CUED CLICK POINT (CCP) ALGORITHM FOR GRAPHICAL PASSWORD TO AUTHENTICATE SHOULDER SURFING RESISTANCE

Soni Sharma[1], Prof. G.S Mate[2], Monali Pawar[3], Snehal Patil[4], Sonam Gole[5]

Department of Information Technology, JSPM's Rajarshi Shahu College of Engineering,
Savitribai Phule Pune University Tathawade, Pune, Maharashtra (India)

ABSTRACT

In this paper,we present an approach using cued click point (CCP) under graphical password that permits to enrich authentication technique of graphical password in(CCP). Our literature studies shows various limitations for textual passwords, they are exposed to shoulder surfing attack however strong textual passwords are tough to memorize. Graphical Passwords are introduced to resist the Shoulder surfing attack. .Looking at the success of this system , using graphical password as input and grid lines for image point verificationand enrich it to provide security using normal login and graphical password. This system can be used in the field such as banking application, military application, civilians, forensic labs, etc.

Keywords: *Authentication, Cued click point ,Graphical password,Hotspot ,Shoulder surfing.*

INTRODUCTION

Authentication plays an important role in security of the user system , without which the performance of user system will not be yield very significant improvement. The need of authentication is required for high security .There are various methods to provide authentication like password authentication but this type of authentication cannot provide in the fields like banking application, military, forensic labs, etc. [1].Textual passwords are attacked by Masquerading, Eaves dropping, Dictionary attack, Shoulder surfing attack, Spyware and Guessing attack [7]. To overcome this drawbacks, graphical passwords were introduced. Using graphical password user is able to set up a complex authentication password and is able to recollect it, even if the memory is not activated periodically [3]. This paper focuses on the issues and eliminates them resulting more secure, reliable and useable for users.

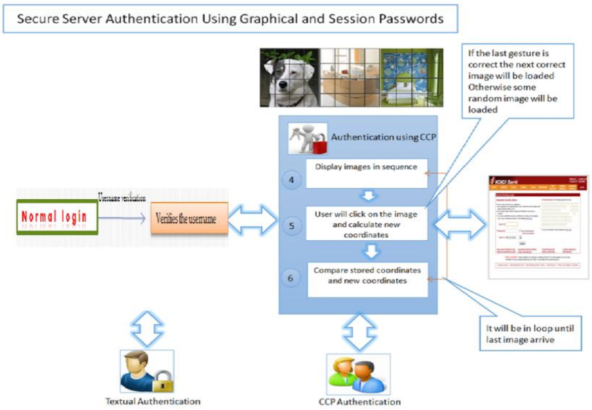

Secure Server Authentication Using Graphical and Session Passwords
If the last gesture is correct the next correct image will be loaded Otherwise some random image will be loaded
Authentication using CCP
Display images in sequence
4
User will click on the image and calculate new coordinates
5
Compare stored coordinates and new coordinates
6
Normal login
Username verification
Verifies the username
It will be in loop until last image arrive
Textual Authentication
CCP Authentication

Fig.1 Architecture of Authentication using cued click point

II. LITRETURE SURVE

In paper[1] author T, R.Nagendran, implemented system in which password is selected block of the image called the view port. But this system failed to secure from hotspot attack. In paper[2] author N. López, M. Rodríguez, C. Fellegi, D. Long. proposed a graphical authentication systems in even odd form.Still unable to resist from shoulder surfing.In paper [3]author S. Man, D. Hong, and M. Mathews, proposed that user should rate colors from 1 to 4 for password and he can remember it as “RGBY”. But the interface is quite difficult to understand to the normal user.In paper [4]author M.Shreelatha, M.Sashi proposed a methodology on Session password which can be used only once,but this technique is proposed to generate session passwords using text which fails to resist shoulder surfing. In paper [5] author, Ushir Kishori Narhar, Ram.B.Joshi proposed a methodology using user name with graphical password using persuasive cued click points along with biometric authentication using finger nail plate.. But biometrics such as face and fingerprints can easily be recorded and potentially misused by biometrics experts without user’s consent. Inpaper [6] Author, Neha Singh, Nikhil Bomanwar proposed a methodology of a persuasive cued click point which reduces the hotspot problem, but provides no security mechanism for shoulder surfing attack .Inpaper[7] Author, Hung- Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh proposed a system based on authentication system Pass Matrix, based on graphical passwords with a one-time valid login indicator. But this System does not resist the shoulder surfing attack and also vulnerable to smudge attack.

III.PROPOSED SYSTEMS

3.1 Problem Statement

From the above literature surveys, we have came to conclusion that there are many attacks taking place regarding the authentication process of the existing system.So we come up with the new authentication system which includes cued click point algorithm to resist shoulder surfing attack based on image password selected by user from image grid and image point is stored in the form of rows and coloumns as password ..

IV.ARCHITECTURE DIAGRAM

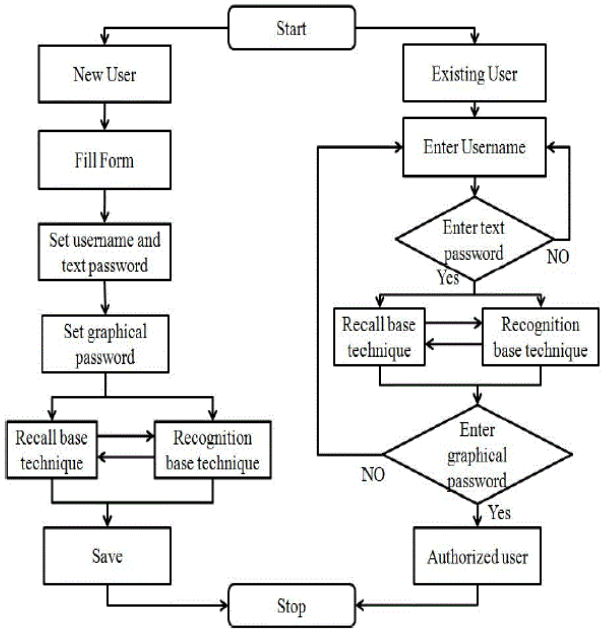


Fig 2: Architectural Flowchart.

3.2 Methods Used

3.2.1. Cued Click Pointalgorithm

By selecting all click point on single image introduces hotspots creation. In CCP user have to select different five images instead of selecting click point on same image. For every image user have to select only one click point[4]. When user click on a correct position on image, then next image will displayed. In CCP address of next image is stored in previous click point. If click point is wrong then wrong image will be displayed. Users have to select sequence of click-point on correct images.

3.2.3. Recall Based Technique

A user is asked to reproduce something that he created or selected earlier during the registration stage.

3.2.4. Recognition Based Technique

A user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected during the registration stage.

3.3 Splits

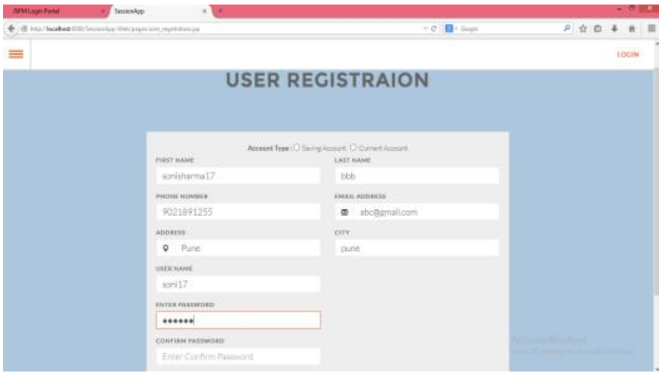
In CCP, user choose one square per image for a sequence of n images. The module of CCP square images divides each image into respective squares. The matrix method is used for dividing the image into squares in the form of rows and columns.The address of each square of the image is recorded in the database when user selects it. This address is stored in the form of rows and columns. For eg.,(1,1),(2,1)etc.

IV. IMPLEMENTATION

4.1. Registration

4.1.1.Text Based Registration

At this stage user creates an account using required credential. However this acts as the first stage of registration of the system.



USER REGISTRAION

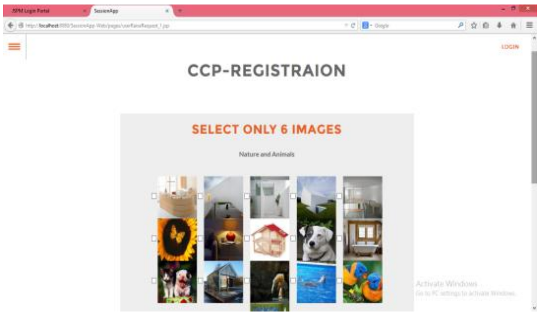
Account Type : ○ Saving Account ○ Current Account

FIRST NAME: sonisharma17
LAST NAME: bbb
PHONE NUMBER: 9021891255
EMAIL ADDRESS: abc@gmail.com
ADDRESS: Pune
CITY: pune
USER NAME: soni17
ENTER PASSWORD: ••••••
CONFIRM PASSWORD: Enter Confirm Password

Fig 3: Text Based Registration.

4.1.2. CCP REGISTRATION

After the first phase, user needs to login using user name and password. CCP registration needs to be done where user is asked to select number of images and splits. User needs to select images from the set of images as shown in fig 4.



ISPM Login Portal | SessionApp

LOGIN

CCP-REGISTRAION

SELECT ONLY 6 IMAGES

Nature and Animals

Fig 4: CCP Registration.

The user needs to select one point from each image for CCP registration.This point will be recorded in the database of the system.After that the user will have to wait for the approval/rejection from admin.

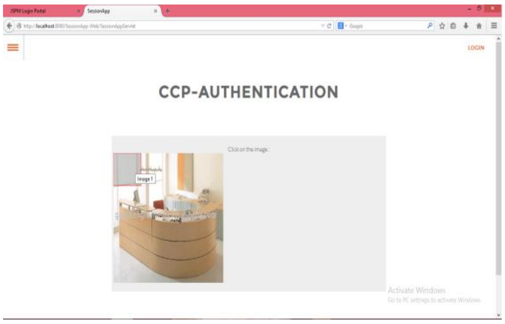
4.2.Login

4.2.1 Normal Login

After registration process, user needs to provide simple login details such as user id followed by password. User is directed to graphical login window.

4.2.2. GRAPHICAL LOGIN

Authorized user will select one click point per image. Each point selection will display another image associated with the address of click point.



ISPM Login Portal | SessionApp

LOGIN

CCP-AUTHENTICATION

Click on the image :

Image 1

Fig 6: CCP Login.

The user is directed to internet banking application as shown in the fig below.

V. MATHEMATICAL MODEL

5.1 Representation in the set format

Let S be set represents various parameters such as input(I), output(O),function(F) and failure case(FC).

S= {(I), (O), (F), (FC)}

Input (I)-

I is the subset of set S which represent input given by the user. Input contains set of images within that images click-points are passed as input.

I = {Username, image 1, image 2,…….image n}

Output (O) -

O is the subset of set S which represent authentication is successfully. If set of click-points of images are correct then it display login successfully.

O = {authentication successful, login successful}

Function (F)-

Set the click point of images. F= {Function}

Failure Case (FC)-

If sequence of click points of images is not correct.

5.2 Calculation for username

Let L be the set of all capital letters A to Z.

L = {A, B ,C……………..Z}

P is set of position on letter in L as,

P = {1, 2, 3 …………. 26}

<L =def {< l, p >: l є L ,p є P }>

u is username such that {u : u is a word which can be described as English words build up of combination of letters in set L} Let u has length „len‟ Then sum of position values is done with function f(x) as ( ) Σ( ) .Such that „n‟ is the index representing the letter in L and Pn is associative position in P.

Sum=f(x) will do the calculation from username.

D1 represent the first digit of sum and always will be from 1 to 9.

5.3 Assigning set of image-

I = {I1, I2 …….I9} set of images such that each Ii is fixed set of rows of images as given J={J1,J2……J9}is fixed set of Columns of images. IJ = {ij}where i1 is one image from set Ii.

5.4 Selection of password-

i1 and i2 will be two images selected from given set Ii

i3 and i4 are two images from server side image set Is

Above 4 images from a password Pw for user Ui Pair (Pw, Ui) will be stored for each user.

VI. RESULTS

6.1 Graph

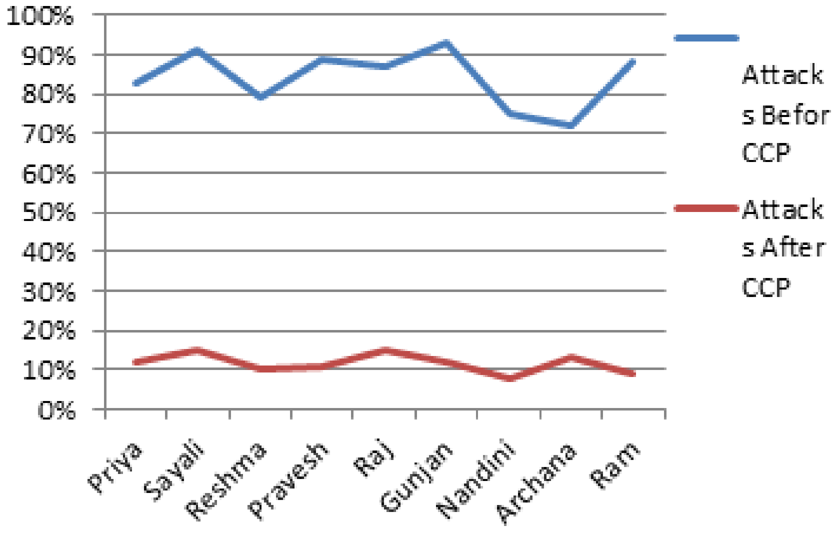


Fig 7: Frequency of Attacks on Systems Before CCP and After CCP.

6.2 TABLE

Table 1. Input parameters Image Id,Image Size, Passpoint Ratio, CCP Ratio.

Image Id & Size	Pass Point Ratio	CCP Ratio
1: 20505	0.004876	0.487685
2:27797	0.003597	0.359710
3:23976	0.004170	0.417083
4:27441	0.003644	0.364418
5:26648	0.003752	0.375262
6:12408	0.008059	0.805931
7:12495	0.008003	0.800320
8:14620	0.006839	0.683994
9:20318	0.004921	0.492174
10:23049	0.004338	0.433858

6.2.1 Equations used in coverage ratio calculation

Image click ratio= (10 *10) /(Image Size)

View Port ratio =(100 *100) /(Image Size)

VII. FUTURE SCOPE

This system can be used for various security systems like system login and logout process in banking, web locking system, folder locking system, etc.

Like most of the other graphical password authentication system shoulder surfing is vulnerable to the guessing attacks. To overcome this problem the user can upload their own images to make it more difficult for attacker to guess it.

VIII. CONCLUSION

Security is most important factor for any system authentication. Firstly pass point method is proposed but due to all click point on the same image minimize the security of system To overcome this problem, we proposed a shoulder surfing

resistant authentication system based on graphical

passwords. In CCP technique more images with separate click point on it is used. The problem of shoulder surfing is solved.

IX.REFERENCES

[1.] Chippy.T, R.Nagendran “Defense against large scale online password guessing attack by using persuasive cued click point” International Journal ofCommunications and Engineering Volume 03– No.3, Issue: 01 March2012.

[2.] N. López, M. Rodríguez, C. Fellegi, D. Long. “Even or Odd: A Simple Graphical Authentication System” IEEE LATIN AMERICA TRANSACTIONS, VOL. 13, NO. 3, MARCH 2015.

[3.] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.

[4.] M.Shreelatha, M.Shashi. M Anirudh, Md.Sultan Ahamer, V Manoj Kumar “Authentication scheme for session password using color and images ” International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

[5.] Hung- Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh 2015 International Conference on Computing Communication Control and Automation.” Highly Secure Authentication Scheme”.

[6.] Improved Authentication Scheme Using Password Enabled Persuasive Cued Click Points”.978-1-4673-7910-6/15/$31.00_c 2015 IEEE.

[7.] DOI 10.1109/TDSC.2016.2539942, IEEE Transactions on Dependable and Secure Computing.”A Shoulder Surfing Resistance Graphical Authentication System. .Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Chen.

[8.] S. Gurav, L. Gawade, P. Rane, and N. Khochare, “Graphical password authentication: Cloud securing scheme,” in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[9.] H. Zhao and X. Li, “S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme,” in Advanced Information Networking and Applications Workshops, 2007, AINAW’07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 467–472.

[10.] M. Martinez-Diaz, J. Fierrez, and J. Galbally, “Graphical password based user authentication with free-form doodles,” IEEE Transactions on Human-Machine Systems, vol. PP, no. 99, pp. 1–8, 2015.