International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 4 94 - 97

# Graphical Password Scheme Using Cued Click Point and Persuasion with Multiple Images

Ansari Sarim
Department of Information Technology
Rajiv Gandhi Institute of Technology
Mumbai, India

Rokade Jayesh
Department of Information Technology
Rajiv Gandhi Institute of Technology
Mumbai, India

Khan Ishan
Department of Information Technology
Rajiv Gandhi Institute of Technology
Mumbai, India

Shaikh Adil
Department of Information Technology
Rajiv Gandhi Institute of Technology
Mumbai, India

Govind Wakure
Department of Information Technology
Rajiv Gandhi Institute of Technology
Mumbai, India

***Abstract***—There are three main categories of authentication system – token-based (what you have), biometric-based (who you are) and knowledge-based (what you know). Cued Click Point is a graphical password scheme which is a type of knowledge based authentication. In CCP, user clicks on one point per picture for an arrangement of pictures.CCP gives more prominent security than PassPoints in light of the fact that the quantity of pictures builds the workload for attackers. The proposed system uses persuasion allowing user's choice to a certain extent while encouraging users towards stronger and less-vulnerable passwords.In the proposed system, the undertaking of choosing less secure passwords (which are simple for attackers to hack) is more monotonous, disheartening users from settling on such decisions.In actuality, this approach makes picking a more secure secret key less weight on clients, it is less demanding to take after the framework's recommendations for a protected password—an element lacking in many systems. CCP is an effective alternative to text-based passwords and other forms of traditional authentication system. Psychological studies have also revealed that human mind can recognize images faster than text and numbers. CCP can be applied to a system front-end which requires high level of security.This paper presents implementation of Cued Click Point (CCP) graphical password which uses persuasion along with multiple images.

***Keywords***-*User Authentication, Cued Click Point, Tolerance, Graphical Password, Persuauion*

_____._____*****_____

## I. Introduction

Different graphical passwordschemehas been proposed as contrasting options to text based passwords. Research and experience have demonstrated that text based passwords are laden with both ease of use and security issues that make them not as much as alluring options. Brain science have uncovered that the human mind is better at perceiving and reviewing pictures than content. Graphical passwords are planned to gain by this human trademark with the expectation that by diminishing the memory load on clients, combined with a bigger full secret key space offered by pictures, more secure passwords can be delivered. A watchword comprises of a single click point for each picture for an arrangement of pictures. The following picture showed depends on the past snap point so clients get prompt certain input with respect to whether they are on the right way when signing in. CCP offers both enhanced ease of use and security rehearses to adapt. In this venture, we propose another snap based graphical secret key plan called Persuasive Cued Click Point with Multiple Images. It helps clients rapidly make and re-enter their passwords. Another element of CCP is the quick certain input telling the right client whether their most recent snap point was effectively entered.

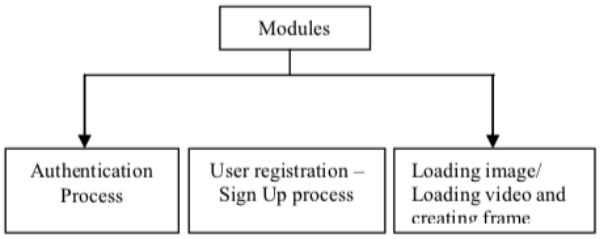
Persuasive Technology - Persuasive Technology was first articulated by Fogg as using technology to motivate and influence people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As detailed below, PCCP accomplishes this by making the task of selecting a weak password more tedious and time consuming. The path of least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across users is minimized since click-points are more randomly distributed. PCCP's design follows Fogg's Principle of Reduction by making the desired task of

choosing a strong password easiest and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

Password space for a system is the number of unique passwords that will be generated depending on system rules. In the method of click point scheme, password space is (w*h )/t2)^c in this the size is in pixel (w*h) is separated with the size of tolerance square (t2), the total number of tolerance squares/image, raised to power of number of click point provided in image password.

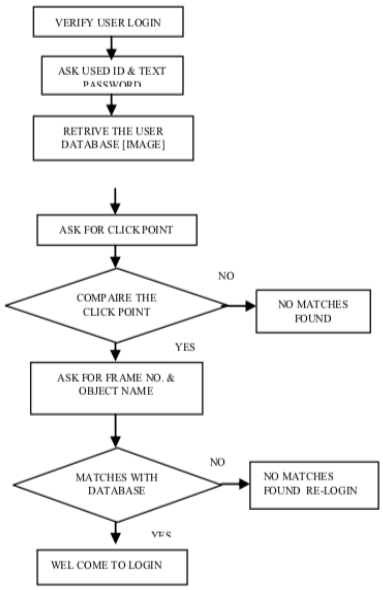
## II. PROPOSED SYSTEM

The system is designed with the help of three modules such as Authentication Process, User registration /Sign Up process module, Loading image module. (see Figure).

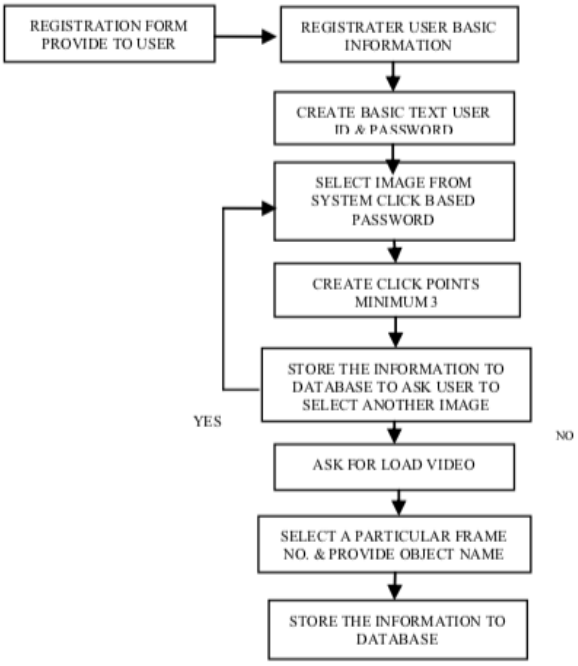



Modules

Fig. In Authentication Process, the system collects user id and password from the user, then the system will retrieve the images for that particular user from the data base and ask user for click points. If the user clicks on all the right click-points, then he/she is authenticated and if the user clicks on wrong click-points for a specified number of attempts then the system will shutdown.




In User Registration module,the user enters the user name in user name field and choose the difficulty level. When user entered all user details in registration phase, these registration data of different users are stored in database and used during login phase for verification. The user select image from system and choose a click-point within that image. The system then stores the total information of user to the database and ask the user to select more images.




## III. LITERATURE SURVEY

SPATIAL PATTERNS: We took a gander at a few watchword attributes to discover whether known examples exist that could enable assailants to adjust an assault methodology. These examples include the spatial position of snap directs relative toward each other and don't consider the foundation picture. In prior work, we played out this examination on a subset of the present information, concentrating fundamentally on information from lab considers. The snap point dispersions of PCCP along the x- and y-tomahawks fell inside the range for irregular conveyances. Combined recurrence dissemination of hotspot scope for PassPoints, CCP, and PCCP. 95 percent likelihood, while those of PassPoints demonstrated an unmistakable movement from upper left to base right in view of the ordinal position of the snap focuses inside the watchword. We trust that the distinction in clients' determination system depends on whether the snap focuses are chosen on one picture, as in PassPoints, or dispersed over a few pictures. With one picture, as in PassPoints, clients tend to begin at one corner of the picture and advance over the picture with each resulting click-point. In any case, with CCP and PCCP, clients see another picture for each snap point and have a

tendency to choose each snap point freely, with no respect to its ordinal position inside the secret word.

As for edges and slants framed between nearby line sections inside passwords, examination demonstrates that PCCP passwords have vast edges and support no specific bearing. Interestingly, PassPoints passwords frequently shape straight even or vertical lines. So also, the recurrence circulations for the general shapes framed by following the way from the first to last snap point for PCCP are inside the scope of the arbitrary informational indexes. PassPoints passwords were significantly more prone to frame identifiable shapes.

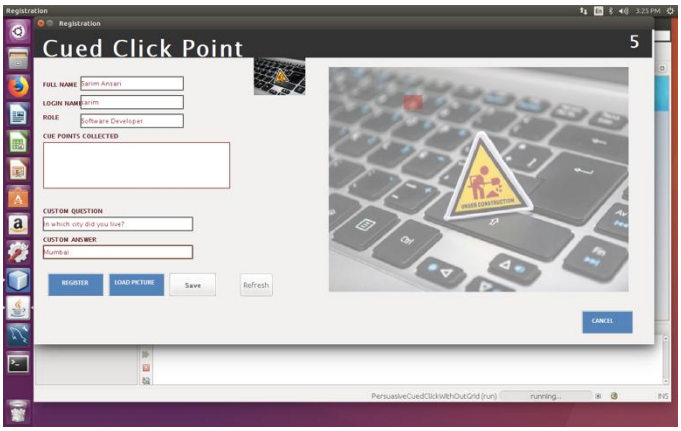
VIEWPORTS: The viewport obvious amid watchword creation must be sufficiently huge to permit some level of client decision, yet sufficiently little to have its expected impact of appropriating click focuses over the picture. Physiologically, the human eye can watch just a little piece of a picture at any given moment. Choosing a tick point requires high keenness vision utilizing the fovea, the zone of the retina with a high thickness of photoreceptor cells . We picked the extent of the viewport to fall inside this region of sharp vision. The viewport situating calculation haphazardly set the viewport on the picture, guaranteeing that the whole viewport was constantly noticeable and that clients had the whole viewport zone from which to choose a tick point. This outline choice had the impact of deemphasizing the edges of the picture, somewhat supporting the focal region. A potential change is permit the viewport to wrap around the edges of the picture, bringing about circumstances where the viewport is part on inverse edges of the picture.

DISCRETIZATION: Discretization of snap focuses takes into account around adjust click-focuses to be acknowledged by the framework without putting away correct snap point facilitates free. Our second model actualized Centered Discretization, wherein an undetectable discretization matrix is overlaid onto the picture, partitioning the picture into square resilience zones, to decide if a login click-point falls inside an indistinguishable resistance zone from the underlying snap point. For each snap point, the framework's position is set amid secret word creation by setting it with the end goal that there is a uniform resistance region based on the first snap point, by figuring the suitable matrix balance (Gx; Gy) (in pixels) from a (0,0) root at the upper left corner of the picture. On ensuing client login, the framework utilizes the initially recorded balances to position the matrix and decide the adequacy of the each login click-point The discretization networks and balances are straightforward and obscure to clients. An aggressor who accessed this data would not know the client's secret word, but rather may endeavor to utilize it to figure higher likelihood click-focuses, e.g., by overlaying comparing lattices onto pictures searching for well known target focuses focused inside framework squares. Regardless of whether this gives any assault advantage over attempting to misuse hotspots without network data remains an open inquiry.

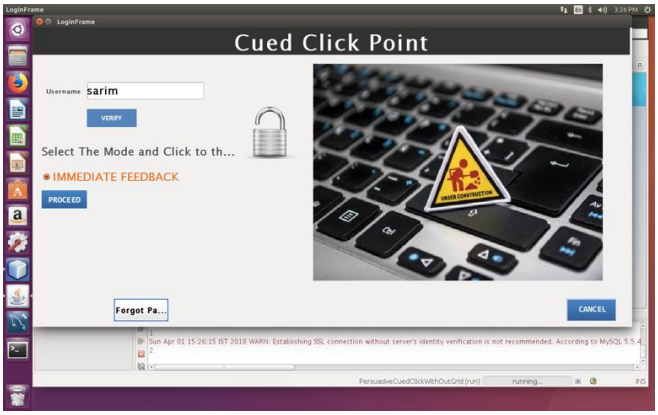
## IV. IMPLEMENTATIONT

The proposed system is successfully implemented by using NETBEANS IDE. Then, snapshots are taken in step wise. The effect of different parameters; such as tolerance size, image size, password space, false accept point are shown.

Registration – A sequence of images is presented to the user to choose. Each image has a randomly highlighted region called viewport. User has to choose a point within viewport. Shuffle button is provided to change the position of viewport to a random position. User can use shuffle button if he unable to find a memorable point within current viewport. Random viewport persuades user to choose point at random location. Thus increases security




Login – The sequence of images which user had chosen while registering himself is presented to the user. User must choose one click-point per image. User has to select the right point from the images they selected during registration. User is authenticated only after clicking in correct tolerance square of image. Not useful for attacker who don't know the correct image sequence.



## V. CONCLUSION

As our system is based on graphical password scheme, it is far easier for users to remember the password. The previous system has been implemented with single images and one or two click-points, our proposed system can contain up to five click-points along with multiple images. By using persuasion to generate random click-points, it becomes difficult for users to select weaker password by avoiding hotspots coverage and easier to select stronger passwords.

## ACKNOWLEDGMENT

We, the authors, are grateful to Prof. Govind Wakure for his great support and guidance throughout this study. He along with other Professors are extremely helpful while carrying out the analysis.

## REFERENCES

[1] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Bddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security CCS), Nov. 2009.

[2] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R.Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.

[3] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Intl J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009.

[4] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords," Proc. ACM Conf. Computer and Comm.

[5] Machado, A. Forget, N. Wright, G. Chan, and R. Biddle, " [Short Paper] The MVP Web-Based Authentication Framework," Proc. Financial Cryptography and Data Security (FC), LNCS, 2012.

[6] S. Chiasson, J. Srinivasan, R. Biddle, and P.C. van Oorschot, "Centered Discretization with Application to Graphical Pass-words," Proc. USENIX Workshop Usability, Psychology, and Security (UPSEC), Apr. 2008.

[7] P. Diggle, Statistical Analysis of Spatial Point Patterns. Academic Press, 1983.

[8] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-Surfing Resis- tance with Eye-Gaze Entry in Click-Based Graphical Passwords," Proc. ACM SIGCHI Conf. Human Factors in Computing Systems (CHI), 2010.

[9] P. Dunphy, J. Nicholson, and P. Olivier, "Securing Passfaces for Description," Proc. Fourth ACM Symp. Usable Privacy and Security (SOUPS), July 2008.

[10] B. Pinkas and T. Sander, "Securing Passwords against Dictionary Attacks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS), Nov. 2002.

[11] A. Duchowski, Eye Tracking Methodology: Theory and Practice, second ed. Springer, 2007.

[12] Dimitri Van De Ville, W.P., Rik Van de Walle, Ignace Lemahieu, Image Scrambling Without Bandwidth Expansion. IEEE Transactions on Cirsuits and Systems for Video Technology, 2004. 14

[13] R. Biddle, S. Chiasson, P. van Oorschot, "Graphical passwords: Learning from the first twelve years," vol. 44, no. 4, 2012