Cued Click-Points of a Knowledge Based Authentication Mechanism

[1]Ms.M.Karthigaiselvi , [2]Ms.M.Manochithra , [3]Ms.S.Sivasankari , [4]Mr.A.AnnaArasu
[1,2,3]CSE dept, Mangayarkarasi college of engineering , Madurai, Tamilnadu.
[4]Hod/ CSE dept , Mangayarkarasi College of engineering,Madurai, Tamilnadu.

Abstract—

This paper presents a security plot with the assistance of Graphical Password which utilizes pictures. The current review based graphical plans under Knowledge based confirmation give the degree to overcome the watched deficiencies of picture choice, hotspot issue, secret phrase creation time, login time we proposed a prompted snap focuses is a tick based graphical secret word conspire, a signaled review graphical secret word system. Clients Click on one point for each picture for an arrangement of pictures. The following picture depends on the past snap point. Execution was great as far as speed, exactness, and number of mistakes. Different graphical secret word plans have been proposed as options in contrast to content based passwords. We propose another snap based graphical secret key plan called Cued Click Points (CCP) with soundsignature. It very well may be seen as a mix of Pass Points , Pass faces , and Story. A secret key comprises of a single tick point for each picture for a succession of pictures. The primary objective of this task is to help the clients in choosing better and safe passwords. It is give very verified verification plot client name with graphical secret phrase utilizing (CCP)cued click focuses with sound signature. The consider demonstrates that graphical picture could be utilized for validation which have different preferred standpoint over content based secret phrase

I. INTRODUCTION

Cloud computing implies that rather than all the PC equipment and programming you're utilizing sitting on your work area, or some place inside your organization's systems, it's given to you as an administration by another organization and got to over the Internet, for the most part in a totally consistent manner. Precisely where the equipment and programming is found and how everything functions doesn't make a difference to you, the client—it's only some place up in the shapeless "cloud" that the Internet speaks to. Distributed computing is a kind of figuring that depends on shared registering assets as opposed to having neighborhood servers or individual gadgets to deal with application. In its most basic depiction, distributed computing is taking administrations ("Cloud benefits") and moving them outside an association's firewall. The current framework is Pass Points. It proposed Passwords which could be made out of a few points anyplace on a picture. They additionally proposed a plan with three covering lattices, taking into account login endeavors that were around right to be accepted. The existing framework is Pass Points. It proposed Passwords which could be made out of a few points anyplace on a picture. They likewise proposed a plan with three covering frameworks, taking into account login endeavors that were around right to be accepted.It appears glaringly evident that a few territories of a picture are increasingly appealing to clients as snap points.If this marvel is excessively solid, the probability that aggressors can figure a secret key essentially increases.If assailants realize which pictures are being utilized, they can choose a lot of likely hotspots through picture handling apparatuses or by watching a little arrangement of clients on the objective picture and after that building an assault word reference dependent on those points.Click prompted focuses is a tick based graphical secret phrase plot, a signaled review graphical secret key method. Different graphical secret word plans have been proposed as options in contrast to content based passwords.It can be utilized as secret key for envelope lock, web-driven applications, work area lock and so on.

II. RELATED WORK

Graphical secret key plans can be gathered into three general classifications: acknowledgment, review, and signaled review Recognition is the simplest for human memory though unadulterated review is most troublesome since the data must be gotten to from memory without any triggers. Signaled review falls between these two as it offers a prompt which ought to set up setting and trigger the put away memory.

A. *Passfaces*

Passfaces is a graphical secret phrase conspire dependent on perceiving human appearances. Amid secret key creation, clients select various pictures from a bigger set. To sign in, clients must recognize one of their pre-chosen pictures from among a few distractions. Clients should accurately react to some of these difficulties for each login. Davis et al executed their own adaptation called Faces and led a long haul client think about. Results demonstrated that clients could precisely recall their pictures however that client picked passwords were unsurprising to the point of being uncertain.

B. *Story*

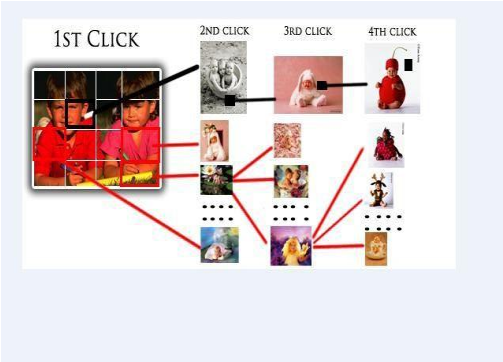
Davis et al proposed an elective plan, Story utilizes everyday pictures rather than appearances, necessitates that clients select their pictures in the right request. Clients were energized for making a story as a memory help. It results in fairly more terrible than Faces for memorability, however client decisions were substantially less unsurprising.

C. *Passpoint*

Wiedenbeck et al proposed PassPoints, where .passwords could be composed of several points anywhere on an image. They also proposed a "robust discretization" schema, with number of overlapping grids, allowing for login attempts that were closely resembling correct to be accepted and converting the entered password into a cryptographic verification key.

D. *Cued Click Point*

Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, users click one point on each image rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point. It also makes attacks based on hotspot analysis more challenging.

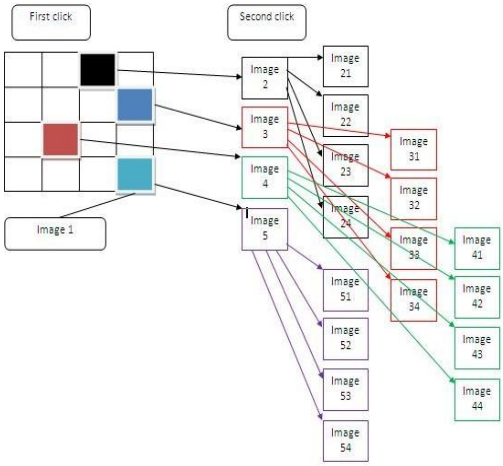


III. PROPOSED SYSTEM

Click cued points is a click-based graphical password scheme, a cued-recall graphical password technique.

Various graphical password schemes have been proposed as alternatives to text-based passwords.

It can be used as password for folder lock, web-driven applications, desktop lock etc.



Various graphical password schemes have been proposed as alternatives to text-based passwords.

Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions.

Psychology studies have revealed that the human brain is better at recognizing and recalling images than text.

IV. LITERATURE REIVEW

Rachagundla, Moulisai, and Syed Gulam Gouse [1] proposed a Graphical Password Scheme using Persuasive Cued Click Points. Even when

there are many types of passwords, knowledge based passwords is very important area of study.

Wiedenbeck, Susan, et al. [2] proposed a design and implementation of a graphical passwords scheme. In this the mechanism allows the resistance of shoulder surfing.

Dirik, Ahmet Emir, Nasir Memon, and Jean-Camille Birget [3] proposed a modelling mechanism which is a user choice by persuasive cued click points. This is done by Graphical passwords using pictures.

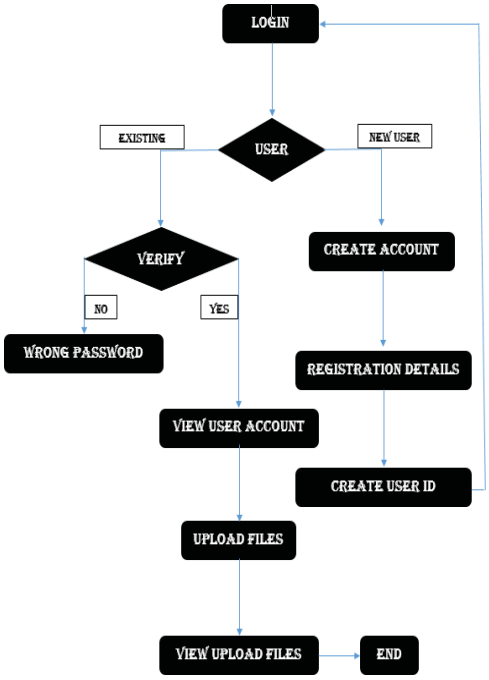
Davis, Darren, Fabian Monrose, and Michael K. Reiter [4] proposed a scheme for users with own selection choice of images and click points. The graphical passwords are better and more traditional than textual passwords.

Gao, Haichang, et al. [5] proposed a different and new scheme using Graphical passwords. This scheme is made to be shoulder surfing resistant by which an attacker cannot directly record the password .

Chiasson, Sonia, Paul C. van Oorschot, and Robert Biddle

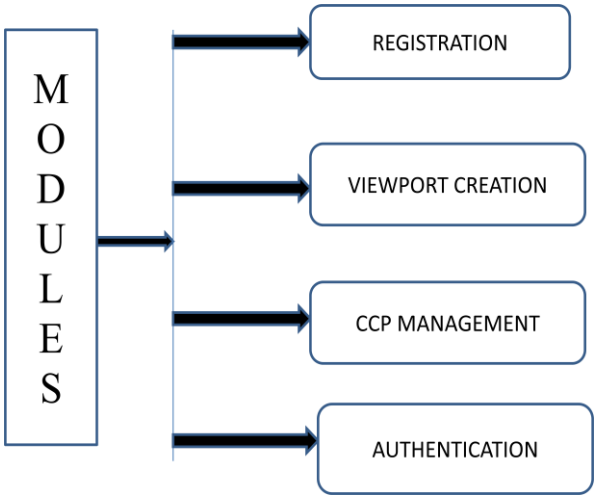
[6] proposed a scheme using graphical passwords which is a new trend in the present generation. They implemented the scheme by using cued click points technique which is also known as a cued recall graphical password technique.

V. SYSTEM DESIGN



The system designed consists of three modules: user registration module, picture selection module and system login module.

The following system modules below:



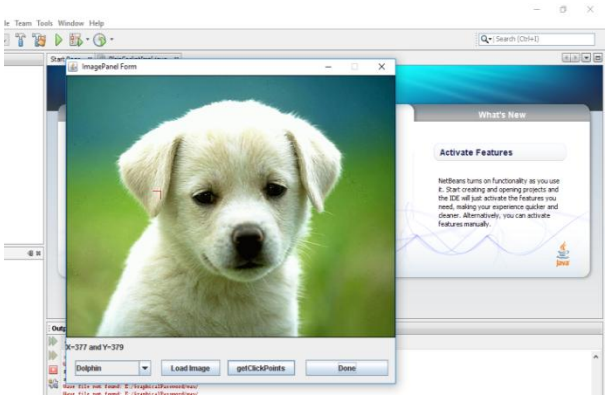
A. *Registration*

In PassPoints, passwords consist of a sequence of Five click-points on a given image. Users may select x,y pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points.

B. *Viewport Creation*

By adding a persuasive feature to CCP encourages users to select less predictable passwords, and makes it more difficult to select passwords where all five click-points are hotspots. Since such information might allow attackers to improve guesses and could lead to the formation of new hotspots. The

viewport's size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points.

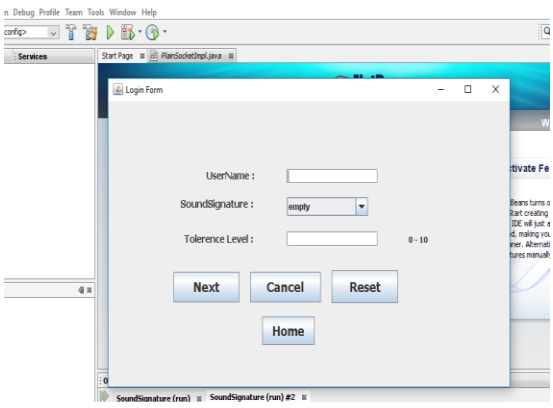


C. CCP Management

Users must select a click-point within this highlighted viewport and cannot click outside of the viewport, unless they press the shuffle button to randomly reposition the viewport. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images.

D. Authentication

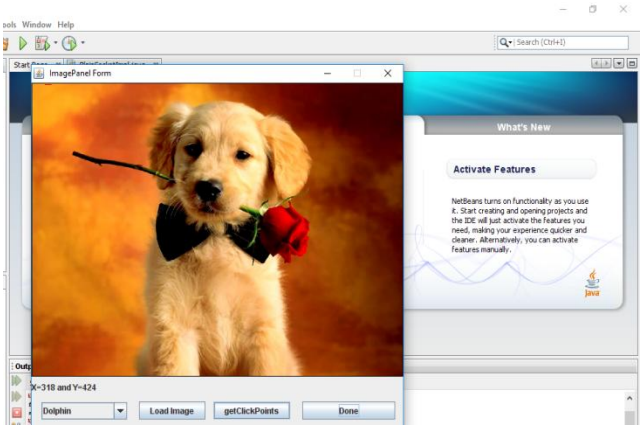
Password entry becomes a true cued-recall scenario, wherein each image triggers the memory of a corresponding click-point. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. When logging on, seeing an image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry.



VI. EXPERIMENTAL RESULTS

The login page of the model contains the Email ID textbox along with create a new user button. We also add the login and cancel buttons.

If we click on the new user link then we will be redirected to the registration process page. In this page the user can enter his personal details like name, date of birth, email ID and phone number. He should click on the points of the images to set a password and submit it. After that a unique ID is generated for the user.



VII. CONCLUSION

The Cued Click-Point method is very usable and provides great security using hotspot technique. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image. Cued Click Point is more secure than the previous graphical authentication methods. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then analyze for hotspot on each of these images. Cued Click-Points method has advantages over other password schemes in terms of usability, security and memorable authentication mechanism. 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. The goal of the security measure is to create a very difficult and safe password which will ensure the safety of the Users resources. This is the main concern for any organization which wants to protect their confidential data from intruders. For this reason we have taken up this project of Graphical Passwords. These types of passwords are a recent trend which will be replacing the textual passwords. The importance of the graphical passwords is been discussed in this project and we also mentioned how these graphical passwords are used in different

areas. Out of many methods implementing the graphical passwords we have chosen to work on Persuasive Cued Click Points. This method will take the click points on images as password and reduce guessing attack by intruders.

In this project we also discussed how the shuffling of images is done to make it more secure by reducing the hot spots. The persuasive method is achieved when we take the small area around selection into consideration rather taking exactly a pixel. This will be accurate for a password and comfortably accessible by the User. We have implemented the project by using .NET as coding language and software used is Microsoft Visual Studios. The database used is SQL Server. The solution system will consider three selection points on three different images and grants access to the user if all selection points are correctly chosen.

The screens are made to user basic requirements and we are able to store the data in a database table. So the main objective of us is to help and encourage users to select better and safe passwords which will secure the confidential data from intruders. The graphical passwords are the future trend considering all types of passwords into account. This means that it has a better scope in coming future and will be implemented in many areas of study and research.

REFERENCE

[1] S. Chiasson, R. Biddle, and P. van Oorschot, “A Second Look at the Usability of Click-Based Graphical Passwords,” Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[2] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, “Influencing Users towards Better Passwords: Persuasive Cued Click- Points,” Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.

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

[4] 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.

[5] V. Varadharajan and U. Tupakula, “Security as a service model for cloud environment,” IEEE Trans. Netw. Service Manag., vol. 11, no. 1, pp. 60–75, Mar. 2014.

[6] R. Durner and W. Kellerer, “The cost of security the SDN control plane,” in ACM CoNEXT—Student Workshop, Dec. 2015

[7] Birget, J.C., D. Hong, and N. Memon. “Graphical Passwords Based on Robust Discretization.” IEEE Trans. Info. Forensics and Security, 1(3), September 2006.

[8] Dirik, A.E., N. Menon, and J.C Birget. “Modeling user choice in the PassPoints graphical password scheme”. ACM SOUPS, 2007.

[9] Thorpe, J. and P.C. van Oorschot. “Human-Seeded Attacks and Exploiting HotSpots in Graphical Passwords.” 16th USENIX Security Symposium, 2007.

[10] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska, “Vulnerabilities and security issues in optical networks,” in 16th Int. Conf. on Transparent Optical Networks (ICTON), July 2014, pp. 1–4.

[11] T. Szyrkowiec, M. Santuari, M. Chamania, D. Siracusa, A. Autenrieth, and V. Lopez, “First demonstration of an automatic multilayer intent-based secure service creation by an open source SDN orchestrator,” in 42nd European Conf. on Optical Communication (ECOC), Sept. 2016, pp. 1–3.

[12] M. Chamania, T. Szyrkowiec, M. Santuari, D. Siracusa, A. Autenrieth, V. Lopez, P. Sköldström, and S. Junique, “Intent-based in-flight service encryption in multi-layer transport networks,” in Optical Fiber Communications Conf. and Exhibition (OFC), Mar. 2017, pp. 1–2.

[13] Clustering analysis of network traf_c for protocol-and Symp., vol. 5. 2008, pp. 139_154.

[14] W. Wu, J. Alvarez, C. Liu, and H.-M. Sun, ``Botdetection using unsupervisedmachine learning," Microsyst. Technol., vol. 24, no. 1, pp. 209_217, 2018.

[15] M. Yahyazadeh and M. Abadi, ``BotOnus: An online unsupervised method for botnet detection," ISC Int. J. Inf. Secur., vol. 4, no. 1, pp. 51_62, 2012.

[16] "A Graphical Password Scheme using Persuasive Cued Click Points." International Journal of Modern Engineer-ing Re-search (IJMER) of a shoulder-surfing resistant graphical password scheme." Proceedings of the working conference on Advanced visual interfaces. ACM, 2006.

[17] Dirik, Ahmet Emir, Nasir Memon, and Jean-Camille Birget. "Modeling user choice in the PassPoints graphical password scheme." Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007.

[18] Davis, Darren, Fabian Monrose, and Michael K. Reiter. "On User Choice in Graphical Password Schemes." USENIX Security Symposium. Vol. 13. 2004.

[19] Gao, Haichang, et al. "A new graphical password scheme resistant to shoulder-surfing." Cyberworlds (CW), 2010 International Conference on. IEEE, 2010.

[20] Chiasson, Sonia, Paul C. van Oorschot, and Robert Biddle. "Graphical password authentication using cued click points." European Symposium on Research in Computer Security. Springer Berlin Heidelberg, 2007.

[21] Muniyandi, Ravie Chandren, and Abdullah Mohd Zin. "Advances in Intelligent Systems and Computing." 7th International Conference on Bio-Inspired Computing: Theories and Applications, BIC-TA 2012. 2013.

[22] Farmand, Samaneh, and Omar Bin Zakaria. "Improving graphical password resistant to shoulder-surfing using 4-way recognition-based sequence reproduction (RBSR4)." Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on. IEEE, 2010.

[23] D. Bogdanova, P. Rosso, and T. Solorio, Exploring high-level features for detecting cyberpedophilia," Comput. Speech Lang., vol. 28, no. 1,pp. 108_120, 2014.