ISSN 2277-2685
IJESR/Jan-Mar. 2026/ Vol-16/Issue-1/10-18
B. Navakanth Raju *et. al.*, /International Journal of Engineering & Science Research

Full Length Article

Graphical User Authentication: Enhancing Multi-Factor Authentication With Images

B. Navakanth Raju[1], Mrs. V. Vijaya Sri Swarupa[2]
B.Tech Student, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology, Hyderabad, India[1]
Associate Professor, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology, Hyderabad, India[2]

battusunny143@gmail.com, swarupa.ecm@jbiet.edu.in

Article Received 19-12-2025, Revised 15-01-2026, Accepted 22-01-2026

ABSTRACT

The aim project is to develop a robust and user-friendly Graphical Password Authentication that enhances the security of digital access by incorporating image-based authentication alongside traditional alphanumeric credentials.In the current digital landscape, where cyber threats are becoming increasingly sophisticated, traditional alphanumeric passwords often fall short of providing sufficient protection. This project addresses these vulnerabilities by introducing an innovative authentication method that leverages graphical passwords. Users are required to select specific images from a predefined set, creating a personalized and unique password. This graphical layer works in tandem with conventional passwords, significantly improving security and making unauthorized access more challenging.Additionally, the project focuses on striking a balance between security and usability. While many advanced authentication systems can compromise the user experience due to their complexity, the graphical password system offers a simple yet effective solution. By providing a visual, intuitive method for authentication, users can easily recall and utilize their passwords without sacrificing security. Graphical Password Authentication highlights the potential of combining innovative image-based techniques with modern technologies, offering a more secure, personalized, and user-friendly alternative to traditional authentication methods. The system aims to reduce the risks associated with unauthorized access to sensitive information and ensure a more secure online environment for users.

Introduction

As cyber threats continue to evolve in complexity and frequency, the traditional reliance on alphanumeric passwords has become increasingly inadequate in providing the necessary level of security. Alphanumeric passwords, although widely used, are prone to security risks such as brute-force attacks, phishing, and social engineering tactics. Furthermore, users often create weak passwords or reuse the same ones across multiple significantly weakening the overall security of their accounts.

Graphical Password Authentication offers an innovative solution by incorporating images as an additional layer of security. Unlike conventional alphanumeric passwords, which are typically based on a combination of characters and numbers, graphical passwords allow users to select specific images from a predefined set to create a unique visual password. This method not only enhances security but also provides a personalized touch, making it much harder for unauthorized users to guess or replicate. The image-based approach significantly increases the complexity of the password while offering users an intuitive and memorable authentication experience. user convenience. By requiring both an image selection and an alphanumeric password, the application offers a more robust defense against unauthorized access.

This dual-layer approach makes it much

more difficult for attackers to gain entry, as they would need to bypass both layers of authentication to successfully log into the account.

The Graphical Password Authentication Application is particularly suited for platforms that require high levels of security, such as online banking, e-commerce websites, and social media services. These platforms store sensitive personal information, financial data, and private communications, making them prime targets for cybercriminals. By integrating graphical passwords, these applications can provide their users with an additional layer of protection, safeguarding their sensitive data from unauthorized access and potential breaches.

One of the critical challenges in authentication design is ensuring a balance between security and user-friendliness. Complex security systems often frustrate users, as they are difficult to remember and manage. In contrast, the Graphical Password Authentication Application offers a more user-friendly solution by allowing users to select images that have personal significance. This method makes passwords easier to recall and reduces the cognitive load associated with remembering complex alphanumeric combinations.

To further enhance security, the application includes a safety feature that temporarily locks the account after three consecutive failed authentication attempts. This mechanism prevents attackers from continuously trying to guess the password.

System Design And Uml Diagram

Dataflow Diagram
The data flow diagram represents the interaction between the user and the system through three main processes: Register, Login, and Update Details. In the Register process, the user submits their username, password, and graphical password (GP), which are stored in the database after validation. In the Login process, the user provides the same credentials, which are verified; if correct, access is granted. The Update Details process allows users to modify their credentials, which are then updated in the system. Each process ensures secure handling of user data for authentication.

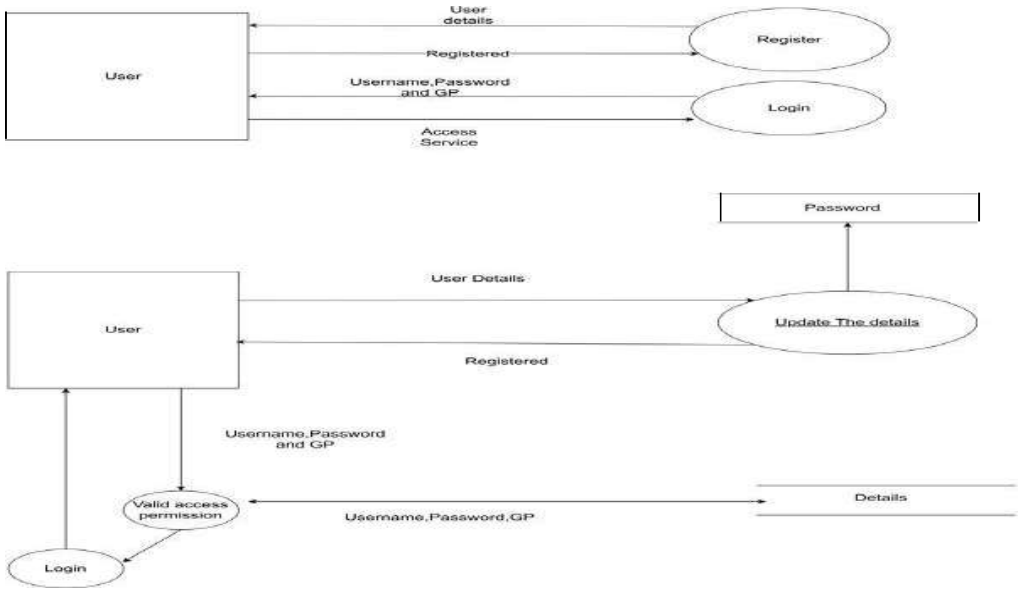

Fig 1 Dataflow Diagram

Architecture Diagram

An Architectural diagram shows a secure user authentication system using both text and graphical passwords. Users first register by providing an email, password, and selecting a graphical password (GP), which are stored in the database. For login, the system verifies the entered credentials—email, password, and GP—against stored data. If valid, the user is signed in; otherwise, access is denied. A sign-out option is available to securely end the session. This setup enhances security by combining traditional and graphical authentication methods.

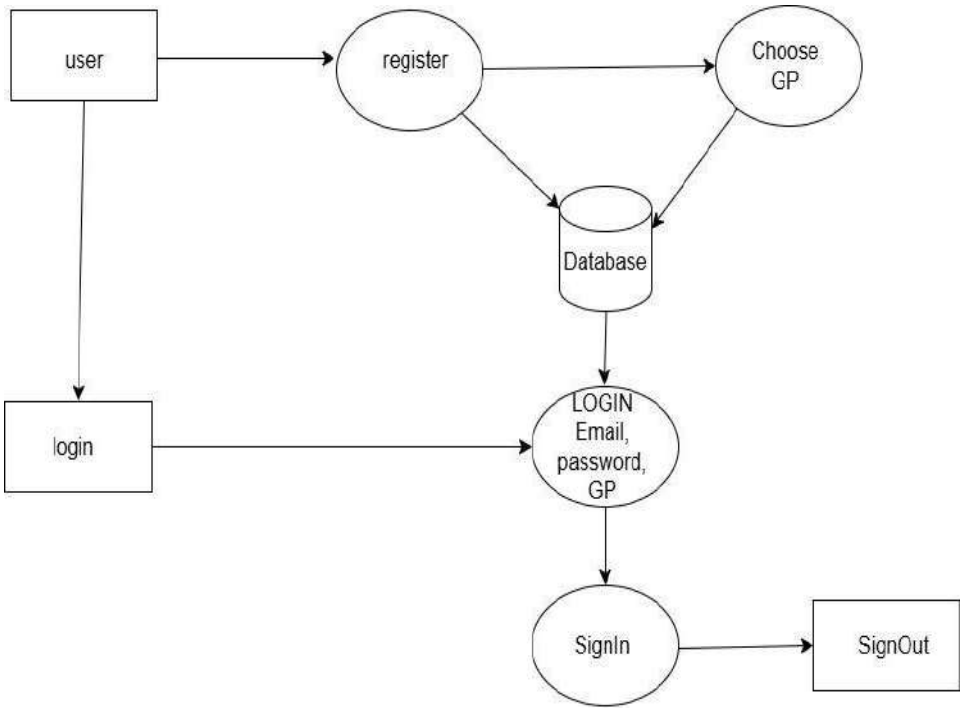

Fig 2 Architecture Diagram

Testing

Introduction Of Software Testing

Software testing is a crucial phase in the development of this graphical password-based authentication system, ensuring the application is reliable, secure, and functions according to the intended design. The primary objective of testing in this project is to verify that users can register and log in using graphical passwords effectively, that authentication is secure, and that account recovery and lock mechanisms work as expected.
Moreover, security testing is essential to ensure resistance to threats like brute-force attacks and unauthorized access. Since the system involves visual elements and user interaction, UI/UX testing also plays a significant role in assessing the usability and responsiveness of the interface.
It is one of two parts of the Box Testing approach to software testing. Its counterpart, Blackbox testing, involves testing from an external or end- user perspective. On the other hand, White box testing in software engineering is based on the inner workings of an application and revolves around internal testing.

Output Screens

Screenshots

Home Page

FIG 1 Home Page

Registration Page

FIG 2 Registration Page

Login page

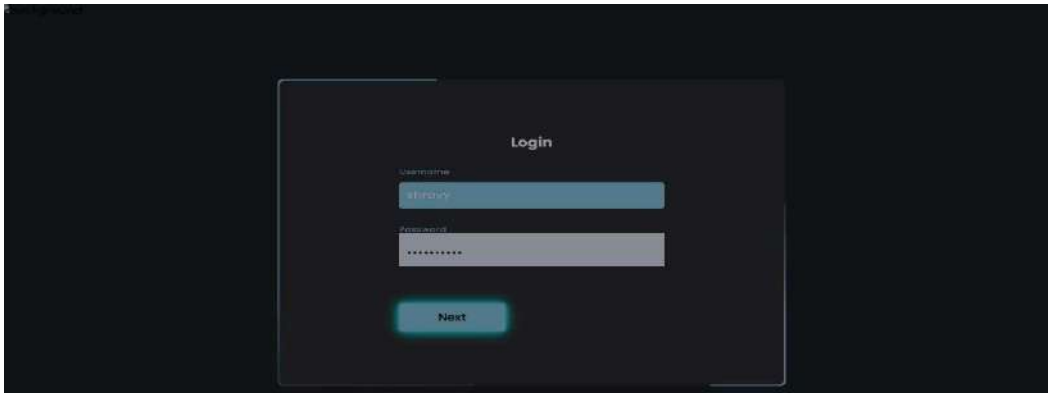

FIG 3 Login Page

Select First Image

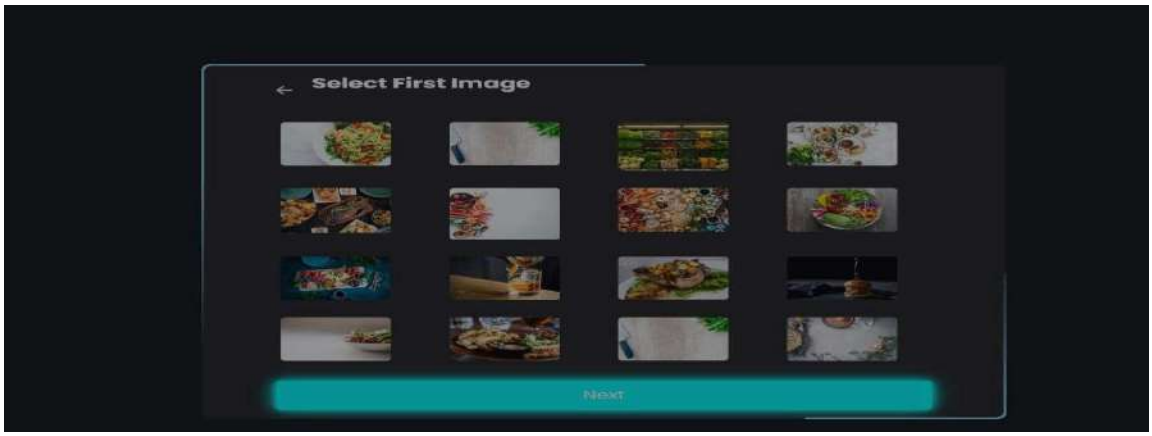

FIG 4 Select First Page

Select Second Image

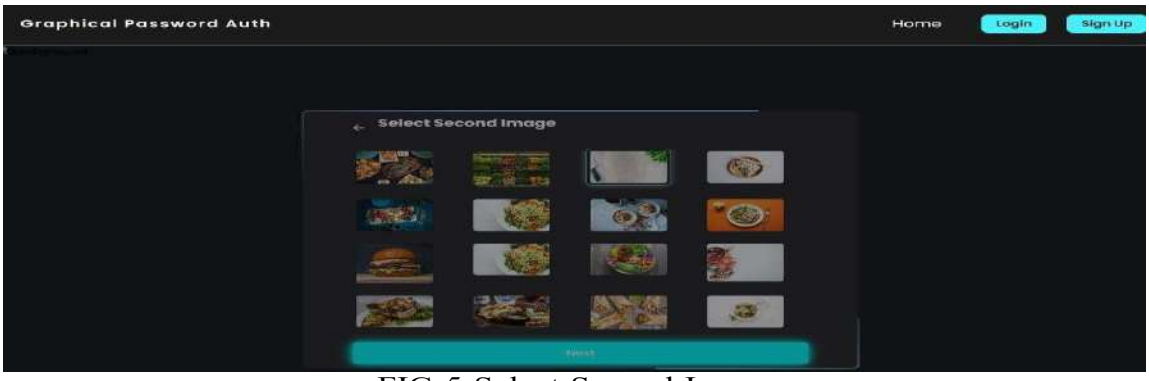

FIG 5 Select Second Image

Select Third Image

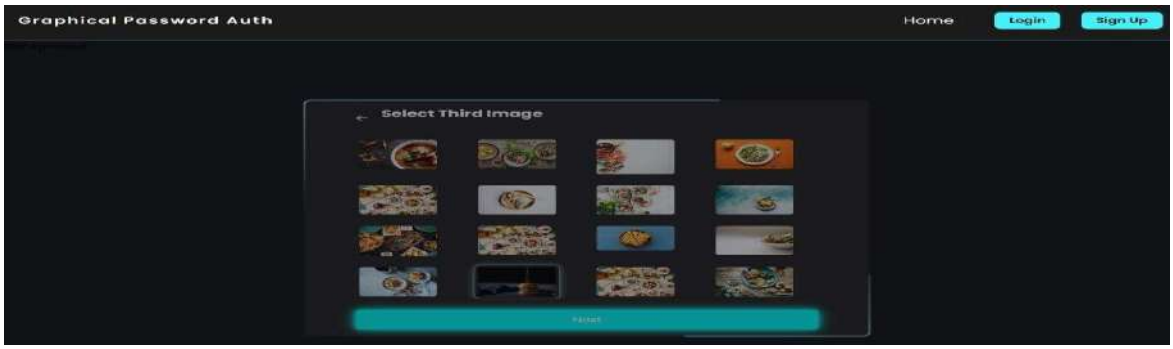

FIG 6 Select Third Image

FIG 7 Select fourth image

Credit Card Fraud Detection

FIG 8 Credit Card Fraud Detection

Transcation Result

FIG 9 Transaction Results

Conclusion And Future Scope

Conclusion

The Graphical Password Authentication system presents an innovative and secure alternative to traditional alphanumeric passwords. By utilizing image- based selection mechanisms, this system enhances both usability and security, particularly against threats like brute-force and dictionary attacks. The two- step verification process — first with textual login credentials and then with graphical password verification — adds an extra layer of security, making unauthorized access significantly more difficult.

This project successfully demonstrates the implementation of a user- friendly authentication mechanism using images, with features like account blocking after multiple failed login attempts and email notifications for suspicious activities. Such features make it practical for real-world applications where high security and user engagement are essential.

Future enhancements could include dynamic image sets, improved image encryption techniques, mobile device integration, and the use of machine learning to detect suspicious login patterns. Overall, this project lays a strong foundation for more intuitive and secure user authentication systems.

Future Scope

The Graphical Password Authentication system demonstrates promising potential in enhancing digital security and user experience. However, there are several areas where this project can be expanded and improved:

Mobile and Touchscreen Integration
Enhancing the UI/UX for mobile devices and tablets would make the system more versatile, especially considering the rise of mobile- first authentication.
Multi-Factor Authentication (MFA)
Integration with biometric verification (like fingerprint or facial recognition) or OTP (one-time passwords) can further improve security.
AI-based Suspicious Activity Detection
Using machine learning to analyze login behavior patterns and flag or block anomalous activities could prevent evolving threats like credential stuffing or session hijacking.
Image Encryption and Obfuscation
Storing and transmitting image data with stronger encryption techniques would protect against image spoofing or data leaks.
Cloud Integration & Scalability
Hosting the authentication system on cloud platforms with database scalability would support enterprise-level deployment and real- time analytics.
Accessibility Improvements
Ensuring the system is accessible to visually impaired users using alternative authentication methods like sound-based or haptic feedback options.
Integration with Existing Authentication Systems
The system can be extended to act as an additional layer for existing login systems used in banking, healthcare, or education platforms.
User Customization Features
Allowing users to upload their own images or select categories for the image grid can enhance memorability and personalization

References

Websites

1. OWASP Foundation (2024). *"Top Ten Security Risks."*
2. https://owasp.org/www-project-top-ten/
3. NIST (National Institute of Standards and Technology) (2024). *"Digital Identity Guidelines – Authentication and Lifecycle Management."* https://pages.nist.gov/800-63-3/sp800-63b.html

Research Papers

1. Blonder, G. E. (1996). *"Graphical Passwords."* U.S. Patent No. 5,559,961.
2. Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C. (2005). *"Design and evaluation of a shoulder-surfing resistant graphical password scheme."* Proceedings of the Working Conference on Advanced Visual Interfaces (AVI '05), ACM, pp. 177–184.
3. Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). *"Graphical passwords: Learning from the first twelve years."* ACM

Computing Surveys (CSUR), 44(4), 1.
4. Tari, F., Ozok, A. A., & Holden, S. H. (2006). *"A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords."*