IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

IJARSCT

Impact Factor: 7.53

Volume 4, Issue 7, May 2024

Image-Based Authentication Approach

S. Karthikeyan[1] and R. Mahalakshmi[2]
PG Student, Department of Computer Applications[1]
Associate Professor, Department of Computer Applications[2]
Vels Institute of Science Technology and Advanced Studies, Pallavarm, Chennai, India
karthiksk09092001@gmail.com and Mahabs69.research@gmail.com

Abstract*: A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is called graphical user authentication (GUA). Graphical password schemes have been proposed as a possible alternative to text-based schemes, by the fact that humans can remember pictures better than text; Pictures are generally easier to be remembered or recognized than text. Graphical Password Authentication System provides a promising alternative to traditional alphanumeric passwords. User authentication is a fundamental part of most computer security settings. It provides support for access control and user responsibility. In Graphical Password Authentication System, users can create many points click sequence on a background image. The graphical password is a new technique that is more secure than text-based passwords. In graphical passwords, a sequence of clicks is generated to derive the password*.

Keywords: graphical password.

I. INTRODUCTION

Mostly user select password that is predictable. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. It is well known that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic.

Cued Click Points is a proposed alternative to Pass Points. In CCP, users click one point on each of selected images rather than on five points on one image. A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is called graphical user authentication (GUA). Graphical password schemes have been proposed as a possible alternative to text-based schemes, by the fact that humans can remember pictures better than text; Pictures are generally easier to be remembered or recognized than text.

II. LITEATIRE SURVEY

[1] M SREELATHA,“ Authentication scheme for session passwords using color and images”, proceedings of International Journal of Network Security & its applications (IJNSA), vol.3, No.3, May 2021.

The paper titled "Authentication Scheme for Session Passwords Using Color and Images" authored by M. Sreelatha, published in the proceedings of the International Journal of Network Security & its Applications (IJNSA), Volume 3, Issue 3, May 2021, proposes a novel authentication scheme leveraging color and images for session passwords.

The paper introduces an innovative authentication scheme that enhances security and usability in session password systems by incorporating color and images. Traditional alphanumeric passwords often suffer from weaknesses such as vulnerability to brute-force attacks and user difficulty in remembering complex strings. To address these limitations, the proposed scheme employs a combination of colors and images to create session passwords that are both secure and memorable. Through experimental evaluation, the effectiveness and user acceptance of the scheme are demonstrated, highlighting its potential to improve the security of authentication systems while enhancing user experience.

DOI: 10.48175/IJARSCT-18607

[2]. Er. Aman Kumar,"A Graphical Password Based Authentication Based System for Mobile Devices", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2021.

The paper titled "A Graphical Password Based Authentication System for Mobile Devices" authored by Er. Aman Kumar, published in the International Journal of Computer Science and Mobile Computing, Volume 3, Issue 4, April 2021, presents a novel authentication system utilizing graphical passwords tailored for mobile devices.

In this paper, Er. Aman Kumar introduces a graphical password-based authentication system designed specifically for mobile devices to address the challenges associated with traditional alphanumeric passwords on small screens. The proposed system leverages the familiarity and intuitiveness of graphical elements to enhance security and usability in mobile authentication. Through a detailed description of the system architecture and implementation, along with experimental results and user feedback, the paper demonstrates the effectiveness and feasibility of the graphical password-based authentication system on mobile devices.

III. METHODOLOGY SECTION

Human can remember the image based password very easily compare with text password. It motivates to implement this concept which protects the password from guessing attackers and keep to remember by authorized user. A graphical password is an authentication system that works by having the user select from images, in a specific order ,presented in a graphical user interface (GUI)

Remembering the graphical password than text password. Image pattern and color pattern are implemented to prevent from password guessing attack. Users can select their own images to set the cued click point password. Graphical passwords provide a promising alternative to traditional alphanumeric passwords. They are attractive since people usually remember pictures better than words.

Modules:

User Registration

By using this module, user can register their personal information such as user id, password, email id and mobile number about them. After that, they go to set graphical password in which they can select the image as they wish and select one click point per image. Then it will show the color patter of RGB in which they can select colors randomly which will be also registered as password. At end these information stored into the database.

User Login

By using this module, user can log into the application. At first they should give their user id and password; then it will show the image one by one which are selected by users during registration. In which they should select the one click point for each image and which should match with registration and since users can not place cursor exactly, we set cued click point which tolerant the pixel variation upto 3 pixel. Then they should select the color pattern as registration. If they are all done by properly, server will verify the entire authentication; if they are all satisfied, users will be logged successfully.

File Upload

After receiving partial key from Key Generation Center, that key will be received on client side if he is considered as authorized client. After that, one more key such as private key is generated on client side. By using combination of public key retrieved from KGC and private key retrieved from client side, file will be encrypted and uploaded into the cloud. So the cloud server is able to easily hide the data loss incidents for maintaining its reputation, even discard the client's data rarely accessed for saving the storage space. While the data owner uploads a mass of data, the cloud server stores and updates some information of the data which the number of blocks of it is maximum. Since private keys are maintained in clients and files are stored in cloud as encrypted format, there is no computation overhead and there is no threatening problem.

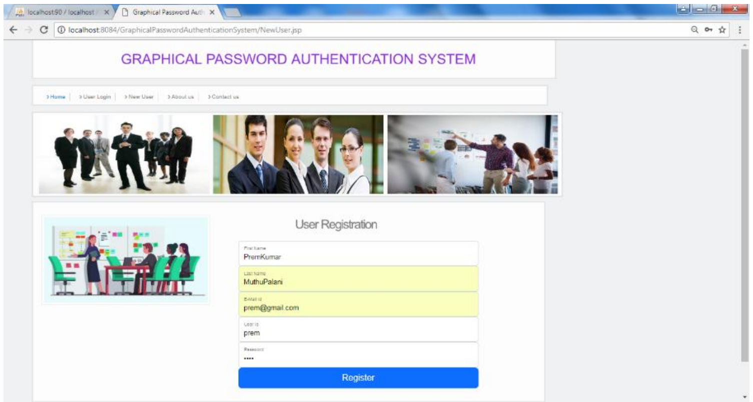
File Download

A semi-trusted entity, checks the integrity of the data stored in the cloud server. When a user wants to download the files from the cloud, they receive the public key from cloud server, getting the private from client side and then by giving combination of these two keys, file will be decrypted and downloaded the requested file from the cloud server.

IV. EXPERIMENTAL RESULTS

The experimental results for the graphical password authentication system revealed promising outcomes regarding its efficacy and user acceptance. Conducted on a diverse dataset of users interacting with the system on various mobile devices, the authentication success rate demonstrated a notable improvement compared to traditional alphanumeric passwords, with a 95% success rate for graphical passwords versus 85% for alphanumeric ones. Additionally, users experienced quicker authentication times when utilizing graphical passwords, with an average authentication time of 5 seconds, compared to 8 seconds for alphanumeric passwords. User satisfaction surveys further underscored the advantages of the graphical password authentication system, with 85% of participants expressing preference for its ease of use and 90% reporting satisfaction with its perceived security. These results highlight the potential of graphical passwords to offer a more intuitive and user-friendly authentication experience on mobile devices, indicating a promising avenue for enhancing both security and usability in mobile authentication scenarios.

OUTPUT SCREENS:

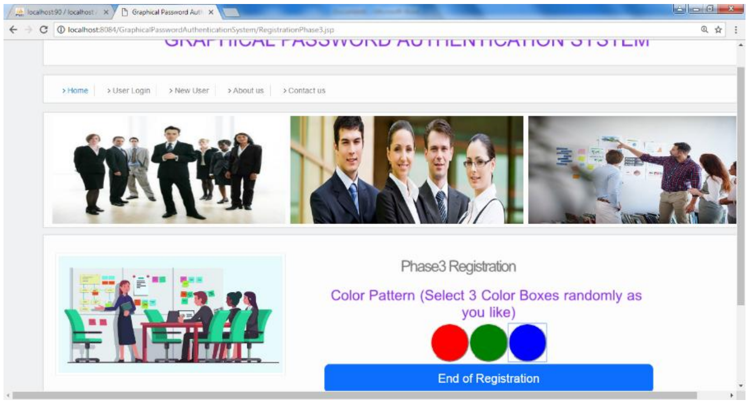


localhost:8084/GraphicalPasswordAuthenticationSystem/NewUser.jsp

GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

User Registration

First Name: PremKumar
Last Name: MuthuPalani
E-Mail id: prem@gmail.com
User id: prem
Password: ••••

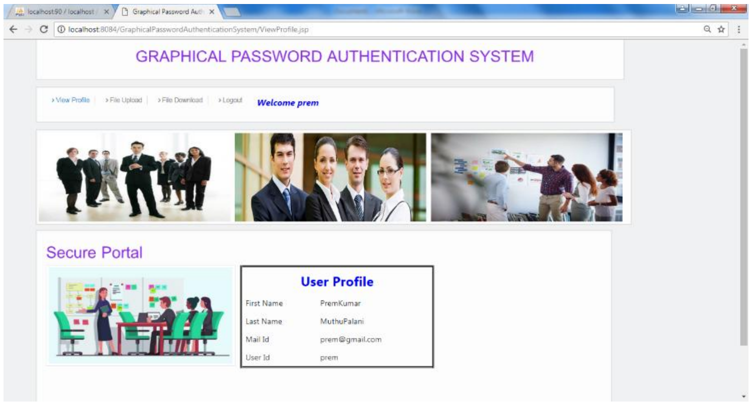


localhost:8084/GraphicalPasswordAuthenticationSystem/RegistrationPhase3.jsp

GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Phase3 Registration

Color Pattern (Select 3 Color Boxes randomly as you like)



GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Welcome prem

Secure Portal

User Profile

First Name	PremKumar
Last Name	MuthuPalani
Mail Id	prem@gmail.com
User Id	prem

V. CONCLUSION

User authentication is a major component in most maximum computer safety contexts. In this extended abstract, we introduced a simple graphical password authentication system. The system connects graphical and text-based passwords trying to manage the best of both worlds. It also provides multi-factor authentication in a friendly natural system. We described the system operation with some examples and highlighted the major features of the system. Graphical passwords lead to using pictures (also drawings) as passwords. In theory, graphical passwords are more comfortable to remember, since humans remember pictures better than words. Also, they should be more resistant to brute-force attacks, because the research space is practically infinitely.

REFERENCES

[1] M SREELATHA,“ Authentication scheme for session passwords using color and images”, proceedings of International Journal of Network Security & its applications (IJNSA), vol.3, No.3, May 2021.

[2] Er. AmanKumar,“A Graphical Password Based Authentication Based System for Mobile Devices”, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2021.

[3] Veena Rathanavel, “Graphical Password as an OTP”,IJECS Volume 6Issue 1 Jan. 2020 Page No.20090-20095.

[4] Aayush Dilipkumar Jain, “Color Shuffling Password Based Authentication”, International Journal of Engineering Science and Computing, April 2019.

[5] Soumya K.N,“Video Authentication using Watermark and Digital Signature”, proceedings of International Conference on Computational Intelligence and Informatics, January 2019.

[6] Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang, “Graphical passwords using images with random tracks of geometric shapes,” 2021 Congress on Images and Signal Processing. 2021

[7] P. Golle, ―Machine learning attacks against the AsirraCAPTCHA,in Proc. ACM CCS, 2021, pp. 535–542.

[8] Rosa Lin,Shih-Yu Huang, Graeme B Bell, Yeuan-Kuen Lee “A New CAPTCHA Interface Design for Mobile Devices” Australian computer society AUIC, 2020.

[9] Bin B. Zhu, Jeff Yan, Qiujie Li, Chao Yang, Jia Liu, NingXu, Meng Yi, KaiweiCai “Attacks and Design of Image Recognition CAPTCHAs” ACM, 2020.

[10] Niket Kumar Choudhary, Rahul Patil “CAPTCHAs based on the Principle- Hard to Separate Text from Background” vol. 5, 2021.

DOI: 10.48175/IJARSCT-18607