ICEST-2K24 [International Conference on Engineering, Science and Technology]
In Association with
International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN - 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

A Shoulder Surfing Resistant Graphical Authentication System

Prof. D. R. Kamble, Prathamesh B. Farade, Aditya D. Patil, Rohit H. Shinde, Nagbhushan S. Tirth
S.B. Patil College of Engineering, Vangali, Indapur, Maharashtra, India

ABSTRACT
The biggest problem in the modern IT sector is information and computer security. Only authorized users should have access to the system or data. A password makes sure that only people with the proper access rights can view or use the computer or the information. A text password, often known as an alphanumeric password, is a common password strategy. However, these text-based passwords are simple to break using numerous attack methods. In order to address these flaws, a graphical. A password-based approach is presented. We came up with there volutionary authentication system Pass Matrix, based on graphical passwords to fend off shoulder surfing assaults, to solve this issue. Pass Matrix provides no suggestion for attackers to figure out or narrow down the password even if they execute several camera-based attacks. It has a one-time valid login indicator and circulative horizontal and vertical bars encompassing the complete scope of pass-images. Cyberattacks surge. Cybercriminals seek efficient channels to spread malware via images. JPEGVigilant, a machine learning method, identifies malicious JPEGs using 10 derived properties.[14] Additionally, we developed a PassMatrix prototype for Android and ran actual user tests to assess its usability and memorability. According to the experimental findings, the suggested approach increases shoulder surfing attack resistance while retaining usability. Pharmaceutical innovation faces challenges. Research merges quantum computing and machine learning to revolutionize drug discovery, simulation, and safety assessment for expedited progress.[13]

Keywords: Shoulder surfing, Computer vision, Privacy, Security, Visual eavesdropping, Detection.

I. INTRODUCTION

Graphical Authentication: The system relies on graphical elements for user authentication instead of traditional text based passwords. This can include patterns, images, or other visual elements.

A. Enhanced Privacy
To resist shoulder surfing, the system ensures that the authentication process doesn't reveal sensitive information to onlookers. The graphical elements should be easy for the user to interact with but difficult for others to interpret.

B. Multi-factor Authentication
Incorporating multiple layers of authentication, such as combining a graphical pattern with a personal identification number (PIN), enhances security.

C. Randomization

The system might introduce an element of randomness in the graphical authentication process, making it challenging for an observer to predict or replicate the user's actions.

II. PROBLEM STATEMENT

To build and implement web application for A Shoulder Surfing Resistant Graphical Authentication System

III. ALGORITHM/WORKFLOW OF SYSTEM

Content Image Selection and choose convolution layer for feature maps: Given a chosen content layer l, the content loss is defined as the Mean Squared Error between the feature map F of our content image C and the feature map P of our generated image Y.

Calculate Gram-matrix for style image: Calculate the Gram-matrix(a matrix comprising of correlated features) for the tensors output by the style-layers. The Gram-matrix is essentially just a matrix of dot-products for the vectors of the feature activations of a style-layer. If the feature map is a matrix F, then each entry in the Gram matrix G can be given by:

The loss function for style is quite similar to out content loss, except that we calculate the Mean Squared Error for the Gram-matrices instead of the raw tensor-outputs from the layers.

The total loss can then be written as a weighted sum of the both the style and content losses.

IV. BLOCK/ARCHITECTURE DIAGRAM

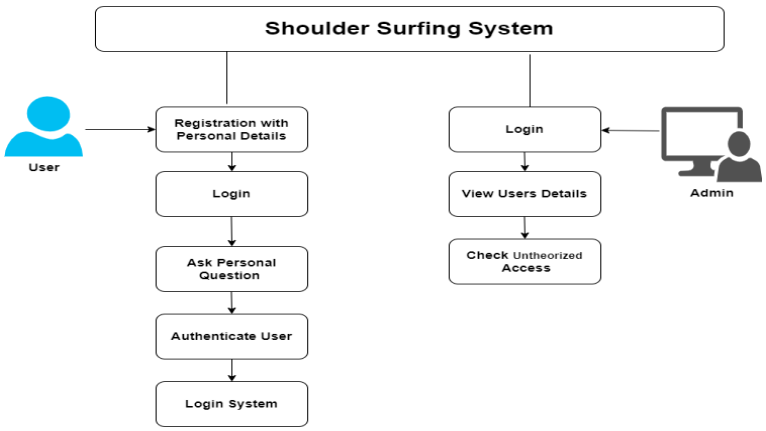


Figure 1: Proposed System

A. Hardware Requirements

- Processor - Intel i3/i5/i7
- Speed- 3.1 GHz
- RAM - 4 GB(min)
- Hard Disk - 40 GB

B. Software Requirements

- Operating System - Windows 7/8/10
- Application Server - Apache Tomcat7/8/9/10
- Front End - HTML, CSS, Bootstrap, JSP
- Language – Java
- Server side Script - Java Server Pages.
- Database - My SQL
- IDE - Eclipse

V. RESULTS AND DISCUSSION

A. Effectiveness

Evaluate how effective the graphical authentication system is at resisting shoulder surfing attacks compared to text-based systems. This could involve analyzing metrics such as success rates of shoulder surfing attempts and user satisfaction.

B. Usability

Discuss the usability of the graphical authentication system. Consider factors such as ease of use, user acceptance, and efficiency in authenticating users compared to text-based systems.

C. Security

Assess the security implications of the graphical authentication system. Determine if it introduces any new vulnerabilities or if it effectively mitigates shoulder surfing risks without compromising security in other areas.

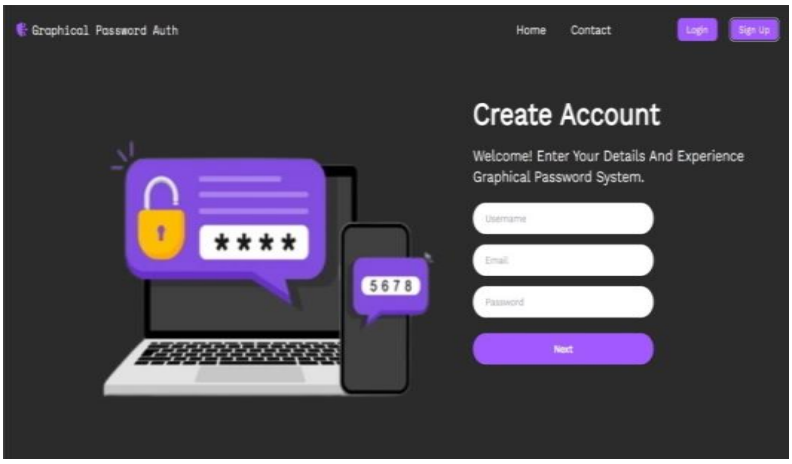
D. User Experience

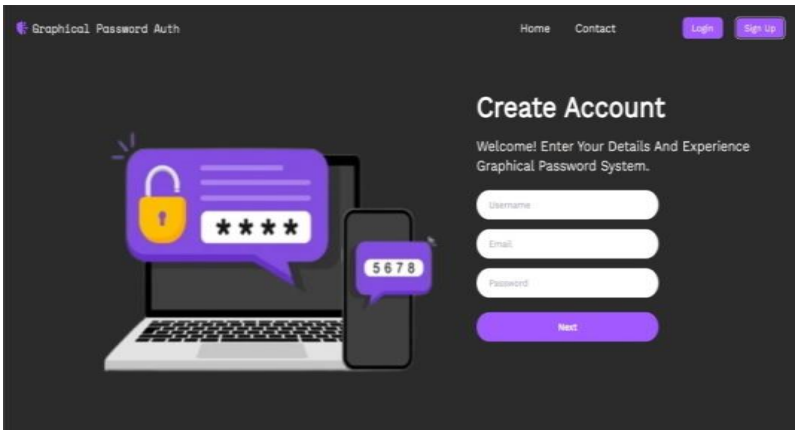
Explore the user experience of interacting with the graphical authentication system. Consider factors such as learnability, memorability, and satisfaction.

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

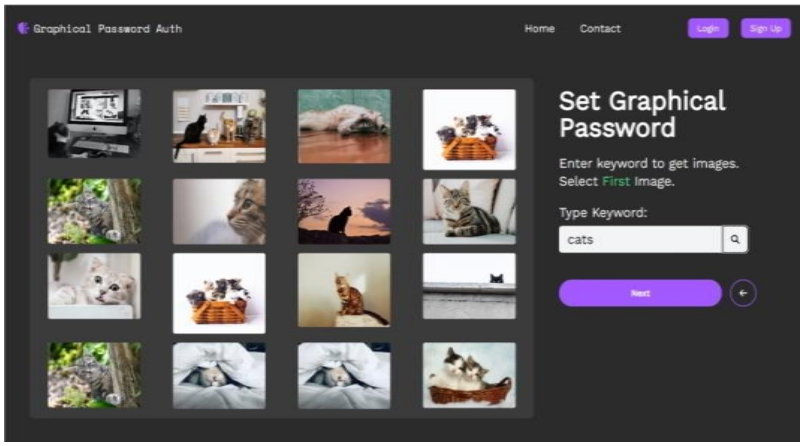
Figure 2: A sample line graph using colours which contrast well both on screen and on a black-and-white hardcopy

VI. HARDWARE AND SOFTWARE DIAGRAMS


Graphical Password Auth
Home
Contact
Login
Sign Up
Create Account
Welcome! Enter Your Details And Experience Graphical Password System.
Username
Email
Password
Next
****
5678


Graphical Password Auth
Home
Contact
Login
Sign Up
Create Account
Welcome! Enter Your Details And Experience Graphical Password System.
Username
Email
Password
Next
****
5678


Graphical Password Auth
Logged In!
Home
Contact
prathamesh
Logout
Discover Graphical Password Authentication
A Novel Approach For Security And User Experience Of Graphical Password Authentication.
Know More



VII. KEY FEATURES

A. Homepage

This would be the main interface where users can access various functions and features of the system. It may include options for logging in, accessing user accounts, and navigating to different sections of the system.

B. Login Page

The login page is where users provide their credentials (username and password) to access the system. It's crucial for security and authentication purposes. The login page may also include features

C. Homepage

This would be the main interface where users can access various functions and features of the system. It may include options for logging in, accessing user accounts, and navigating to different sections of the system.

D. Login Page

The login page is where users provide their credentials (username and password) to access the system. It's crucial for security and authentication purposes. The login page may also include features like password recovery and account registration for new users.

E. Privacy Measures

Implementation of privacy filters or techniques to prevent unauthorized users from observing login credentials during shoulder surfing attempts.

F. User Awareness

Providing users with guidance on how to protect their Credentials from shoulder surfing attacks, such as by being aware of their surroundings and shielding their input from prying eyes.

G. Multi-factor Authentication (MFA)

Adding an extra layer of security beyond passwords, such as SMS verification codes or biometric authentication, to further protect user accounts.

VIII. CONCLUSION

Because of their poor efficiency, current PIN authentication techniques that are resistant to shoulder-surfing attacks are not very usable. Recently, touchscreen devices that offer localised tactile feedback (LTF) have been created, patented, and/or put into use. It appears likely that touchscreen devices that support LTF will soon be widely accessible. Here, we've introduced Vpoints PES, an effective PIN authentication technique that is immune to shoulder-surfing assaults and can be used in a variety of user authentication systems, including cloud authentication systems.

IX. REFERENCES

[1]. Efficient Shoulder Surfing Resistant PIN Authentication Scheme Based on Localized Tactile Feedback, Wei-Chi Ku,HaoJun Xu,2019.

[2]. “Directional Based Graphical Authentication Method with Shoulder Surfing Resistant”, Noor Ashitah Abu Othman,2018.

[3]. “CRASH-CuedRecall Authentication resistant to Shoulder Surfing attack”, Sruthi P V, 2015.

[4]. “A Shoulder Surfing Resistant Technique for Login on Mobile Devices”, Eram Fatima ,Mohd Ashfaq , AfrahNazir , Muneeb Hasan Khan , M. Sarosh Umar, 2018.

[5]. “Scalable Shoulder Surfing Resistant Textual-Formula Base Password Authentication System”, Muhammad Shakir, Abdul Ayaz Khan,2010.

[6]. “Graphical Password: Shoulder-surfing Resistant using Falsification”, Andrew Lim CheeYeung, Bryan Lee WengWai, Cheng Hao Fung, Fiza Mughal, Vahab Iranmanesh,2015.

[7]. “Pass Neighbor:A Shoulder Surfing Resistant Scheme”, Swaleha Saeed, M Sarosh Umar,2016.

[8]. “A Novel Shoulder-Surfing Resistant Graphical Authentication Scheme”, Misbah Urrahman Siddiqui, Mohd. Sarosh Umar, Miftah Siddiqui, 2018.

[9]. K. S. Gaikwad and S. B. Waykar, "Detection and Removal Of Node Isolation Attack In OLSR Protocol Using Imaginary Nodes with Neighbour Response in MANET," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017, pp. 1-5, doi: 10.1109/ICCUBEA.2017.8463762.

[10]. Swapnali, L., Megha, J., Ranjeet, S., Belsare, P. P., & Ashwini, G. B. (2017). A Cryptographic Key Generation on a 2D Graphics Using RGB Pixel Shuffling and Transposition. In Proceedings of the International Conference on Data Engineering and Communication Technology: ICDECT 2016, Volume 2 (pp. 189-196). Springer Singapore.

[11]. Karve, S. M. ., Kakad , S. ., Swapnaja Amol, Gavali, A. B. ., Gavali , S. B. ., & Shirkande, S. T. . (2024). An Identification and Analysis of Harmful URLs through the Application of Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 12(17s), 456–468. Retrieved from https://www.ijisae.org/index.php/IJISAE/article/view/4905

[12]. Nalawade, V. S., Jadhav, O. D., Jadhav, R. M., Kargal, S. R., &Panhalkar, N. S. (2023). A Survey On Creating Digital Health Ecosystem with Lifewellness Portal Including Hospital and Insurance Company with Cloud Computing and Artificial Intelligence.

[13]. Ekatpure, J. N., Jadhav, P., Gavali, R., Kale, P., & Padasalkar, S. (2023). Pharmaceutical Data Optimisation Using Quantum Machine Learning.

[14]. Ekatpure, J. N., Kharade, N., Korake, D., Kshirsagar, D., & Mind, R. (2023). JPEG Vigilant: AI-Powered Malware Image Detection.