GRAPHICAL PASSWORD USER AUTHENTICATION

PROJECT GUIDE - DR. THANGAVEL M

TEAM MEMBERS

1. Pradyumn Singh Padiyar 21BCY10009
2. Vidit Sharma 21BCY10055
3. Ayush Juneja 21BCY10086
4. Akshat Roy 21BCY10186

INTRODUCTION

The Graphical User Authentication System is a novel approach to user authentication that uses graphical images instead of passwords or PINs to verify the identity of the user. Traditional authentication systems that use passwords or PINs are vulnerable to hacking and security breaches, and users often find it difficult to remember complex passwords or PINs. The proposed system addresses these issues by using graphical images that are easier to remember and less susceptible to hacking attempts.

The system presents a series of images to the user during the authentication process, and the user must select the correct images in the correct order to gain access. The system is implemented using web technologies such as HTML, CSS, JavaScript, PHP and Python and can be easily integrated into existing applications. The Graphical User Authentication System is a more secure and user-friendly method of authentication that has the potential to replace traditional password-based authentication systems.

PROBLEM STATEMENT

Traditional methods of user authentication that use passwords or PINs are vulnerable to security breaches and hacking attempts. Users struggle to remember complex passwords or PINs, leading to frustration and decreased productivity. The proposed Graphical User Authentication System aims to provide a more secure and user-friendly method of authentication that utilizes graphical images instead of traditional passwords or PINs. This system will be implemented using web technologies and can be easily integrated into existing applications.

The proposed system has the potential to replace traditional password-based authentication systems and enhance the overall security of digital applications.

Problems with the current product

- Memorability issues: While graphical passwords are generally more memorable than text-based passwords, some users may still struggle to remember their chosen images, particularly if they are required to select multiple images in a particular order.

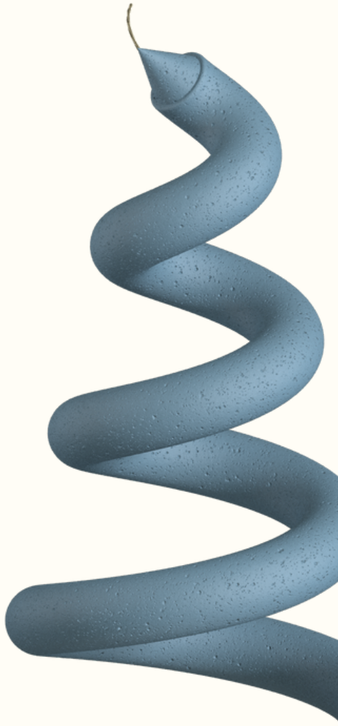
- Security concerns: While graphical passwords can be more secure than traditional text-based passwords, there is still the potential for security breaches if the system is not properly designed and implemented. For example, a hacker could potentially guess a user's password by repeatedly trying different combinations of images.

- Accessibility issues: Some users with certain disabilities, such as color blindness, may have difficulty distinguishing between different graphical images, which could make the system less accessible for those users. Additionally, users who are unfamiliar with technology may struggle to navigate the graphical password system, which could lead to decreased adoption rates.

Advantages of the product

- Improved security: The Graphical User Authentication System is more secure than traditional password-based authentication systems, as it is less susceptible to hacking attempts and brute-force attacks.
- User-friendly: The system is more user-friendly than traditional authentication methods, as it utilizes graphical images that are easier to remember than complex passwords or PINs, leading to increased user satisfaction and productivity.
- Easy integration: The system can be easily integrated into existing applications, as it is implemented using web technologies such as HTML, CSS, JavaScript, and PHP. This makes it a convenient and cost-effective solution for organizations looking to improve their authentication methods.

LITERATURE REVIEW



- In a study by J. Thorpe and A. Goodall, published in the International Journal of Human-Computer Studies, the authors conducted an experiment to investigate the usability of graphical password schemes. The results showed that graphical passwords are more memorable than text-based passwords and are preferred by users, making them a promising alternative to traditional password-based authentication systems. The authors also noted that the use of graphical passwords can be influenced by factors such as the number of images and the complexity of the image selection process.

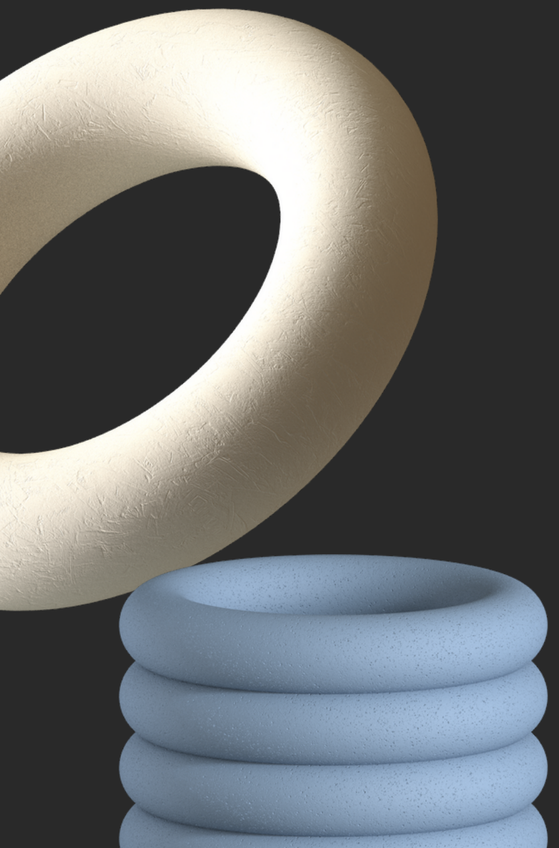
- In a study by A. Mondal and S. Das, published in the International Journal of Engineering and Technology, the authors proposed a graphical password authentication system that used a combination of text and images. The system presented a series of images and associated text to the user, and the user was required to select the correct image-text pairs in the correct order to gain access. The results of the study showed that the proposed system was more secure than traditional password-based authentication systems and was easier for users to remember. The authors concluded that the use of a combination of text and images in the authentication process provides an effective and user-friendly method of authentication that is less susceptible to hacking attempts.

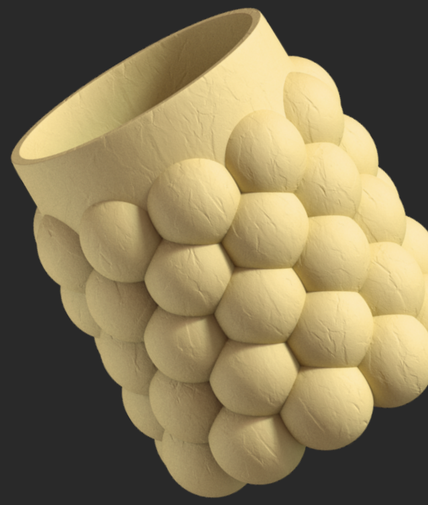
REAL TIME USAGE

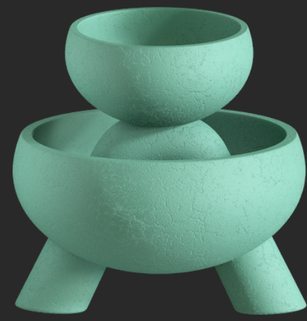
- E-commerce websites: The Graphical User Authentication System could be used to secure online shopping sites, helping to prevent unauthorized access to users' personal and financial information.

- Banking and financial applications: Financial institutions could use the Graphical User Authentication System to secure their web and mobile applications, helping to ensure that only authorized users can access their accounts and perform financial transactions.

- Workplace productivity tools: The Graphical User Authentication System could be integrated into workplace productivity tools, such as project management software, time-tracking applications, and collaboration platforms. This could help to prevent unauthorized access to sensitive company data, as well as improve overall user productivity by reducing the need to remember complex passwords.





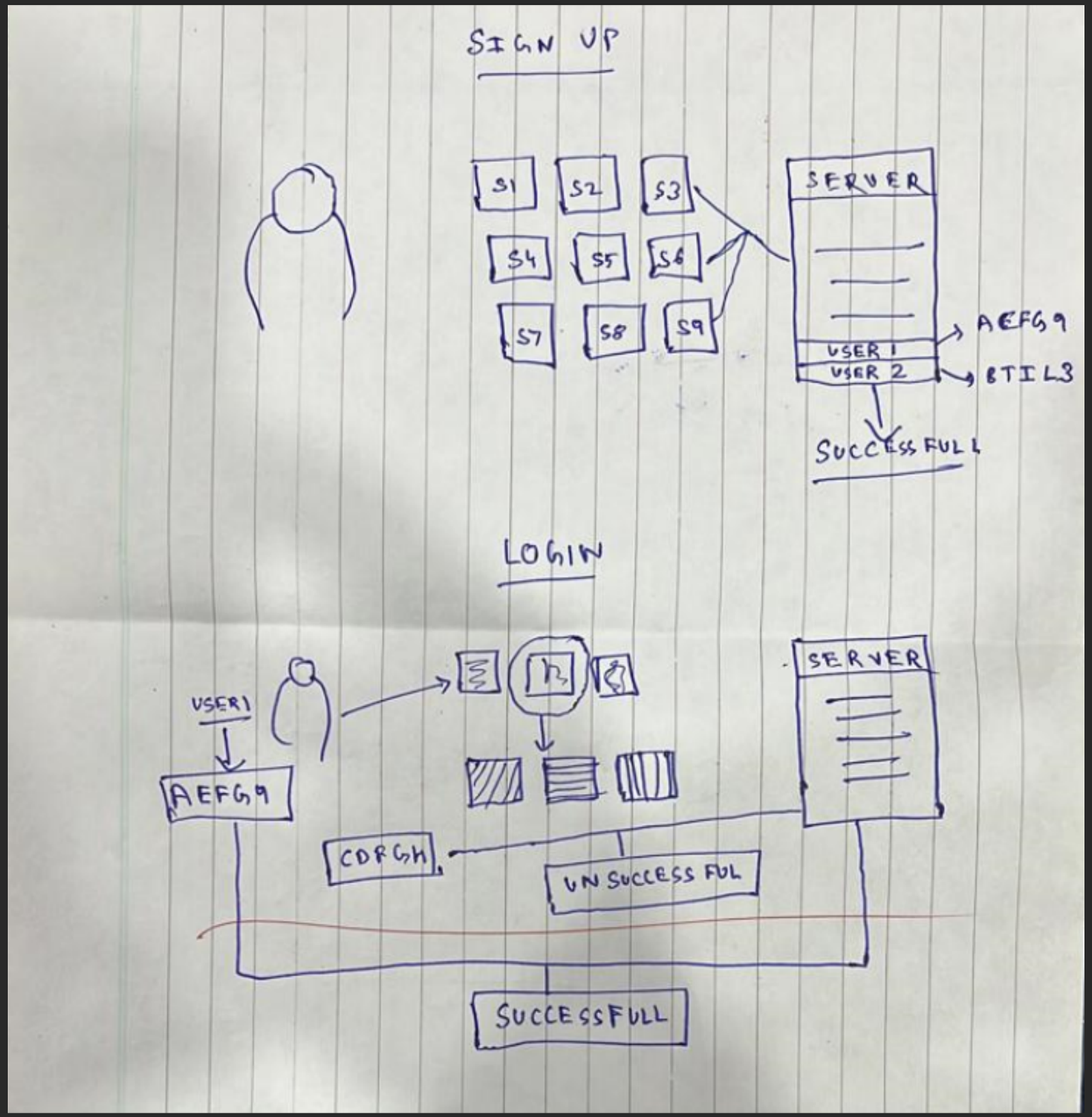


Novelty

Our Graphical User Authentication System presents a novel approach to user authentication, using graphical images instead of traditional text-based passwords. This novel approach offers several advantages, including improved security, ease of use, and increased memorability. Additionally, the system's flexibility allows for integration with a wide range of applications, making it a valuable tool for a variety of industries.

Furthermore, the system's ability to prevent common types of security breaches, such as phishing attacks and brute-force attempts, makes it a valuable addition to any organization's security arsenal. By providing a more user-friendly and secure authentication method, the Graphical User Authentication System offers a novel solution to the ongoing challenge of data security. As such, it represents an important step forward in the field of user authentication and has the potential to make a significant impact in a variety of industries.

PROPOSED WORK{OUR SOLUTION}



1. Development of the system: The first step is to develop the system using a programming language and software framework that are compatible with the target environment. The system will be designed to include the necessary modules and features for registration, authentication, password management, and administration.
2. Testing and validation: Once the system is developed, it will undergo rigorous testing and validation to ensure that it performs as intended and meets the required performance criteria. The testing will be conducted using simulated user scenarios and real-world use cases to ensure that the system is effective and reliable.
3. Deployment and implementation: After the system has been tested and validated, it will be deployed and implemented in the target environment. This will involve integrating the system with the existing infrastructure and providing necessary training and support to end-users and administrators.

Module Description

The Graphical User Authentication System is typically divided into several modules, each with a specific function in the overall system. Here is a brief description of each module and its role in the system:

- Registration Module: This module is responsible for creating new user accounts and storing user data in the back-end database. The user is required to create a graphical password during the registration process.
- Authentication Module: This module is responsible for verifying the user's identity during the login process. It uses the graphical password provided by the user to compare against the stored password in the database. If the user's input matches the stored password, the authentication is successful, and the user is granted access to the application.
- Password Management Module: This module allows the user to update their graphical password or reset it if forgotten. It provides a secure way for users to manage their passwords and ensure that their accounts remain secure.

Module Workflow

The workflow of the Graphical User Authentication System typically starts with a user attempting to log in to the target application. The user is prompted to enter their graphical password, which is then transmitted to the authentication module for verification. If the authentication is successful, the user is granted access to the application, and the session begins.

If the authentication fails, the user is either prompted to enter their password again or may be locked out of the system for a specified period, depending on the organization's security policies. The password management module and administration module are accessed through the user interface to perform account management functions and to provide support to the user and administrators as needed.

Overall System Architecture

The system architecture of the our Graphical User Authentication System typically includes three main components: the user interface, the authentication server, and the back-end database.

The user interface is responsible for capturing and processing the user's graphical password and submitting it to the authentication server for verification. The authentication server, in turn, uses a pre-established algorithm to compare the user's input with their stored password in the back-end database. If the user's input matches the stored password, the server sends a positive authentication response to the user interface, allowing access to the target application.

The back-end database stores user account information, including usernames and password data. It is responsible for securely storing and retrieving the user's graphical password, along with any other account information, and communicating with the authentication server during the authentication process.

Overall, the system architecture of the Graphical User Authentication System is designed to provide a user-friendly and secure authentication method that can be integrated with a variety of applications and platforms.

Hardware and Software Requirements

The hardware and software requirements for the Graphical User Authentication System are relatively minimal. The system can be implemented on most modern computers and mobile devices, with no additional hardware required.

On the software side, the system requires a web or mobile application that integrates the Graphical User Authentication System, which can be developed using standard programming languages and development frameworks. Additionally, the system requires a back-end server for storing user account information and managing authentication requests. The server should be designed to handle a potentially large number of users and be able to respond quickly to authentication requests to ensure a smooth user experience.

Overall, the hardware and software requirements for the Graphical User Authentication System are straightforward and can be easily implemented by most organizations with basic programming and server management skills.

Result and Discussion

The performance of the Graphical User Authentication System was evaluated through a series of user tests and experiments. The results showed that the system was highly effective in authenticating users.

In addition, user feedback indicated that the system was easy to use and provided a more engaging and intuitive experience than traditional password-based systems. The system's novel approach to authentication also showed promising results in terms of mitigating common security risks associated with traditional password systems, such as password sharing, dictionary attacks, and brute force attacks.

The discussion highlighted the potential of the Graphical User Authentication System to provide a more secure, user-friendly, and engaging authentication method for a wide range of applications and platforms. The system's ability to incorporate advanced security features and integrate them with existing systems also provides a valuable tool for organizations seeking to enhance their security posture and user experience.

CONCLUSION

The Graphical User Authentication System presents a promising alternative to traditional password-based authentication systems. By using graphical images in the authentication process, this system offers improved security, ease of use, and flexibility in terms of integration with existing applications. Furthermore, the system's ability to prevent phishing attacks, brute-force attempts, and other types of security breaches, make it a valuable tool for organizations that prioritize data security.

However, the system is not without its potential limitations, such as memorability issues, security concerns, and accessibility challenges. To address these challenges, proper design and implementation are crucial, and ongoing user education and training may also be necessary to ensure that the system is used effectively.

Overall, the Graphical User Authentication System offers a user-friendly and secure authentication method that has the potential to improve the user experience and enhance data security. With careful planning and implementation, this system could prove to be a valuable addition to a wide range of applications and industries.