GRAPHICAL PASSWORD AUTHENTICATION SYSTEM USING DJANGO FRAMEWORK

Nishat Fathima[1], Dr. Mohammed Pasha[2], Dr. K. Palani[3]
[1]PG Scholar, Department of CSE, fathimanishat23@gmail.com
[2]Asst Professor, Department of IT, muhammed.pasha@gmail.com
[2]Asst Professor, Department of CSE, principalswcet2020@gmail.com
Shadan Women's College of Engineering and Technology, Hyderabad, India

ABSTRACT
One essential element of information security is user authentication. Alphabetic passwords are the most widely used & widely accepted form of user authentication. However, employing alphanumeric authentication techniques has a number of disadvantages. This project uses the Django Framework (DF) to demonstrate a graphical password authentication scheme. It provides resistance against a few common attacks. Test-based passwords may not offer as much protection as graphical passwords.
Keywords- Graphical Password Authentication, Alphanumeric, Django Framework

I. INTRODUCTION

Considering how digital security is changing, it is becoming more widely accepted that standard alphanumeric passwords are weak & challenging to remember. A potential substitute is provided by Graphical Password Authentication Systems (GPAS), which authenticate users using graphical graphics rather than alphanumeric characters. This novel method makes use of the human brain's exceptional capacity for visual recognition & recall, which can greatly improve authentication processes' security & usability.

Cognitive science provides evidence that humans have a better visual recall than they do for textual information, which is the basis for graphical passwords. This innate capacity makes it easier for users to remember & correctly recall images, which lowers the possibility that passwords will be forgotten. Graphical passwords are more in line with innate human cognitive abilities than text-based passwords, which can be difficult to remember & frequently force users to turn to unsafe actions (such writing them down or employing readily guessed passwords).

GPAS is effective in two ways: it increases security & user experience simultaneously. From a security perspective, graphical passwords can lessen a number of typical risks connected to conventional passwords, including key logging, phishing, & brute force assaults. Additionally, consumers find the login procedure to be less confusing & more intuitive when graphical passwords are used. Because graphical passwords are so easy to use, adoption rates may be higher & security procedure compliance may be better.

Using graphical passwords offers strong protection against numerous common security risks. Graphical passwords are more difficult to guess or duplicate due to their uniqueness & complexity. Furthermore, these systems frequently ask users to choose a series of photographs in a precise order or to identify specific spots within an image, making it much harder & take longer to try unauthorized access.

II. LITERATURE SURVEY

Graphical Password Authentication: A Survey, M. T. A. S. Rahman, A.H. Abdullah & S. Y. N. H. Hossain, 2021.

As a potential replacement for alphanumeric passwords, graphical password authentication aims to improve both security & user experience. This report offers a thorough examination of several graphical password authentication methods, classifying them into three categories: hybrid, recognition-based & recall-based. The study looks at these strategies' security & usability, assessing how well they withstand brute force, guessing & shoulder surfing attacks. The survey also emphasizes the drawbacks & difficulties using graphical passwords & provides information on possible remedies & future lines of inquiry. This work attempts to contribute to the development of more secure & user-friendly graphical password systems by synthesizing existing literature.

A Survey on Graphical Password Authentication, Atif M. Memon & Tae Lee Hwang, 2020.

Because they have the potential to improve both security & usability, GPAS have drawn a lot of attention as an alternative to conventional text-based passwords. The most recent graphical password techniques are reviewed in-depth in this survey & are divided into three categories: recognition-based, recall-based, & hybrid systems. We evaluate the advantages & disadvantages of every category, looking at how well-defended they are against different types of attacks including phishing, guessing & shoulder surfing. We also examine usability concerns, such as user acceptability & memorability, and talk about the consequences for practical application. The study ends with a discussion of potential future research areas, emphasizing the necessity of better security protocols & graphical password systems with user-friendly designs.

A New Scheme of Graphical Password Authentication, X. Li, Y. Wang & Z. Xu, 2019.

In order to improve security & usability, a novel graphical password authentication technique is

proposed in this study. The suggested plan combines aspects of recall- & recognition-based strategies to produce a hybrid system that benefits from each approach's advantages. We present novel approaches to counter typical vulnerabilities like password reuse, guessing attacks & shoulder surfing. Our security research reveals that our scheme offers strong protection against multiple attack vectors, while usability evaluations show that it is simple to use & learn. With this new method, the shortcomings of the current graphical password systems will hopefully be addressed & a workable and safe substitute for conventional text-based authentication techniques will be provided.

A Survey of Graphical Password Techniques, Muhammad Hussain, Mazhar Khan & Mohamed Elhoseny, 2018.
Due to the drawbacks of conventional password systems, including their poor usability, vulnerability to dictionary attacks & susceptibility to phishing, graphical passwords have been suggested as a possible replacement for text-based passwords. This survey offers a thorough analysis of the numerous graphical password strategies, classifying them into distinct groups according to their layout & ease of use. The study assesses the advantages & disadvantages of each method, talks about how resilient they are to frequent attacks & suggests future lines of inquiry to increase their efficacy & security. The intention is to present a comprehensive overview of the state of the art in graphical password research & discuss its useful applications for enhancing authentication systems.

III. PROBLEM ANALYSIS

A Existing System

Users enter the application's login screen to begin the login procedure for the graphical password authentication system. Users are prompted to enter their email address or username in a specified field on this page. After that, users utilize the keyboard to enter their password. A combination of alphanumeric letters & special symbols may be used in the password; however, special symbols are not as important for this authentication procedure.
After entering their password & username (or email address), users click the Login button to submit their information. After receiving the login request, the server checks the username & password entered against the information that has been saved in the SQL Database. Using a database query, the validation process retrieves the credentials that are stored for the specified username & compares them with the password that was entered.
The server directs the user to their account dashboard, where they can access their personalized account features & data, provided that their credentials match & the validation process is successful. On the other hand, the server generates an error message stating that the "Username & password is wrong" if the validation fails The user is then prompted to reenter their credentials or fix any errors by seeing this message. This preserves the application's security & integrity by guaranteeing that only authorized users can access the system.because the username or password is incorrect.

B Proposed System

By incorporating a multi-layered authentication method, the suggested solution for the graphical password authentication project aims to improve both security & user experience. Users of the system will be able to log in using their credentials—a username or email address & a password—using a web-based interface that is available through ordinary web browsers.
Users will enter their email address or username on the login screen, followed by their password which can be any combination of special characters & alphanumeric characters after logging in. Upon selecting the Login button, a validation procedure will be started by the system. In order to retrieve & compare the stored credentials with the ones that were submitted, the server must query the SQL Database. This validation procedure is managed by the authentication module, which is a component of the Django Application (DA) running on the web server.
Users will be taken to their personal account dashboard, where they can access services & features that are specifically designed for them, if the credentials are properly validated. In the event that authentication is unsuccessful, users will be directed to amend their input with a clear & straightforward error notice stating that their "Username & password is wrong."
The system will also include account management & password reset capabilities. If a user needs to reset their password, they can do so through the system, which will create & transmit a reset link to the user's registered email address. To manage user accounts, keep an eye on system performance & supervise authentication procedures, administrators will have access to an admin interface.
The overall goal of the suggested system is to offer a safe & easy-to-use authentication method, all the while guaranteeing strong administrative control & effective management of user credentials & sessions.

IV. SYSTEM ARCHITECTURE

The graphical password authentication project's system architecture aims to offer administrative management, an easy-to-use user interface & a reliable and secure authentication method. The client side, server side & admin side comprise the three primary parts of the architecture.

Client Side:

On the client side, users use a Web Browser on their User Device to communicate with the system. The online application is accessed through the browser, where users can authenticate by entering their graphical

passwords. The graphical password entry fields & other user-facing components are displayed on the client side.

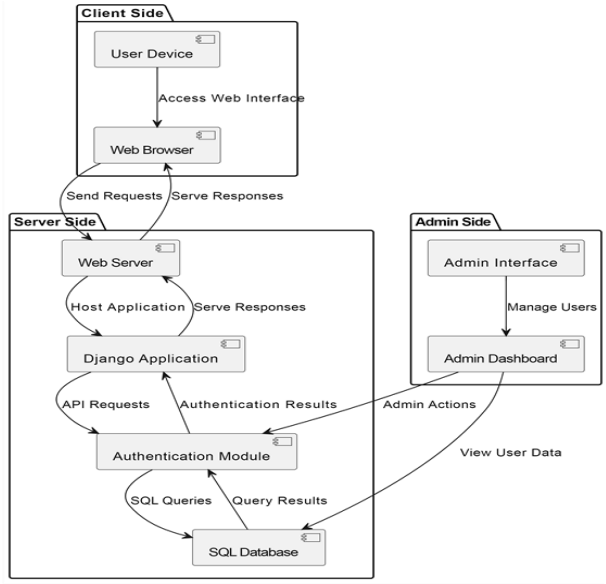


Figure 1: System Architecture

Server Side:
The main functionality of the application is located on the server side. It consists of the following elements:

- **Web Server**: This server handles client HTTP requests & hosts the application. It is in charge of managing the first exchange of information between the client & the application as well as serving the web pages.

- **DA**: This is the web server's primary application framework. It was created with the DF & manages application state, user requests & business logic. The DA manages the communication between the several modules, processes incoming requests & calls the required authentication procedures.

- **Authentication Module**: This part is in charge of the graphical password verification procedure. It processes requests for password resets, verifies user credentials & tracks unsuccessful login attempts. The authentication module retrieves user data & updates records as needed by interacting directly with the **SQL Database**.

- **SQL Database**: User credentials, session data & other application data are kept in the database. The authentication module queries it in order to verify passwords, update user information & preserve the accuracy of authentication procedures.

- **Admin Side:**

Administrative oversight & functions are provided by the administration side:Es.

- **Admin Interface**: This is a different interface made specifically for application management by administrators. It has features & tools for managing users, keeping an eye on system performance & adjusting application settings.

- **Admin Dashboard**: This dashboard, which is accessible via the admin interface, enables administrators to manage user accounts, see comprehensive user data & take care of administrative responsibilities pertaining to system settings & authentication. To carry out these functions, it communicates with the SQL database & the authentication module.

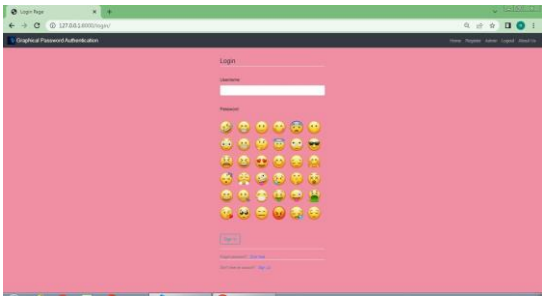
The system architecture offers extensive administration capabilities & guarantees a smooth & safe user experience. Users connect to the system using web browsers, which exchange data with the DA & the web server. To handle authentication & other functions, the application communicates with the database & authentication module. The administrative side makes it easier to monitor & supervise the system's operation.

V. RESULT

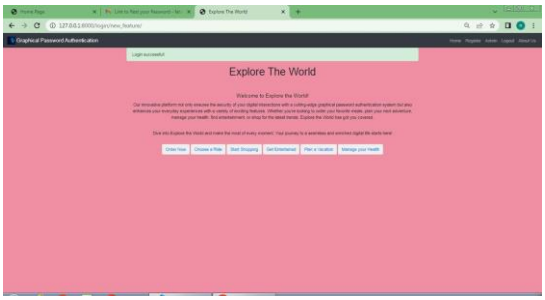
The graphical password authentication system was successfully implemented using the Django framework, incorporating features that enhance both security and user experience. Users can register by creating a graphical password, which is stored securely in the database. During login, users are required to input their graphical password, and the system verifies this by comparing it with stored data. If authentication is successful, users are granted access to various services such as ordering food, booking a cab, and managing health. The system also includes security measures like account blocking after three failed login attempts and a password reset option. The project demonstrates how graphical passwords can provide a more user-friendly and secure alternative to traditional alphanumeric passwords, effectively protecting user data while ensuring ease of use.

REGISTER PAGE

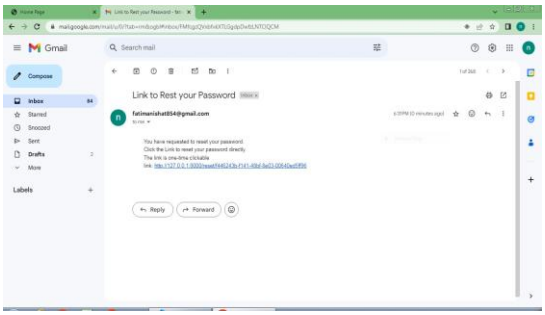
LOGIN PAGE



EXPLORE PAGE



RESET E-MAIL



VI. CONCLUSION

An easy-to-use & safe substitute for conventional alphanumeric passwords is the GPAS. It improves security & reduces common problems like password reuse & vulnerability to brute-force attacks by utilizing images & patterns. The system's modular architecture, which includes security measures, user management & authentication, guarantees strong protection for sensitive data in a range of applications. The system's efficacy will be reinforced by upcoming improvements including biometric integration, multi-factor authentication & adaptive security measures. All things considered, this initiative offers a strong basis for enhancing digital security in a world that is becoming more & more online.

REFERENCES

1. R. S. Shree, S. K. Yadav ,"Graphical Password Authentication: Design and Implementation", Journal of Computer Science and Technology,2022
2. M. T. A. S. Rahman, A. H. Abdullah, S. Y. N. H. Hossain, "Graphical Password Authentication: A Survey", International Journal of Computer Applications,2021.
3. S. Lee, M. B. Schutzer ,"Usability and Security of Graphical Passwords: A Review", Computers & Security,2021.
4. M. Memon, T. L. Hwang ,"A Survey on Graphical Password Authentication",2020.
5. X. Li, Y. Wang, Z. Xu ,"A New Scheme of Graphical Password Authentication", 2019.
6. Muhammad Hussain, Mazhar Khan, and Mohamed Elhoseny, “A Survey of Graphical Password Techniques", 2018.
7. Blocki, J., Christin, N., & Czech, M. , “Graphical Passwords: Learning from the First Twelve Years",2014.
8. Dunphy, P., Yan, J., & O’Brien, M., “A Hybrid Approach to Image-Based Authentication Using Persuasive Cued Click Points", 8th International Conference on Passwords (Passwords), 2013.
9. Sobrado, L., & Birget, J. C., “Graphical Password Authentication Using Cued Click Point”, 2008
10. Susan Wiedenbeck, Jim Waters, “Symposium on Usable Privacy and Security (SOUPS)”, 2008.
11. Jean-Camille Birget, Alex Brodskiy, and Nasir Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system", 2005.
12. Yan, J., Blackwell, A. F., Anderson, R., & Grant, “A On the Security of Text and Graphical Passwords”, In Proceedings of the USENIX Security Symposium, 2004.
13. Saranya Ramanan, Bindhu J S,” A Survey on Different Graphical Password Authentication Technique”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.
14. Amol Bhand, Vaibhav desale, Swati Shirke, Suvarna Pansambal (Shirke), “Enhancement of Password Authentication systemusing Graphical Images”. 2015 International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015.
15. Hung-Min Sun,Shiuan-Tung Chen,Jyh-Haw Yeh and Chia-Yun Cheng, “A Shoulder Surfing Resistant Graphical Authentication System” DOI10.1109/TDSC.2016.2539942IEEE.
16. Sarojini, Priya, Bhuvaneshwari, “Graphical Authentication System Using Pass Matrix“. International Journal of Computer Trends and Technology(IJCTT) Special Issue April – 2017.
17. Robert Reeder, Stuart Schechter, “When the Password Doesn’t Work: Secondary Authentication for Websites”. IEEE Security & Privacy (Volume: 9, Issue: 2, March-April 2011).
18. William Stallings and Lawrie Brown. Computer Security: Principle and Practices. Pearson Education, 2008.
19. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13thUsenix Security Symposium. San Diego, CA, 2004.
20. Lashkari, A. H., Gani, A., Sabet, L. G., & Farmand, S. (2010). A new algorithm on Graphical User

Authentication (GUA) based on multi-line grids. Scientific Research and Essays, 5(24), 3865–3875.
21. Aakansha Gokhale, & Vijaya Waghmare. (2013). Graphical Password Authentication Techniques: A Review. 7.
22. K. Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60–85,June 2009.

25.

23. A.De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.
24. K.-P. L. Vu, R. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J.Cook, and E. Schultz, "Improving password security and memorability to protect personal and organizational information," International Journal of Human-Computer Studies, vol. 65, pp. 744–757, 2007.