iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41416

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Implementation of Graphical Password Authentication Technique for Security Using Cued Click Points Algorithm

Mr. Shantanu Rangari[1], Prof. K. R. Ingole[2]
[1]*PG Scholar,* [2] *Professor, Computer Science & Engineering, Sipna College Of Engineering And Technology, Amravati, Maharashtra, INDIA*

Abstract: ***In today's world, most Internet applications still establish user authentication with a traditional text-based password. Designing a secure as well as user-friendly password-based method has long been on the agenda of security researchers. On the one hand, there are password manager programs that make it easy to create site-specific strong passwords from a single user's password to eliminate the memory burden caused by multiple passwords.***
We offer different levels of authentication such as Textual Authentication, Image Authentication and Audio Authentication to provide better security for applications. User will select username and password while registering in text step. During registration the user has to enter the registered username and password, if it matches the database then the user can log in to the system. In Image Authentication Model, we take image as input from user at the time of registration and put quid point, qud point is selected part of image which is selected by user. At the time of login the user has to select the image and select the part of the image which he/she wants to include at the time of registration, which is called as Cued Points.
Keywords: Graphical password, Text based password, usability, security, Attacks, Authentication

I. INTRODUCTION

In this project, we've proposed a replacement graphical password scheme for accessing web accounts, called "Web Account Access Secured by Identity-Based Graphical Passwords via Watermarking".
In this project, however, we focused on another option: using pictures as passwords. Graphical password schemes are proposed as a possible alternative to text-based schemes, partly motivated by the actual fact that pictures may be remembered better than text; Psychological studies support such a notion. Pictures are easier to recollect or recognize than text. Furthermore, if the amount of possible images is large enough, the potential password space of a graphical password scheme could also be greater than that of text-based schemes, and thus may provide better resistance to dictionary attacks. together with these (presumed) benefits, there's increasing interest in graphical passwords additionally to workstation and web login applications, graphical passwords have also been implemented on ATM machines and mobile devices.

II. LITERATURE SURVEY

1) In this survey paper, they discuss about graphical password authentication methods and exiting graphical password based methods. It fulfills both differing requirements i.e.it is easy to recall and it is tough to predict. Graphical password schemes offer a way of creating more human-friendly passwords. In this safety of the system is very extraordinary. Dictionary attacks and brute force search are infeasible. Passwords are easy to recall. Pictures are stress-free to recall than text strings. Then, they tried to survey on attack patterns and common attacks in graphical password authentication methods. Finally they have discussed different issues related to graphical password.

2) In this system they proposed scheme has various advantages such as it will be hard for attackers to guess the password because using feature of PCCP pattern formation attacks and HOTSPOTS will be removed using viewport & shuffle button. By adding feature of secret drawing to PCCP, attackers fails to know that there is use of secret drawing technique in between these images, unfortunately if they knows about secret drawing, they don't get exact idea that on which image secret has to be done .The one more advantage is that the message of correct password or incorrect password is displayed after the final click only, by this feature it will hard for attackers to find on which image their guess is correct or incorrect. So by this their proposed scheme will provide higher security in authentication

3) In this study they analyzed the properties of a recognition-based graphical password which uses a set of single-object images as the authentication key. They identified factors which implicate source of bias in graphical password selection, based on user preferences. They additionally studied the effects that graphical password length on memo ability and observed the gender role of the participants as a factor for differences in the selection process. The research study in this paper examined the properties of the graphical password in more details and defined user preferences for single-object images based on category, color and shape. Based on the findings in this experiment there are several design implications for similar systems. First, the initial selection of images available in the authentication database has to be adapted to the preference of the users in order to increase the number of images that would be effectively selected as a graphical password. More importantly, the algorithm that selects decoy images to complete the authentication image set should not be strictly random. In order to lower the probability of a guessing attack the decoy selector algorithm should be based on a matrix that is partially aligned with the probabilities of a user selecting images from a specific category and/or with a specific color/shape. For future research, there are several different directions that can expand the results presented in this paper. Initially, we would like to clarify the implications that the users' favorite color might have a strong influence in object preference and evaluate other personal characteristics that affect graphical password selection. Furthermore, several studies with elderly participants conclude that there are no significant differences between men and women when it comes to color preference (Mather et al., 1971; Tate & Allen, 1985; Wijk et al., 1999), indicating that gender differences might dissipate with age. They would like to study how this effect translates in graphical password selection by evaluating selection criteria and differences among senior users. Finally, they would like to deploy this authentication mechanism on mobile devices and evaluate its usable security characteristics in a touch-based interaction environment.

4) In this system they concluded that a major advantage of proposed scheme is that it provides larger password space then the alphanumeric passwords. For Graphical passwords there is a rising interest is that they are better than the Text based passwords, while the important argument for graphical passwords are that people are better at memorizing graphical passwords than text-based passwords. Also it removes the pattern formation and hotspot attack since it provides the system suggestion. Also the proposed system removes the shoulder surfing attack.

III. SYSTEM DIAGRAM

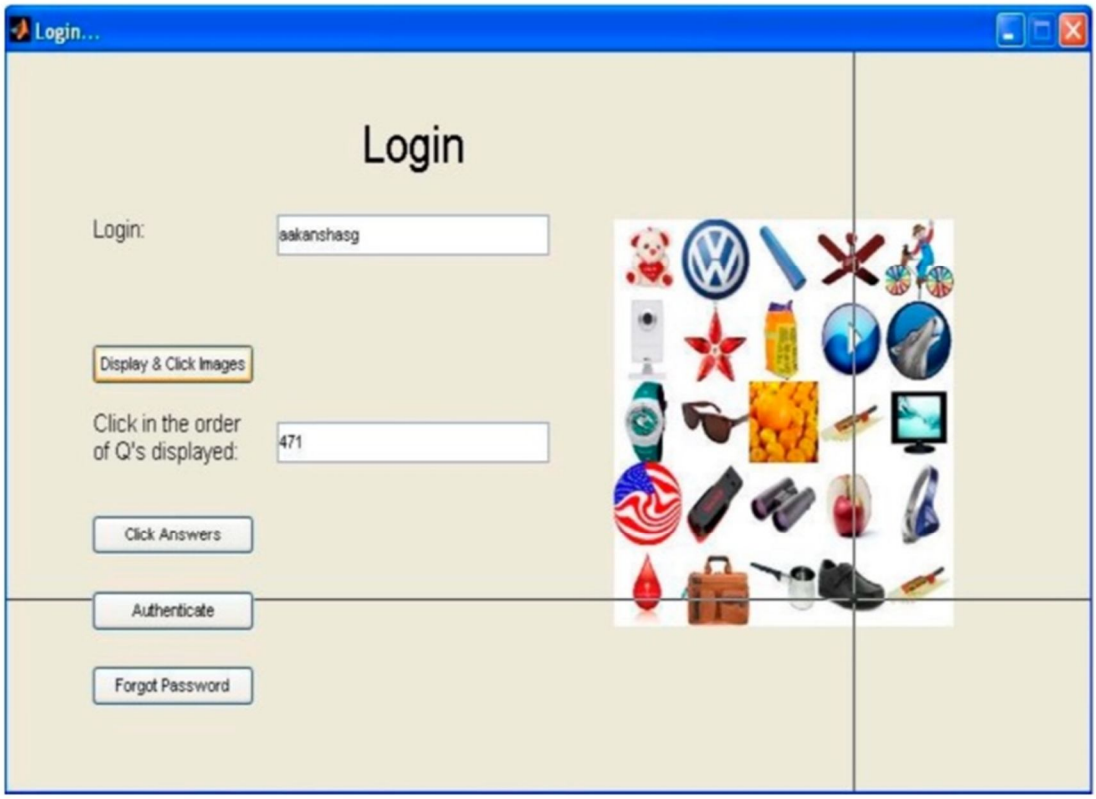
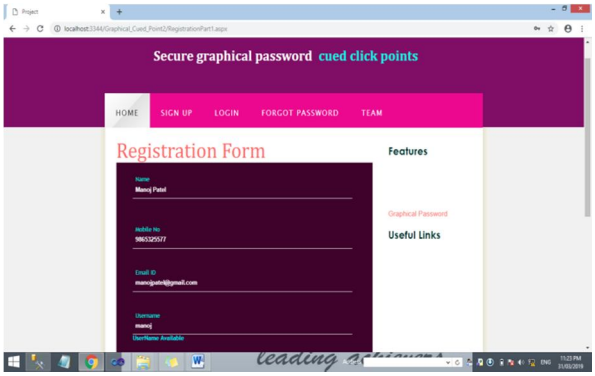
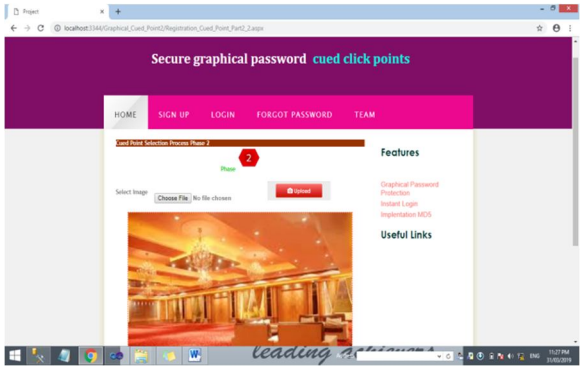


Fig: Graphical Password for Authentication

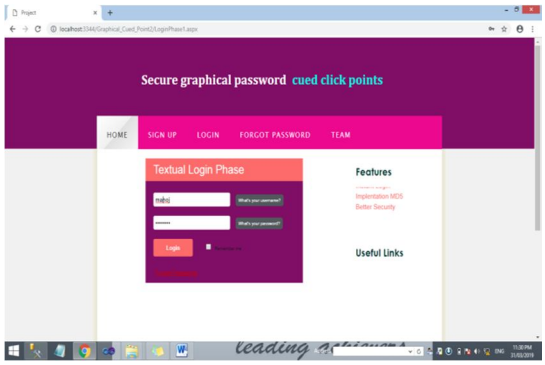
IV. SYSTEM DESIGN



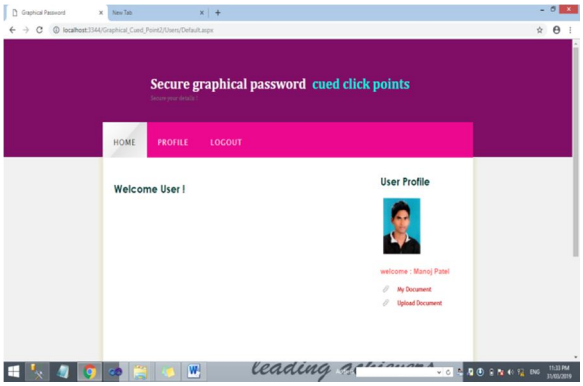
1. Registration Page



2. Cued Point Selection Process Phase 2



3. Login Page



4. After Login Page

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

V. CONCLUSION

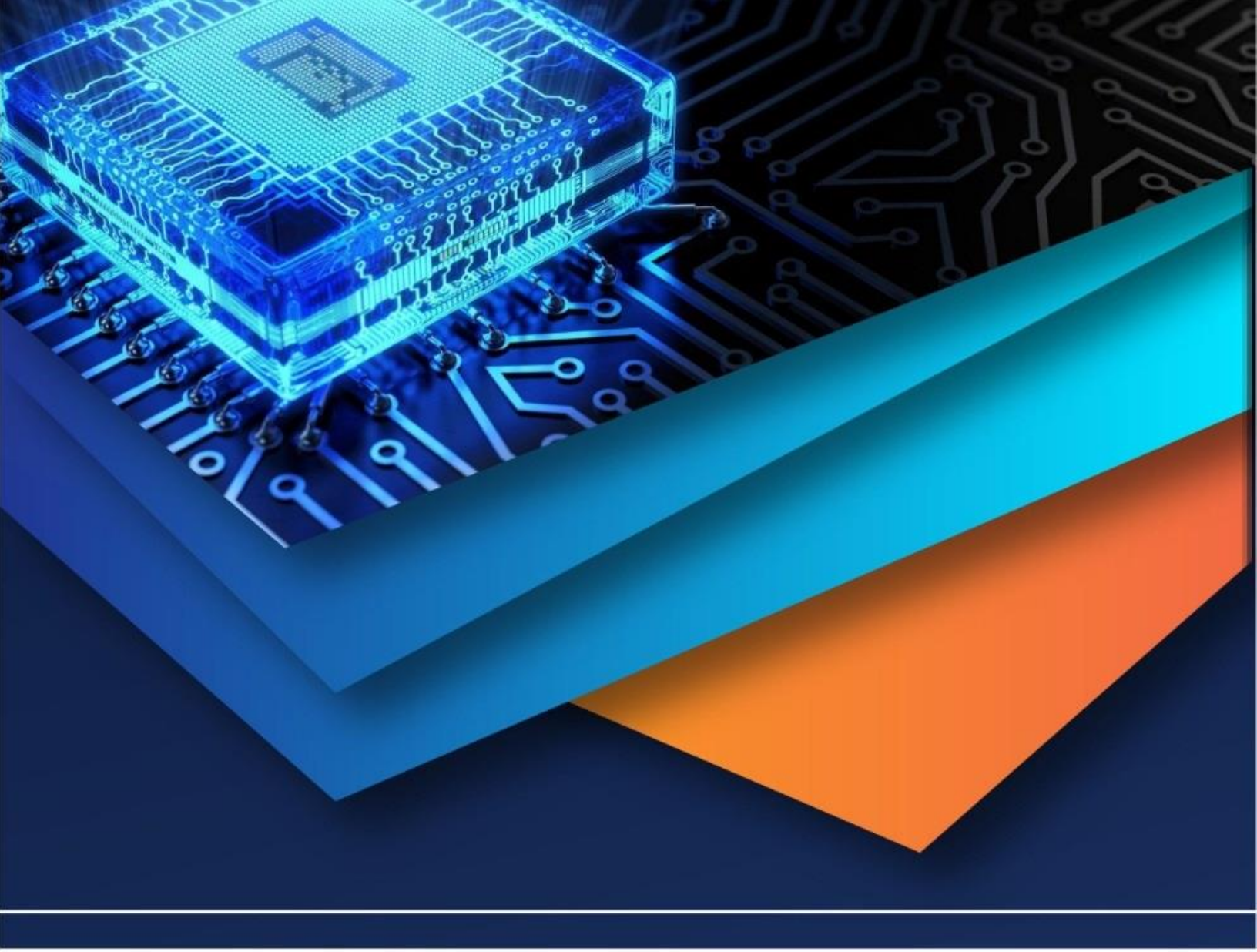
In this survey paper, we discuss about graphical password authentication methods and exiting graphical password based methods based on different survey papers. Hence we successfully concluded and it is easy to recall and it is tough to predict. Graphical password schemes offer a way of creating more human-friendly passwords. Pictures are stress-free to recall than text strings. Then, we tried to survey on attack patterns and common attacks in graphical password authentication methods. Finally we have discussed different issues related to graphical password.

VI. ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to my **Prof. K. R. Ingole** who has in the literal sense, guided and supervised me. I am indebted with a deep sense of gratitude for the constant inspiration and valuable guidance throughout the work.

REFERENCES

[1] Sharayu S.Ganorkar1 ,Prof. H. V. Vyawahare 2 " Review Paper On Graphical Password Authentication Techniques " Volume 5, Issue 03, March -2018
[2] P. R. Devale Shrikala, M. Deshukh and Anil B. Pawar, "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme", International Journal of Soft Computing and Engineering, Vol.3, Issue-2 May 2013.
[3] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9 USENIX Security Symposiums, 2000.
[4] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.
[5] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.
[6] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019 2020, Dec. 2003.
[7] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.
[8] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[9] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.
[10] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY