WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

DYNAMIC PASSWORD SYSTEM

Ms.S.Amsavalli[1], D.Divya Dharshini[2], M.Aruna Devi[3]

Assistant Professor [1] ,B.S.Abdur Rahman Crescent Institute of Science and Technology,Vandalur-600048, Department of Computer Science Engineering.
Student [2] , Student [3] , B.S.Abdur Rahman Crescent Institute of Science and Technology,Vandalur-600048,Department of Computer Science Applications.

ABSTRACT :

In today's digital landscape, the reliance on conventional password-based authentication systems exposes user accounts and critical data to a variety of cyber threats, including credential stuffing, brute-force attacks, and social engineering. This project proposes a novel authentication system built using Django, which enhances conventional login methods by integrating facial recognition as a secondary verification layer, and a dynamic password-changing mechanism to respond to unauthorized access attempts.

The proposed system actively defends against security breaches by validating a user's facial features in real-time during login. If the facial identity does not match the registered image, the system autonomously modifies the user's password, effectively locking the intruder out even if the original password is known. This dual-security approach ensures enhanced safety, user convenience, and proactive threat mitigation. The combination of biometric verification with an automated password management system offers an innovative solution to modern authentication challenges, aiming to redefine secure access practices across digital platforms.

Keywords : Facial Recognition, Biometric Authentication, Django, Dynamic Password System, Secure Login, Cybersecurity.

Introduction

In the ever-evolving domain of cybersecurity, authentication plays a crucial role in safeguarding systems, services, and personal data from unauthorized access. Password-based systems, although prevalent, are increasingly susceptible to breaches owing to weak password practices, leaks, and sophisticated cyberattacks. This has urged the industry to look beyond static credentials and integrate multi-factor authentication and biometrics.

Facial recognition has emerged as one of the most convenient yet secure forms of biometric authentication, leveraging unique physical features that are hard to replicate. However, even biometric systems face challenges if they are not combined with intelligent response mechanisms.

This paper presents a hybrid authentication model developed using Django, a high-level Python web framework, that integrates facial recognition technology with a dynamic password system. The objective is to create a system that not only authenticates users based on their face but also takes immediate action when unauthorized access attempts are detected — by automatically altering the password and notifying the user. This makes unauthorized access extremely difficult even if the password is compromised.

Objective

- To develop a secure and intelligent user authentication system using facial recognition and Django.
- To integrate a dynamic password modification mechanism triggered by unauthorized face detection.
- To enhance cybersecurity defenses through real-time biometric validation.
- To reduce the risk of brute-force, password-leak, and credential reuse attacks.
- To improve user experience by minimizing login friction while maintaining high-security standards.

Methodology

1. System Design: The system architecture is built on Django's Model-View-Template (MVT) framework. It uses Django's built-in authentication mechanisms for secure password storage and user management, enhanced with Python libraries for facial recognition such as OpenCV and face_recognition.

2. Facial Recognition Module: Upon login, the user's webcam captures a live image, which is compared to a pre-registered facial encoding stored securely in the database. If the facial match score exceeds a pre-set threshold, the user is authenticated and granted access.

3. Dynamic Password Mechanism: In the event of a mismatch — where the detected face is not recognized as the legitimate user — the system automatically triggers a function that resets the user's password to a newly generated random password. This action prevents unauthorized users from reattempting access with the same known credentials.

4. Notification System: Upon password change due to an unauthorized attempt, an email notification or SMS alert is dispatched to the legitimate user, informing them of the security incident and providing instructions for resetting their credentials.

5. Security Practices: Passwords are hashed using Django's PBKDF2 algorithm. Facial data is stored as encrypted encodings rather than raw images. Logs are maintained for all login attempts, including successful and failed facial recognition events.

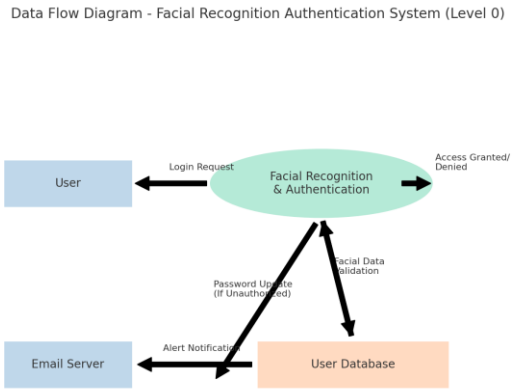
6. Testing & Evaluation: The system was tested under various scenarios using controlled datasets and live webcam feeds. Different lighting conditions, face angles, and impersonation attempts were simulated to evaluate the robustness of the recognition system and the efficiency of the dynamic password mechanism.

Results and Discussion

The developed system was subjected to repeated real-world test cases, including authorized logins, face mismatch simulations, and forced intrusion attempts. The results demonstrated that the facial recognition module correctly identified authorized users with high precision and prevented access when a face was unrecognized.

In cases of unauthorized access:
- The dynamic password mechanism successfully changed the password within milliseconds.
- Intruders, even when possessing the original password, could not proceed without passing the facial verification.
- Legitimate users were immediately notified, allowing them to initiate recovery actions.

The integration of facial recognition with real-time password update logic proved highly effective in minimizing the window of vulnerability, ensuring that even if a password leak occurred, the damage would be swiftly contained. The hybrid approach offered both convenience and high resilience to contemporary attack vectors.



Conclusion

This project successfully demonstrates the development of a secure and intelligent authentication system that integrates facial recognition and a dynamic password strategy using Django. The system enhances conventional authentication methods by providing biometric validation and instant security responses, thereby offering robust protection against unauthorized access.

The dual mechanism reduces the dependency on passwords as the sole security measure and provides a fail-safe system that reacts intelligently to potential breaches. This approach represents a forward step toward more secure and user-friendly authentication in an era where data protection and user identity validation are of paramount importance.

Future work can extend this project to support multi-user environments, additional biometric factors such as voice recognition, and deeper AI-driven anomaly detection for heightened security.

REFERENCES :

1. Bradski, G. & Kaehler, A. (2008). Learning OpenCV: Computer Vision with the OpenCV Library. O'Reilly Media.
2. Django Software Foundation, Django Documentation. Retrieved from https://docs.djangoproject.com.
3. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.
4. OpenCV.org — Open Source Computer Vision Library. https://opencv.org.
5. Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint Face Detection and Alignment Using Multi-task Cascaded Convolutional Networks. IEEE Signal Processing Letters.