Graphical Password Authentication

Shruti Dhage, Heena Barach, Sanakruti Jadhav,
Vaishnavi Shivsharan, Shravani Pichake, Suchita Barkund
Zeal Polytechnic, Pune, India.

Abstract- Authentication is a critical component of digital systems, ensuring that only authorized users gain access to sensitive information and services. Traditional text-based password mechanisms, while widely used, suffer from vulnerabilities such as weak password selection, reuse across platforms, and susceptibility to brute-force and phishing attacks. To address these issues, this research presents the Graphical Password Authentication System, a web-based platform designed to enhance security by combining conventional password hashing with graphical pattern verification. The proposed system is developed using Java Server Pages (JSP), Servlets, MySQL database, HTML, CSS, and JavaScript, and deployed on the Apache Tomcat server. It includes features such as secure user registration, SHA-256 password hashing, graphical password setup and validation, OTP-based password recovery, and session management with duplicate login prevention. By introducing a dual-layer authentication mechanism, the system reduces risks of impersonation and unauthorized access while providing a user-friendly interface. The implementation demonstrates how graphical authentication can strengthen digital identity management and improve usability in academic, corporate, and community environments.

Keywords – Graphical Passwords, Authentication, Web Security, SHA-256, Session Management, Digital Identity, Cybersecurity.

I. INTRODUCTION

Authentication plays a vital role in safeguarding digital systems and ensuring secure access to resources. Traditional text-based passwords, though widely adopted, are increasingly inadequate due to common practices such as weak password creation, reuse across multiple platforms, and vulnerability to brute-force and phishing attacks. These limitations compromise system integrity and user trust.

With the rapid advancement of web technologies and increasing cybersecurity threats, alternative authentication mechanisms have emerged. Graphical password systems leverage human visual memory, allowing users to authenticate by selecting image-based patterns rather than relying solely on alphanumeric strings. This approach improves usability while significantly enhancing resistance to attacks.

To address these challenges, this research proposes the Graphical Password Authentication System, a web-based platform that integrates text-based credentials with graphical pattern verification. The system allows users to register securely, set graphical passwords stored in JSON format, and authenticate through a dual-layer mechanism. Incorrect attempts are tracked, accounts are blocked after threshold breaches, and session management ensures secure termination and isolation. By combining cryptographic hashing, graphical verification, and structured session handling, the system provides a robust and user-friendly authentication solution.

II. PROBLEM DEFINITION / RESEARCH GAP

- Existing authentication systems rely heavily on text-based credentials, which present several challenges:
- Weak security: Users often choose simple or reused passwords, making them vulnerable to brute-force and phishing attacks.
- Limited usability: Password fatigue leads to poor memorization and frequent reset requests.
- Single-factor reliance: Most systems depend solely on text input, lacking multi-layer verification.
- Session vulnerabilities: Inadequate session management can lead to hijacking or unauthorized access.

While graphical password systems have been proposed in research, many lack scalability, integration with hashing mechanisms, or structured session handling. Few platforms combine cryptographic password storage, graphical verification, and duplicate prevention in a unified system.

Therefore, the research gap lies in the absence of a secure, scalable, and user-friendly authentication platform that integrates graphical passwords with modern web technologies. The proposed system addresses this gap by providing dual-layer authentication, robust session management, and structured error handling, thereby improving both security and usability.

Objective
The primary objective of this research is to develop a Graphical Password Authentication System, a web-based platform that enhances digital security by combining traditional password mechanisms with graphical pattern verification. The system aims to provide users with a secure, scalable, and user-friendly authentication process that reduces risks of impersonation, brute-force attacks, and password fatigue.

The specific objectives of this research are:

1. To design and implement a web-based authentication system that integrates text-based credentials with graphical password verification.
2. To enable users to securely register, set graphical patterns, and manage their authentication credentials.
3. To ensure secure storage of user data using SHA-256 hashing and structured database constraints.
4. To implement session management and duplicate login prevention for reliable access control.
5. To provide a user-friendly interface that simplifies authentication while maintaining strong security standards.
6. To validate system performance through testing of login accuracy, response times, and scalability under concurrent usage.

III. LITERATURE REVIEW

Several research studies have explored alternatives to traditional password authentication, focusing on graphical methods, biometrics, and multi- factor approaches.

- Blonder (1996) introduced one of the earliest graphical password schemes, where users clicked on predetermined regions of an image. While innovative, the scheme suffered from limited password space and predictability.
- PassPoints (2005) improved upon this by allowing users to select multiple points on an image, increasing complexity. However, usability issues and susceptibility to shoulder-surfing attacks limited adoption.
- Wiedenbeck et al. (2006) analyzed graphical password usability and found that while users remembered visual patterns better than text strings, systems required stronger protection against observation attacks.
- Chiasson et al. (2009) proposed Cued Click Points (CCP), which improved memorability by guiding users through multiple images. Despite better usability, scalability and integration with web systems remained challenges.
- Recent studies (2018–2023) emphasize combining graphical authentication with cryptographic hashing, session management, and multi-factor verification to strengthen security. However, many implementations lack scalability, structured duplicate prevention, or integration with modern web technologies.

Overall, the literature indicates that while graphical password systems improve usability and memorability, existing solutions remain fragmented. Common gaps include weak integration with hashing algorithms, insufficient session management, lack of scalability, and limited support for real-world deployment. These limitations highlight the need for a secure, scalable, and user-friendly graphical authentication platform, which forms the foundation for the development of this system.

Proposed Work Overview
1. System Concept
The Graphical Password Authentication System is a web-based platform designed to provide secure and user-friendly authentication by combining traditional password mechanisms with graphical pattern verification. The primary concept of the system is to create a dual-layer authentication process where users first enter their credentials and then validate their identity through a graphical password. This approach reduces the risks associated with weak or reused text-based passwords while leveraging human visual memory for improved usability.

The system leverages modern web technologies to provide a centralized authentication platform that simplifies secure login, password recovery, and session management. By digitizing the authentication process with graphical verification, the platform improves security, transparency, and efficiency in digital operations. The system contributes to the adoption of stronger cybersecurity practices by making authentication more robust and accessible through a structured and user-friendly interface.

2. Working Process of the System
The working process of the Graphical Password Authentication System involves several steps that enable secure interaction between users and the platform:

- Users register and create an account by providing credentials such as username, email, and password (stored securely using SHA- 256 hashing).
- During registration, users set a graphical password pattern, which is stored in JSON format in the database.
- At login, users first enter their credentials, which are validated against the database.
- Once validated, users must correctly reproduce their graphical password pattern to gain access.
- Incorrect attempts are tracked, and accounts are blocked after exceeding the allowed threshold.
- Successful login establishes a secure session, which is terminated upon logout to prevent unauthorized access.
- All user data, graphical patterns, and login attempts are stored in the system database, enabling efficient management and monitoring of authentication activities.

3. User Roles in the System

The platform is designed to support a single primary user role: User:

Users are individuals who require secure access to the system. They can register, set up graphical passwords, log in, and manage their profile. The system ensures that users benefit from enhanced security without the complexity of remembering long alphanumeric strings.

4. How the Platform Solves the Problem

The Graphical Password Authentication System addresses the major challenges associated with traditional text-based authentication by introducing a dual-layer mechanism. By requiring both credentials and graphical verification, the system reduces dependency on weak passwords and prevents unauthorized access.

The platform improves security by:

- Using SHA-256 hashing for password storage.
- Enforcing duplicate login prevention and account blocking after failed attempts.
- Providing session isolation to prevent hijacking.

At the same time, users benefit from a more intuitive and memorable authentication process, reducing password fatigue and improving usability. Overall, the proposed system promotes secure resource access, supports modern cybersecurity practices, and contributes to building trust in digital platforms.

IV. SYSTEM ARCHITECTURE / SYSTEM DESIGN

A. System Architecture

The architecture of the Graphical Password Authentication System is designed using a multi-layer web application structure that enables secure and efficient interaction between users and the system. The platform follows a client–server architecture, where users access the system through a web interface, and the server processes authentication requests and manages data using backend technologies and a database system.

The system is developed using Java Server Pages (JSP) and Servlets for backend processing, MySQL as the database for storing user credentials and graphical patterns, and HTML, CSS, and JavaScript for the frontend interface. The application is deployed on the Apache Tomcat server, which handles client requests and server responses.

The architecture consists of three major layers:

1. Presentation Layer

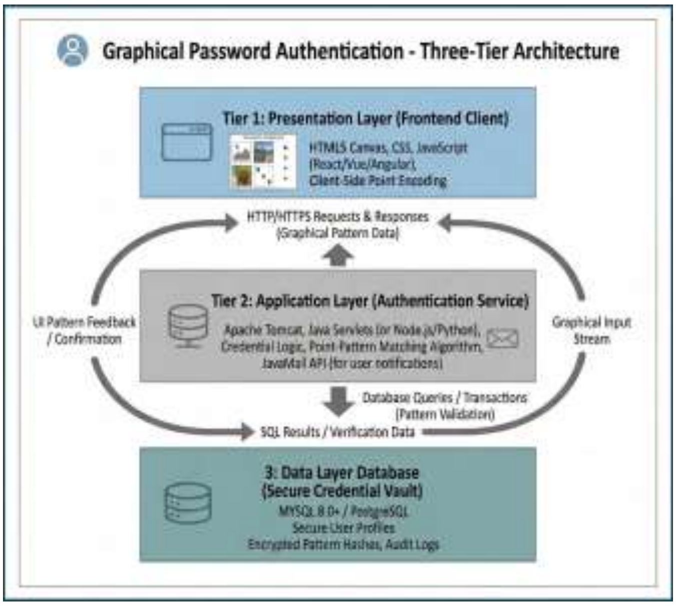
This layer provides the user interface through web pages where users interact with the system. It includes features such as registration, login, graphical password setup, pattern validation, and password recovery.

2. Application Layer

This layer contains the business logic of the system implemented using JSP and Servlets. It processes user requests, validates credentials, manages graphical password verification, tracks login attempts, enforces duplicate prevention, and coordinates communication between different system modules.

3. Data Layer

The data layer manages the storage and retrieval of authentication data using a MySQL database. It stores information such as user profiles, hashed passwords, graphical patterns (in JSON format), login attempts, and session records. This layered architecture ensures scalability, modularity, and secure communication between system components.


Graphical Password Authentication - Three-Tier Architecture
Tier 1: Presentation Layer (Frontend Client)
HTML5 Canvas, CSS, JavaScript
(React/Vue/Angular),
Client-Side Point Encoding
HTTP/HTTPS Requests & Responses
(Graphical Pattern Data)
Tier 2: Application Layer (Authentication Service)
Apache Tomcat, Java Servlets (or Node.js/Python),
Credential Logic, Point-Pattern Matching Algorithm,
JavaMail API (for user notifications)
UI Pattern Feedback
/ Confirmation
Graphical Input
Stream
Database Queries / Transactions
(Pattern Validation)
SQL Results / Verification Data
3: Data Layer Database
(Secure Credential Vault)
MYSQL 8.0+ / PostgreSQL
Secure User Profiles
Encrypted Pattern Hashes, Audit Logs

B. System Modules

The Graphical Password Authentication System is composed of multiple functional modules that work together to provide a structured and secure authentication service. Each module performs a specific task and contributes to the overall functionality of the system.

1. User Authentication Module

Responsible for managing user access and ensuring secure interaction with the platform. It provides functionality for user registration, login authentication, and password recovery. Passwords are stored using SHA-256 hashing, and OTP-based recovery ensures secure resets.

2. Graphical Password Module

Enables users to set, manage, and validate graphical password patterns. Patterns are stored in JSON format and verified during login. This module enhances usability by leveraging visual memory while strengthening security against brute- force attacks.

3. Session Management Module

Handles secure session creation, validation, and termination. It ensures that authenticated users maintain isolated sessions and that sessions are invalidated upon logout to prevent hijacking.

4. Duplicate Login Prevention Module

Tracks login attempts and enforces account blocking after repeated failed attempts. This module prevents unauthorized access and ensures controlled authentication.

5. Notification and Updates Module

Provides real-time updates regarding login attempts, password recovery requests, and account status changes. This improves transparency and keeps users informed about their authentication activities.

6. User Profile Management Module

Allows users to manage their personal account information, including updating credentials, viewing login history, and monitoring activity records. This module ensures that users have full control over their authentication data.

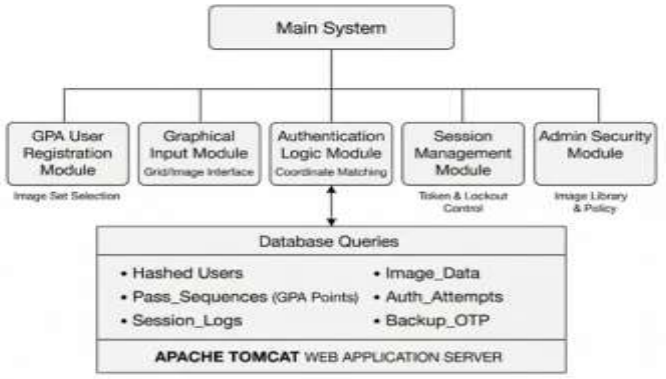


Figure 2. System Module Structure Diagram for Graphical Password Authentication

V. IMPLEMAINTATION

The implementation of the Graphical Password Authentication System focuses on developing a web-based platform that provides secure authentication through a combination of text-based credentials and graphical password verification. The system is designed using modern web technologies and a structured client–server architecture to ensure reliability, usability, and scalability.

A. Technologies Used

The system is developed using the following technologies:

1. Java Server Pages (JSP)

JSP is used for creating dynamic web pages and displaying content retrieved from the server and database. It allows seamless integration between the front-end interface and backend logic.

2. Java Servlets

Servlets handle server-side processing and manage user requests. They control the application logic, including authentication, graphical password validation, session management, and data communication with the database.

3. MySQL Database

MySQL is used as the relational database management system to store and manage all application data such as user credentials, hashed passwords, graphical patterns (stored in JSON format), login attempts, and session records.

4. Apache Tomcat Server

Apache Tomcat is used as the web application server that hosts the JSP and Servlet-based application. It processes HTTP requests and manages communication between the web interface and backend logic.

5. HTML, CSS, and JavaScript

These technologies are used to design the user interface and improve user interaction. HTML provides the structure of web pages, CSS ensures responsive and visually appealing design, and JavaScript enables dynamic functionality such as graphical password setup and validation.

B. Development Process

1. Requirement Analysis

The initial phase involved identifying the challenges faced by users in traditional text-based authentication systems, such as weak password selection, reuse, and vulnerability to brute-force attacks.

2. System Design

During this stage, the system architecture, database schema, and data flow diagrams were designed to define how different modules (authentication, graphical password, session management, duplicate prevention) interact with each other.

3. Development Phase

The system was developed using JSP and Servlets for backend functionality, while HTML, CSS, and JavaScript were used for the front- end interface. Database connectivity was implemented using JDBC to interact with the MySQL database.

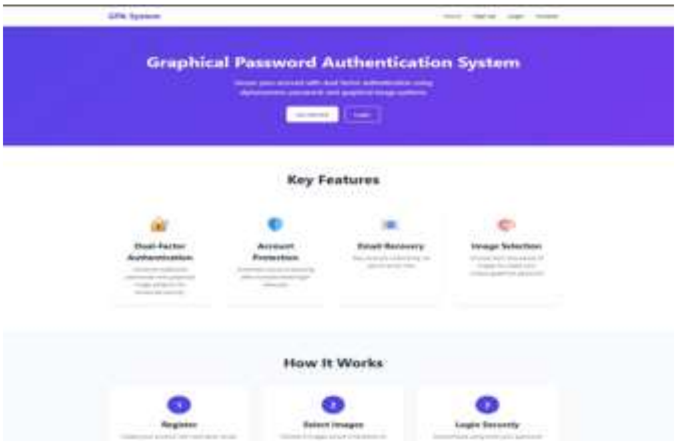
4. Testing Phase

The application was tested to verify system functionality, database connectivity, graphical password setup and validation, session handling, and duplicate login prevention. Various scenarios were tested to ensure reliability, accuracy, and performance under concurrent usage.

5. Deployment

The system is deployed on the Apache Tomcat server, allowing users to access the authentication platform securely through a web browser.

VI. RESULT



GPA System

Graphical Password Authentication System

[illegible]

Key Features

Dual-Factor Authentication

Account Protection

Email Recovery

Image Selection

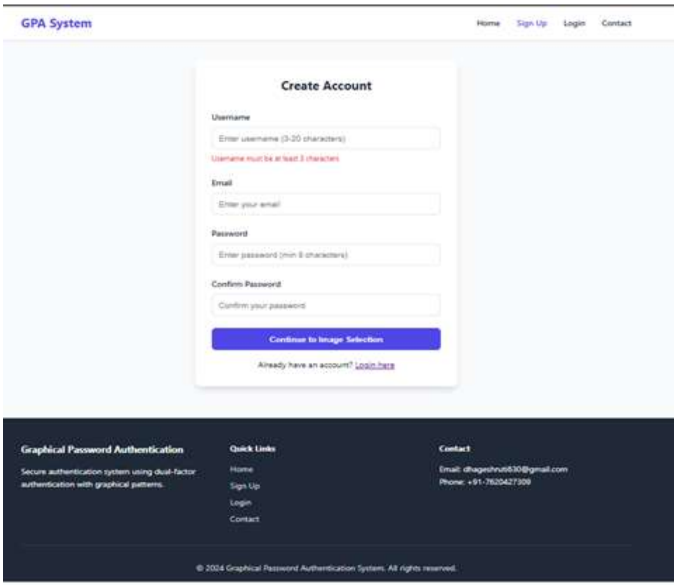
How It Works

Register

Select Images

Login Securely

Home Page



GPA System

Home Sign Up Login Contact

Create Account

Username

Enter username (3-20 characters)

Username must be at least 3 characters

Email

Enter your email

Password

Enter password (min 8 characters)

Confirm Password

Confirm your password

Continue to Image Selection

Already have an account? Login here

Graphical Password Authentication

Secure authentication system using dual-factor authentication with graphical patterns.

Quick Links

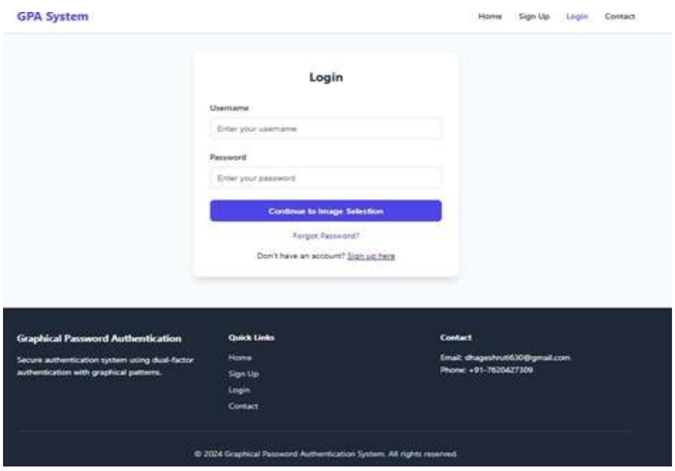
Home
Sign Up
Login
Contact

Contact

Email: dhageshruti630@gmail.com
Phone: +91-7620427309

© 2024 Graphical Password Authentication System. All rights reserved.

User Registration



GPA System

Home Sign Up Login Contact

Login

Username

Enter your username

Password

Enter your password

Continue to Image Selection

Forgot Password?

Don't have an account? Sign up here

Graphical Password Authentication

Secure authentication system using dual-factor authentication with graphical patterns.

Quick Links

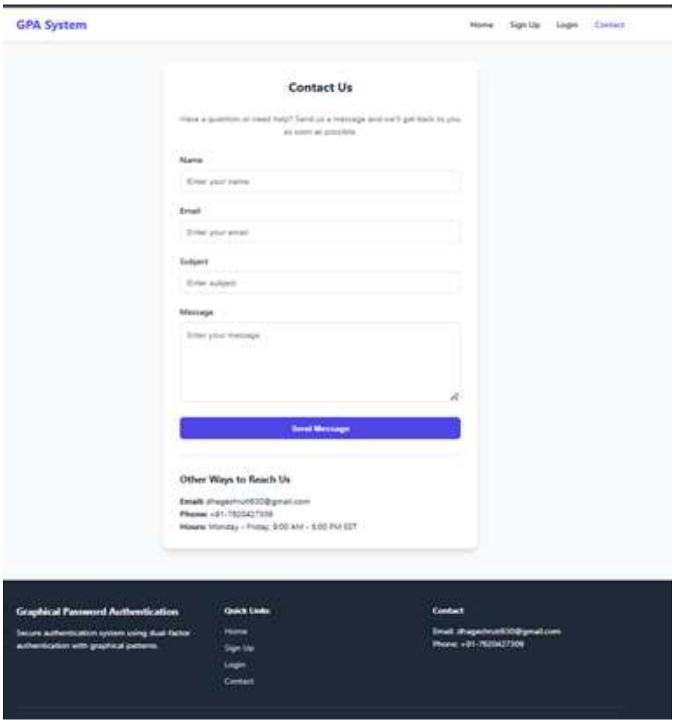
Home
Sign Up
Login
Contact

Contact

Email: dhageshruti630@gmail.com
Phone: +91-7620427309

© 2024 Graphical Password Authentication System. All rights reserved.

User login



GPA System

Home Sign Up Login Contact

Contact Us

Have a question or need help? Send us a message and we'll get back to you as soon as possible.

Name

Enter your name

Email

Enter your email

Subject

Enter subject

Message

Enter your message

Send Message

Other Ways to Reach Us

Email: dhageshruti630@gmail.com
Phone: +91-7620427309
Hours: Monday - Friday: 9:00 AM - 5:00 PM EST

Graphical Password Authentication

Secure authentication system using dual-factor authentication with graphical patterns.

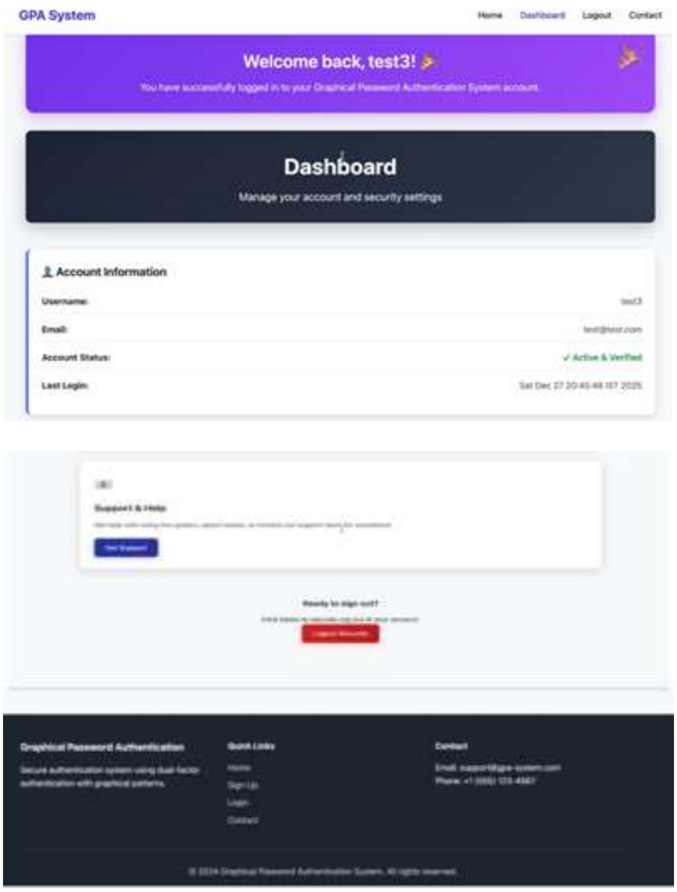
Quick Links

Home
Sign Up
Login
Contact

Contact

Email: dhageshruti630@gmail.com
Phone: +91-7620427309

Contact



GPA System

Home Dashboard Logout Contact

Welcome back, test3!

You have successfully logged in to your Graphical Password Authentication System account.

Dashboard

Manage your account and security settings

Account Information

Username: test3

Email: test@test.com

Account Status: ✓ Active & Verified

Last Login: Sat Dec 27 20:45:48 IST 2025

Support & Help

[illegible]

Ready to sign out?

[illegible]

Graphical Password Authentication

Secure authentication system using dual-factor authentication with graphical patterns.

Quick Links

Home
Sign Up
Login
Contact

Contact

Email: support@gpa-system.com
Phone: +1 (555) 123-4567

© 2024 Graphical Password Authentication System. All rights reserved.

Dashboard

VII. CONCLUSION

The Graphical Password Authentication System demonstrates that web technologies such as JSP, Servlets, MySQL, and Apache Tomcat can be effectively utilized to build secure and user-friendly authentication mechanisms. By shifting from traditional text-based passwords to image-based credentials, the system enhances resistance against brute-force and dictionary attacks while improving usability through reliance on visual memory.

The project highlights the potential of graphical authentication in addressing common password-related vulnerabilities and providing a more intuitive login experience. Its modular design ensures scalability, making it adaptable for integration with mobile applications, biometric verification, and intelligent security monitoring.

Ultimately, this research validates that graphical authentication is not only a viable alternative to conventional password systems but also a promising step toward more secure, accessible, and user-centric digital security solutions.

REFERENCES

1. A. Perrig and D. Song, “Hash visualization: A new technique to improve real-world security,” in Proceedings of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC), 1999, pp. 131–138.
2. R. Dhamija and A. Perrig, “Déjà Vu: A user study using images for authentication,” in Proceedings of the 9th USENIX Security Symposium, 2000, pp. 45–58.
3. H. Tao and C. Adams, “Pass-Go: A proposal to improve the usability of graphical passwords,” International Journal of Network Security, vol. 7, no. 2, pp. 273–292, 2008.
4. J. Yan, A. Blackwell, R. Anderson, and A. Grant, “Password memorability and security: Empirical results,” IEEE Security & Privacy, vol. 2, no. 5, pp. 25–31, 2004.
5. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” International Journal of Human-Computer Studies, vol. 63, no. 1–2, pp. 102–127, 2005.
6. A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.
7. M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, “Reducing shoulder-surfing by using gaze-based password entry,” in Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS), 2007, pp. 13–19.