

GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

¹Mr. Dr.CH.V. PHANI KRISHNA, ²BADIKELA LIKHITHA ,

³CHENNUPALLI YASHWANTH SAI, ⁴EDAM BHARGAV SAI.

¹Professor, Teegala Krishna Reddy Engineering College, Hyderabad.

^{2,3,4}B,tech scholar, Teegala Krishna Reddy Engineering College, Hyderabad.

Abstract

Graphical password authentication systems signify a contemporary evolution in user verification, shifting away from traditional alphanumeric passwords towards image-based authentication. This novel method involves users engaging with an image grid, replacing the act of typing a password.

The limitations of alphanumeric passwords, being either susceptible to hacking or challenging for users to memorize, have spurred the development of modern, more memorable secret phrase authentication systems. However, these newer methods come with their own vulnerabilities, susceptible to brute-force and phishing attacks.

The conventional username-password authentication systems, while widely used, exhibit various weaknesses that render them susceptible to security breaches and attacks. The dichotomy between the vulnerability of alphanumeric passwords and the drawbacks of modern, easily memorable authentication methods underscores the ongoing pursuit of more robust and user-friendly authentication systems.

1. INTRODUCTION

1.1 PROBLEM STATEMENT

Design a graphical password authentication system using images where users select and arrange a set of personalized images in a specific sequence to gain access, enhancing security and user engagement compared to traditional text-based passwords.

1.2 OBJECTIVES

The objective of this project:

- Develop a Robust Graphical Password Authentication System
- Enhance User Experience and Usability
- Mitigate Security Vulnerabilities

1.3 MOTIVATION

The need to address the limitations of traditional alphanumeric passwords. Alphanumeric passwords are often challenging to remember and susceptible to various security risks. By exploring graphical password authentication, which leverages the human brain's ability to

recall images better than text, this project aims to create a more secure, user-friendly, and memorable authentication system. The goal is to enhance user experience, reduce security vulnerabilities, and promote a safer and engaging approach to user authentication in the digital age.

1.4 STRUCTURE

The modern digital landscape demands a fundamental rethinking of user authentication methods, seeking a delicate balance between robust security measures and user-friendly experiences. This project serves as an expedition into the realm of graphical password authentication systems—an innovative departure from the conventional alphanumeric password paradigm. Amidst the vulnerabilities and limitations inherent in traditional password systems, the evolution towards graphical authentication signifies a paradigm shift, replacing the act of inputting passwords with the engagement of images within an interactive grid. This exploration aims to delve deeply into the evolution, strengths, vulnerabilities, and future trajectories of these novel authentication systems.

Systems like conventional password systems such as wordbased password system, graphical system are commonly used for authentication. But these systems are susceptible to dictionary attack, shoulder surfing attack, accidental login. Hence the word-based Shoulder surfing resistant graphical password schemes have been proposed. The shoulder surfing attack is an attack where illegal user can get authorized user's password by observing over his shoulder when he enters his password. Though, as most handlers are more aware with word-based passwords than graphical passwords.

The existing word-based shoulder surfing resistant graphical password systems are not secured and effective enough Another vulnerability attack regarding textual password is keyloggers. In Keyloggers any key pressed by the user is monitored by unauthorized users. A keylogger can be either software or hardware. By using Keylogger a person can steal the victim's personal information, transmission can be interrupted by hackers, it can prove very dangerous for people who are using online cash sites, or when they are typing their passwords. In various proposed system, the user can simply and efficiently login to the system without using any keyboard. It is very relaxed for the user to login. It has become very hard to guess the password because of text and color combination.

The systems provide extra security. Most of the authentication system now-a-days uses a combination of username and password for authentication. Due to the restriction of human memory, most users incline to select short or simple passwords which are easy to recall. Graphical passwords use images rather than word-based passwords and are comparatively

inspired by the fact that users can recall pictures more simply than a string of characters. A graphical password is an validation method where the user have to pick from images, in a certain order, accessible in a graphical user interface. Graphical passwords may provide improved security than word-based passwords because various individuals, in an attempt to remember word-based passwords, use basic words. In various proposed systems one time passwords are used for security purpose. An OTP is a set of characters that can act as a form identity for one time only. Once the password is used, it cannot be used for any extra authentication. Even if the hacker gets the password, it is possible that it was previously used once, as it was being conveyed, therefore unusable to the hacker. Another way used for providing increased security is session passwords. Session passwords are passwords that are used only once. When the session is completed, the session password is no more useful. For every single login procedure, users input dissimilar password.

2 . LITERATURE SURVEY

[1] In Dec 2009 author H. Gao proposed graphical password scheme using color login. In this color login uses background color which decrease login time. Possibility of accidental login is high and password is too short. The system developed by Sobrado is improved by combining text with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. The advantages of this system is that it reduces the login time, session passwords are also generated to improve security. The disadvantage of this system is that it the possibility of accidental login is high and password is too short.

[2] In this paper M. Sreelatha proposed Hybrid Textual Authentication Scheme. This scheme uses colors and user has to rate the colors in registration phase. During login phase four pairs of colors and 8*8 matrix will be displayed. As the color rating given by the user, the password will generate. First color shows row number and second shows column number of the grid. The drawback of this system is intersecting element is the first letter of the password. The user has to memorize the rating and order of the colors. So it becomes very hectic to user. The benefit of this system is that it is flexible and simple to use.

[3] A hybrid graphical password based method is advised, which is a mixture of recognition and recall based methods having many advantages as compare to existing systems and more suitable for the user. In this system the user draws the selected object which is then stored in the database with the specific username. Objects may be symbols, characters, auto shapes, simple daily seen objects etc. Then the user draws pre-selected objects as his password on a

touch sensitive screen with a mouse. Then the system performs preprocessing. Then after stroke merging, the system constructs the hierarchy then the next step is sketch simplification, then the three types of features are extracted from the sketch drawn by the user. The last step is called hierarchical matching. The plus point of this system is it's a combination of recognition and recall based technique, hence provides flexibility. This system performs some complex actions like pre-processing, stroke merging. So it can be a weakness of this system.

[5] Authors proposed a system in which password scheme uses colors and text for generating session password. They have introduced a session password scheme in which the passwords are used only once for each session and when session is completed the password is no longer in use. In this system two session password schemes pair-based textual authentication scheme and color code-based authentication scheme are introduced. In the pair based textual authentication scheme the user submits his password during the registration. The password should contain number of characters. When the user enters login an interface containing of a grid is showed during the login phase. The grid is of size 6 x 6 and it contains of alphabets and numbers. These are randomly placed on the grid and the interface changes every time. Depending upon the password which is submitted during the registration phase, user has to enter the password. Users have to consider his password in terms of pairs. In the color code based scheme, the user has to get his password with the help of colors. During registration phase, user should fill up all his information and also rate colors. The merit of this system is it provides much better security. Demerit of the system is sometimes users may consider wrong password as they are supposed to consider the password in terms of pair.

[6] Authors proposed a scheme which mainly focuses on shoulder surfing. In this system, they proposed a new clickbased color password scheme called Color Click Points (CCP). It can be viewed as a combination of Pass-Points, Pass faces, and Story. A password consists of one click-point per Color for a sequence of Colors. The next Color displayed is built on the previous click-point. In this proposed scheme, we propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system.

[7] Recent research has explored advanced authentication techniques integrated with graphical systems. Li et al. (2018) proposed a hybrid authentication method combining graphical passwords with biometric authentication to enhance security without compromising usability. Their study showcased promising results in improving the resilience of graphical systems against various attacks.

[8] Studies by Li and Li (2021) provided an overview of emerging threats targeting graphical password systems, including advanced phishing techniques and machine learning-based attacks. Moreover, ongoing research by Wang et al. (2022) focused on leveraging machine learning algorithms to enhance the robustness of graphical authentication against evolving cyber threats.

3 . SYSTEM DESIGN

3.1 Graphical password authentication design

The system design for “Graphical password authentication system” Each of these components forms a crucial part of the system's architecture and functionality, contributing to a seamless user experience and efficient system operation.

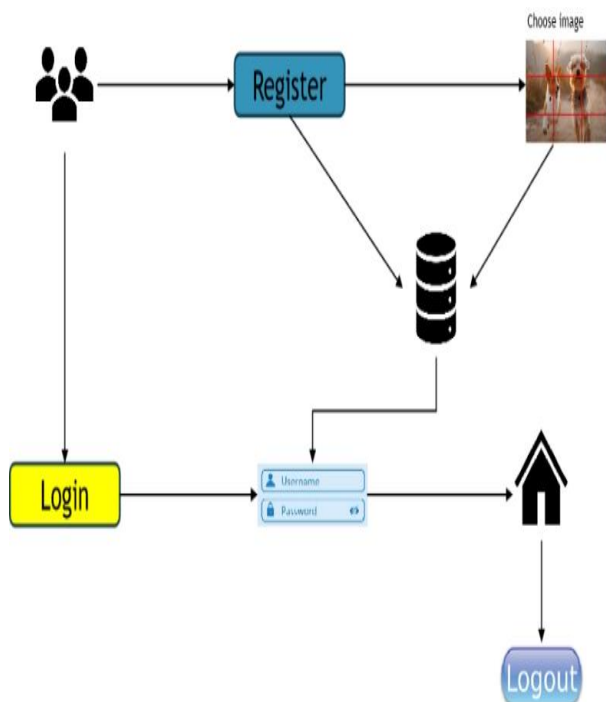


Fig 3.1 - Graphical password authentication design

User Management:

The system involves the management of user-related actions such as registration, login, and logout. This includes authentication processes and user session management.

Image and Pattern Selection:

This section pertains to the functionality where users can select images and patterns, possibly for profile customization or other features within the system.

Registration Process:

This outlines the steps and processes involved in user registration, including validation, storing user details in the database, and confirming successful registration.

Login Mechanism:

Details the login process, including user authentication, session establishment, and redirection to the homepage upon successful authentication.

Database Architecture:

The system relies on a database structure to store user information, images, patterns, and any other relevant data. This includes considerations for data storage, retrieval, and management.

Homepage Design and Functionality:

Describes the layout, features, and functionalities available on the homepage once a user successfully logs in. It may include personalized content, navigation options, and interactive elements.

Logout Functionality:

Explains the steps taken when a user initiates logout, such as clearing session data, logging out from the system, and redirecting to a designated page or login screen. Graphical password authentication systems (GPAS) offer a promising alternative to traditional text-based password authentication, employing images instead of characters to verify a user's identity. This approach aims to address the limitations of text-based passwords, which are vulnerable to guessing attacks, shoulder surfing, and memorability issues.

One of the primary advantages of GPAS lies in its enhanced security. Unlike text-based passwords, which can be easily guessed or stolen, images provide a larger and more complex information space, making it significantly more difficult for an attacker to crack a user's password. Additionally, GPAS are less susceptible to shoulder surfing, as users do not need to enter their passwords in plain text.

3.2 UML DIAGRAMS

A Unified Modeling Language (UML) diagram is a visual representation of a system or software application. It can be used to model the structure, behavior, and interactions of a system. UML diagrams are used to improve communication, reduce errors, and increase productivity. They are also supported by many software development tools, which makes it easy to create and share them with others. Some of the benefits of using UML diagrams include improved communication, reduced errors, increased productivity.

UML diagrams are a standardized way of representing the structure, behavior, and interactions of a software system or other complex system. They are created using a set of graphical

symbols and notations, and they can be used to communicate design ideas, document requirements, and generate code.

Overall,UML diagrams are a valuable tool for software engineers and system analysts. They can be used to improve communication, reduce errors, increase productivity, and improve understanding of complex system

3.2.1 CLASS DIAGRAM

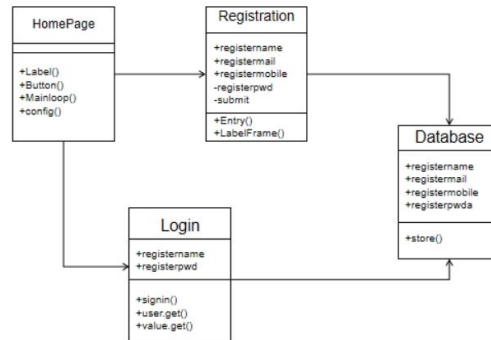


fig 3.2.1- Class Diagram

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains which information.

3.2.2 USECASE DIAGRAM

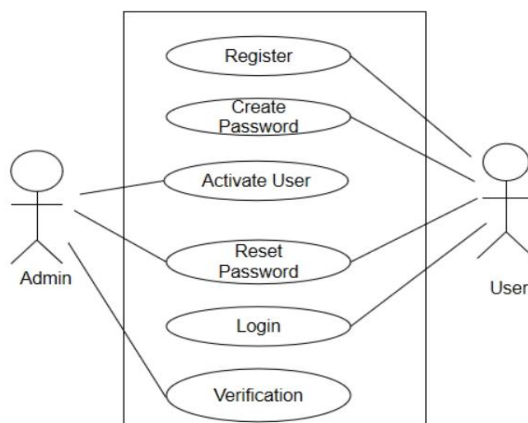


fig 4.2.2-Usecase Diagram

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview

of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases.

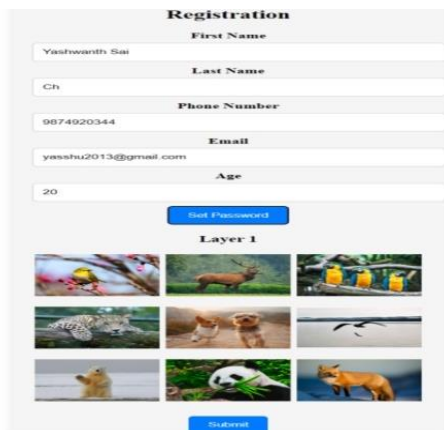
4 . OUTPUT SCREEN

4.1 Homepage -



SS 4.1- Homepage

4.2 Registration –



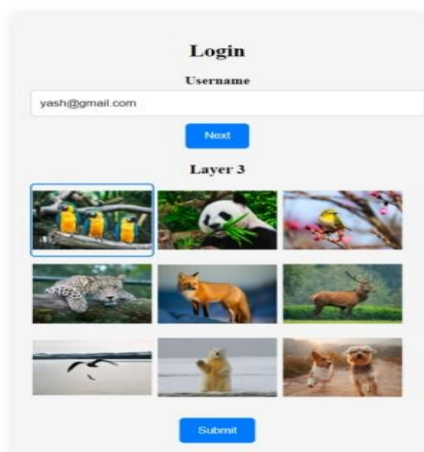
SS 4.2.1 – Registration



The registration form is titled "Registration" and contains the following fields: "First Name", "Last Name", "Phone Number", "Email", and "Age". Below these fields is a "Next" button. Underneath is a "Layer 1" image verification section with a 3x3 grid of images showing a brown deer. A "Submit" button is located at the bottom of the grid.

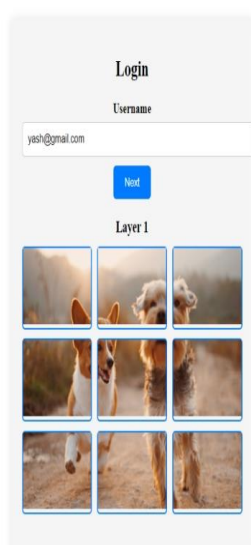
SS 4.2.2 - Registration Pattern

4.3 Login –



The login form is titled "Login" and has a "Username" field containing "yash@gmail.com". Below the field is a "Next" button. Underneath is a "Layer 3" image verification section with a 3x3 grid of images showing various animals like birds, a panda, a tiger, a fox, a deer, a bird, a seagull, a bear, and a dog. A "Submit" button is located at the bottom of the grid.

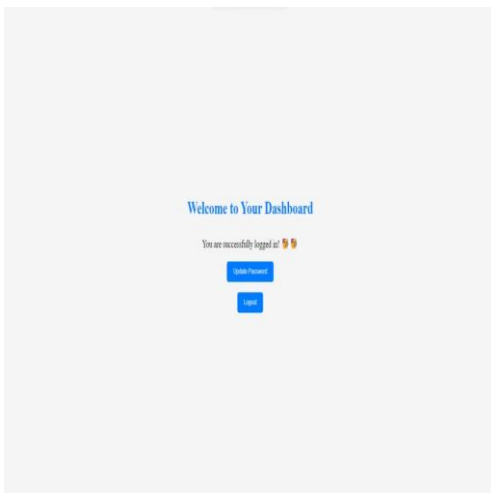
SS 4.3.1 – Login



The login form is titled "Login" and has a "Username" field containing "yash@gmail.com". Below the field is a "Next" button. Underneath is a "Layer 1" image verification section with a 3x3 grid of images showing a white dog's face. A "Submit" button is located at the bottom of the grid.

SS 4.3.2 - Login Pattern

4.4 Dashboard -



SS 4.4.1 --Dashboard

5 . CONCLUSION

In the realm of digital security, user authentication stands as the guardian of one's digital assets and privacy. However, traditional authentication methods involving textual passwords or PINs often fall prey to shoulder surfing attacks, particularly in public settings. The vulnerability arises from the need to physically input these passwords, leaving them susceptible to exposure through visual interception or recording devices. To address this critical vulnerability, our proposal introduces a novel approach - a Graphical Password Authentication System leveraging image patterns instead of traditional alphanumeric codes. By harnessing a color schema, our system offers a visually intuitive and robust alternative to conventional textual passwords, mitigating the risks associated with shoulder surfing attacks. This graphical authentication paradigm not only enhances security but also provides users with a more user-

friendly and secure means of accessing their digital assets, ensuring confidentiality and safeguarding against unauthorized access.

6 . FUTURE ENHANCEMENTS

• **Multi-Factor Authentication (MFA):**

Implement a multi-factor authentication approach that combines graphical passwords with other authentication factors like SMS codes, email verification, or hardware tokens to enhance security..

• **Machine Learning and Behavioral Analysis:**

Utilize machine learning algorithms to analyze user behavior and patterns when creating graphical passwords. This can help detect anomalies or suspicious activities, adding an additional layer of security

7. REFERENCES

- 1.Abhijith S, Soja Sam, Sreelekshmi K U, T T Samjeevan, Sneha Mathew, 2021, Web based Graphical Password Authentication System, international journal of engineering research & technology (ijert) iccidt – 2021
- 2.Graphical Password Authentication. Shraddha M. Gurav Computer Department Mumbai University RMCET Ratnagiri, India. Leena S.Gawade Computer Department Mumbai University RMCET Ratnagiri, India, 2014 IEEE.
- 3.Design and implementation of a graphical password authentication system using persuasive cuedClick point in cloud computing , SRM University, India, may 2013.
- 4.Enhancement of Password Authentication System Using Graphical Images. Amol Bhand,Vaibhav desale Savitrybai Phule Pune University, Swati Shirke Dept.of Computer Engineering NBN Sinhgad School of Engineering, Pune, Dec 16-19, 2015
- 6.Eugene H. Spafford. Observing reusable password choices. In Proceedings of the 3rd Security Sympo- sium. Usenix, pages 299–312, 1992.
7. Sigmund N. Porter. A password extension for improved human factors. Computers & Security, 1(1):54– 56, 1982.
- 8.Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages 463–472, 2005.



9. Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*, 63:128–152, July 2005.
10. Real User Corporation. The science behind passfaces, June 2004.
11. G. E. Blonder. Graphical password. U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995
12. Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63:102–127, July 2005.
13. Robert Morris and Ken Thompson. Password security a case history. *Communications of the ACM*, 22:594–597, November 1979