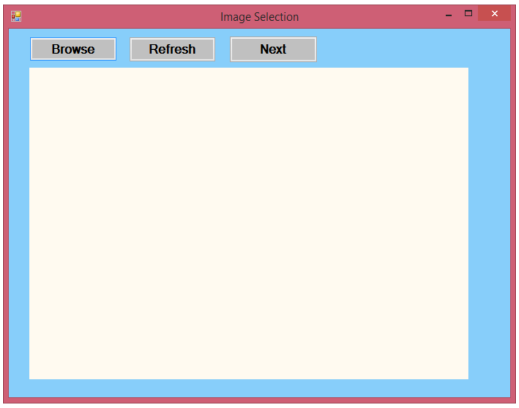

Fig 4.Image Selection Form

Figure 4 shows images with viewport where user can select one point inside the viewport and these procedure will repeat with five images and graphical password will get saved successfully.

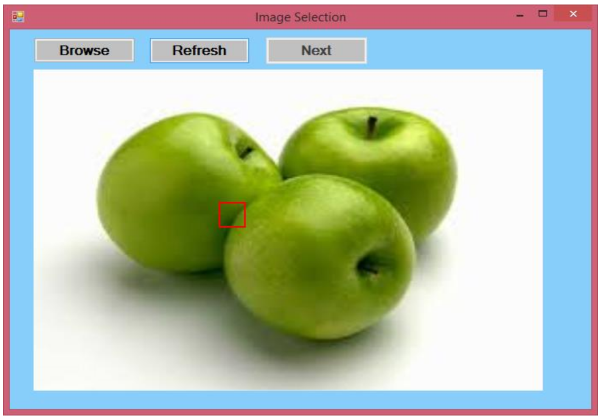

Fig 5.Image with viewport

5. CONCLUSION

Improved Persuasive Cued Click-Points (IPCCP) authentication system is a secure and more user friendly system which contains graphical password, which are easy and flexible for the users to remember as compared to text based passwords and difficult to attack for the attackers. Improved Persuasive Cued Click-Points (IPCCP) approach has tried to reduce the formation of shoulder surfing attack and hotspot. The Improved Authentication Scheme Using Improved Persuasive Cued Click Points system is very efficient to use, secure and flexible to use. This system is very cheap as compared of as biometrics system.

REFERENCES

[1] Neha Singh, Nikhil Bomanwar "Improved Authentication Scheme Using Password Enabled Persuasive Cued Click Point, 2015, IEEE.

[2] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Middle, P.C.van Oorschot "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism, 2012, IEEE.

[3] Arash Habibi Lashkari, Farnaz Towhidi, Dr. Rosli Saleh, Samaneh Farmand ,"A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms", 2009, IEEE

[4] Maslin Masrom, Farnaz Towhidi, Arash Habibi Lashkari, "Pure and Cued Recall-Based Graphical User Authentication", 2009, IEEE

[5] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah K. Mammi, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique", 2008, IEEE.

[6] Fatehah M.D., Mohd Zalisham Jali & Wafa M.K., Nor Badrul Anuar, "Educating Users to Generate Secure Graphical Password Secrets: An Initial Study" 2013, IEEE.

[7] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey" 2005, IEEE.