International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | March – 2026 DOI:10.55041/ISJEM05842
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Personalized Image Verification in a User-Centric Two-Factor Authentication System

Dr. K. Satyam[1], Nandhimandalam Akash[2]

[1]Associate Professor, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India.

[2] Post Graduate, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India.

Abstract

Strong authentication procedures are necessary for modern web apps to prevent unwanted access to private user information. Attacks like password guessing, phishing, and credential theft can compromise traditional password-based authentication systems. This study suggests a user-centric two-factor authentication system that combines conventional password authentication with customized image verification in order to overcome these difficulties. In the suggested method, users select their pre-registered personalized image to confirm their identity after initially authenticating with their credentials. While preserving usability, this extra layer of authentication greatly increases security. With features like user registration, login authentication, customized image management, and optional Google Authenticator integration for increased security, the system is constructed as a web application using Python and Django. Results from experiments show that the suggested method successfully improves authentication security without sacrificing an easy-to-use interface.

Keywords

Two-Factor Authentication, Image-Based Authentication, Web Security, User Authentication, Multi-Factor Authentication, Django Framework

I. Introduction

The demand for safe authentication methods has greatly expanded due to the quick expansion of digital platforms. Traditional password-based authentication techniques are still used by many online systems, and they are susceptible to a number of security risks, including phishing, brute-force attacks, and password reuse. These flaws frequently lead to data breaches and illegal access. By forcing users to submit two separate forms of verification, two-factor authentication (2FA) has become a popular way to improve security. SMS codes, email verification, and authenticator apps are typical 2FA techniques. These approaches might still have usability issues or rely significantly on other equipment, though.

Personalized image verification is included as an extra authentication factor in this study's user-centric authentication method. To properly use the system, users must recognize their registered image from a collection of photographs after providing valid login credentials. This approach improves security and offers a user-friendly interface. The Django framework is used to construct the suggested system as a web-based application, and Google Authenticator support is optional to enhance authentication security.

II. Problem Statement

Passwords, which are frequently weak and readily compromised, are a major component of traditional authentication methods. Systems are susceptible to attacks like credential stuffing and brute-force attempts because many users frequently reuse passwords across several platforms. Furthermore, traditional authentication techniques don't always offer enough defense against unwanted access.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | March – 2026 DOI:10.55041/ISJEM05842
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

While two-factor authentication increases security, certain implementations may cause usability problems or rely on external devices like mobile phones. As a result, a safe and easy-to-use authentication system that enhances identity verification while preserving user simplicity is required.

III. Proposed System

A two-factor authentication method that combines password authentication with customized image verification is introduced by the suggested system. Users create an account and choose a customized photo to utilize as an extra authentication factor throughout the registration process.
The system first checks the username and password when a user tries to log in. The system shows a collection of photos, including the user's registered photo, following successful credential validation. To finish the authentication procedure, the user must accurately recognize their customized image.

Additionally, by integrating Google Authenticator for time-based one-time passwords (TOTP), the system offers an optional security boost. This multi-layer authentication method preserves user convenience while greatly enhancing system security.

IV. Outputs

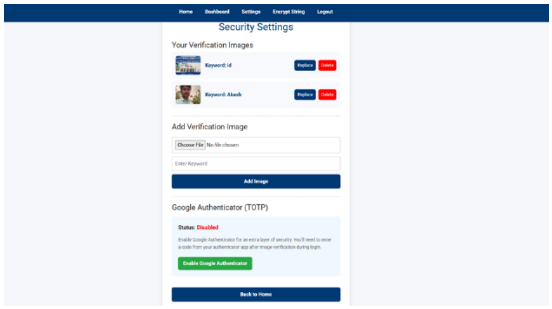

Fig: User Security Settings Interface

Users can control the customized verification images that are used for authentication through this interface. For identification, the user can browse previously uploaded photographs and the keywords that correspond with them. Users can update or remove their authentication photos as needed with options like replace and delete. By supplying an image file and a matching phrase, the system also enables users to upload new verification photos. To further strengthen security upon login, users can also activate Google Authenticator (TOTP).

Fig: User Registration Page with Personalized Image SetupThis site serves as a representation of the system's registration interface, where new users set up their accounts. To register, users must provide their password, email address, and username. The technology enables users to submit a customized image and provide a keyword for authentication in addition to these details. Later on in the login process, these pictures are utilized in the second authentication stage. By associating a distinctive visual component with the user's identity, this procedure improves system security.

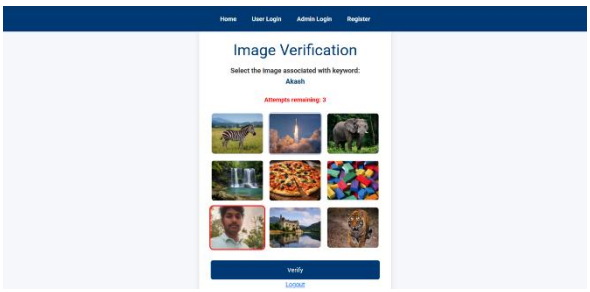

Fig: Personalized Image Verification for Two-Factor Authentication

The image-based verification step, which serves as the second authentication element, is shown on this screen. The system shows the user several graphics once they have entered their login information correctly. The image that corresponds to the registered term must be found and chosen by the user. In order to stop unwanted access, the interface also shows how many attempts are left. By combining tailored visual verification with password authentication, this method improves security.

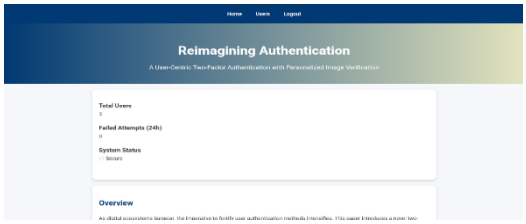

Fig: Admin Dashboard and System Overview

Administrators can see system activity and user data on this dashboard. Important indicators like the total number of registered users and unsuccessful login attempts within the previous 24 hours are displayed. The overall security status of the system is also displayed on the interface. Administrators can guarantee appropriate user management and keep an eye on the authentication system. The authentication framework's dependability and security are preserved in part via this centralized control panel.

V. Conclusion

This study introduced a user-centric two-factor authentication system that combines conventional password-based authentication with customized image verification to improve security. By forcing users to recognize a pre-registered image during the login process, the suggested solution adds an extra degree of security. This strategy lessens the possibility of illegal access brought on by password-related flaws like phishing or guessing. The Django framework was used to create the system as a web-based application with capabilities including administrative monitoring, picture management, and user registration. Additionally, the optional Google Authenticator integration increases security by using time-based one-time password verification. All things considered, the suggested authentication framework enhances security and usability, making it appropriate for contemporary online applications that need robust and trustworthy user authentication methods.

References

[1] 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, Jan. 2004.

[2] D. Florêncio and C. Herley, “A Large-Scale Study of Web Password Habits,” in Proceedings of the 16th International World Wide Web Conference, Banff, Canada, 2007, pp. 657–666.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson Education, 2017.

[4] M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2018.

[5] N. Provos and D. Mazieres, “A Future-Adaptable Password Scheme,” in Proceedings of the USENIX Annual Technical Conference, 1999.