Web-Based Facial Authentication System

Prepared By: Surya Hanuman KONJETI

Position: Cyber Security Intern

Intern ID: SMI81626

College: ESAIP, École d'Ingénieurs

Company: Slash Mark IT Solutions (OPC) Pvt. Ltd.

Batch: November 15, 2025 to January 15, 2026

TABLE OF CONTENTS

1. ABSTRACT

Passwords and traditional authentication methods are prone to security threats such as brute force attacks, password reuse, and phishing. To overcome these issues, this project introduces a Web-Based Facial Authentication System that uses facial recognition along with liveness detection to ensure that the user is physically present during authentication.

The system captures real-time facial images using a webcam, processes them using OpenCV, and authenticates users based on trained facial data. A liveness detection mechanism further enhances security by verifying blink or head movement to prevent spoofing using photographs or videos.

This project demonstrates the integration of computer vision and cybersecurity principles to create a robust biometric authentication solution.

2. INTRODUCTION

In today's digital environment, authentication systems are essential for protecting user data and preventing unauthorized access. However, most existing systems rely on passwords, which are vulnerable to security threats such as phishing, brute force attacks, keylogging, and password reuse. Users also tend to create weak or predictable passwords, further increasing security risks.

These traditional methods fail to verify the real physical presence of the user, making them susceptible to identity impersonation. Therefore, there is a need for a more secure, reliable, and user-friendly authentication mechanism that reduces dependency on passwords and improves overall authentication accuracy.

2.2 Need for the System

Facial authentication provides a secure and convenient alternative by utilizing biometric features unique to every individual. Adding liveness detection ensures that the system cannot be tricked by static images or recorded videos.

3. OBJECTIVES OF THE PROJECT

- To develop a web-based facial authentication system.
- To integrate real-time face recognition using OpenCV.
- To include liveness detection for enhanced security.
- To provide a secure dashboard for authenticated users.
- To demonstrate practical cyber security implementation.

4. SCOPE OF THE PROJECT

- Focuses on facial recognition authentication.
- Suitable for demonstration and academic usage.
- Uses local data storage for user information.
- Includes basic liveness checking mechanisms.

5. SYSTEM STUDY

5.1 Existing System

Current authentication systems mainly use usernames, passwords, OTPs, and security questions. Although widely used, these methods have serious security weaknesses. They depend on information the user knows, which can be stolen through phishing, brute force attacks, keylogging, or credential stuffing. Managing complex passwords also creates inconvenience for users.

Even some biometric systems lack liveness detection, allowing attackers to bypass security using photos or videos. In addition, many advanced solutions rely on expensive cloud services, limiting accessibility for academic purposes. As a result, existing systems do not provide reliable identity verification or strong protection against modern cyber threats.

5.2 Proposed System

The proposed Web-Based Facial Authentication System replaces traditional login methods with facial recognition combined with liveness detection. It verifies both the identity and physical presence of the user, ensuring secure authentication.

The system uses real-time face detection with OpenCV, recognizes faces using the LBPH model, and performs liveness checks by detecting facial movement. User data is stored securely, and access is controlled through session management.

This approach eliminates the need for passwords, prevents spoofing using photos or videos, improves security, and offers a user-friendly authentication experience suitable for both academic and real-world cybersecurity applications.

6. SYSTEM REQUIREMENTS

Hardware Requirements:

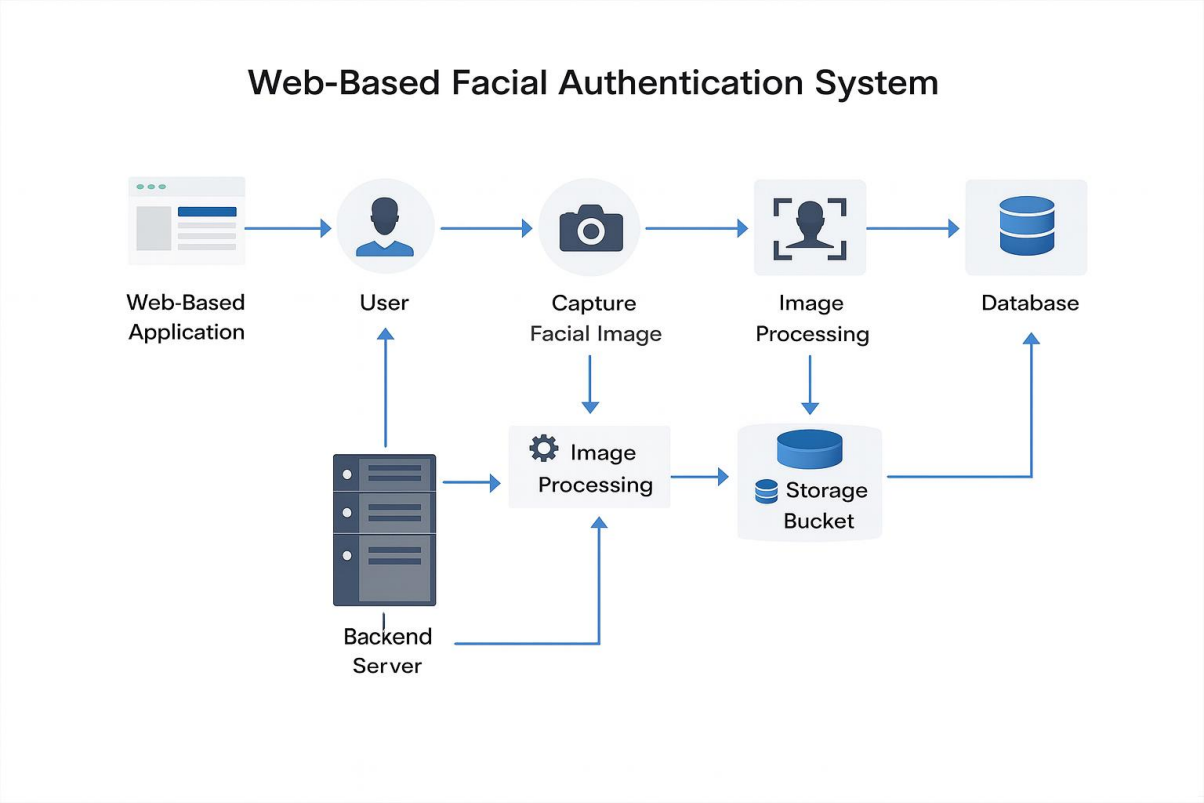
- Webcam
- Minimum 4GB RAM
- Dual-core processor or higher

Software Requirements:

- Python 3.x
- Flask Framework
- OpenCV Library
- Web Browser

7. SYSTEM ARCHITECTURE

7.1 Architecture Diagram



This architecture diagram visually represents the complete working structure of the Web-Based Facial Authentication System. It demonstrates how user interaction flows through the frontend interface, webcam capture, processing engine, backend server, and finally into permanent storage for authentication and verification.

7.2 Architecture Explanation

The architecture is designed using a layered approach to clearly separate responsibilities and enhance both performance and security.

Web-BasedApplication:
This is the frontend layer accessed through a browser. It provides all graphical interfaces such as Home, Register, Login, and Dashboard pages. The application captures user input and communicates with the backend server for further processing.

User:
The user interacts with the system by registering or logging in. The user's face acts as the primary authentication factor.

Capture Facial Image:
The system activates the webcam to capture live facial images. These images are used for both enrolment and real-time authentication.

Image Processing:
The captured face image is converted into grayscale, normalized, cropped, and processed using computer vision algorithms to extract facial features.

BackendServer:
The server handles all logical operations, including face detection, recognition, liveness verification, and session management.

Storage Bucket:
Processed facial data and images are stored securely for future comparison and auditing.

Database:
Stores structured user information such as name, age, email, facial image reference, and last login time.

Overall Flow:

1. User interacts with the web interface
2. Webcam captures facial image
3. Image is processed and analysed
4. Backend performs recognition and liveness check
5. User data is stored or verified from database
6. Authentication result is returned
7. Access is granted to dashboard

8. MODULE DESCRIPTION

Home Page Module

Provides access to registration and login functionalities.

Registration Module

Captures user details and facial image for enrolment.

Login Module

Validates user identity through face recognition and liveness detection.

Dashboard Module

Displays authenticated user information.

9. IMPLEMENTATION DETAILS

Backend uses Flask and OpenCV for image processing and recognition. Frontend interfaces are built using HTML, CSS, and JavaScript.

10. OUTPUT SCREENS & EXPLANATION

10.1 Home Page – Main Interface

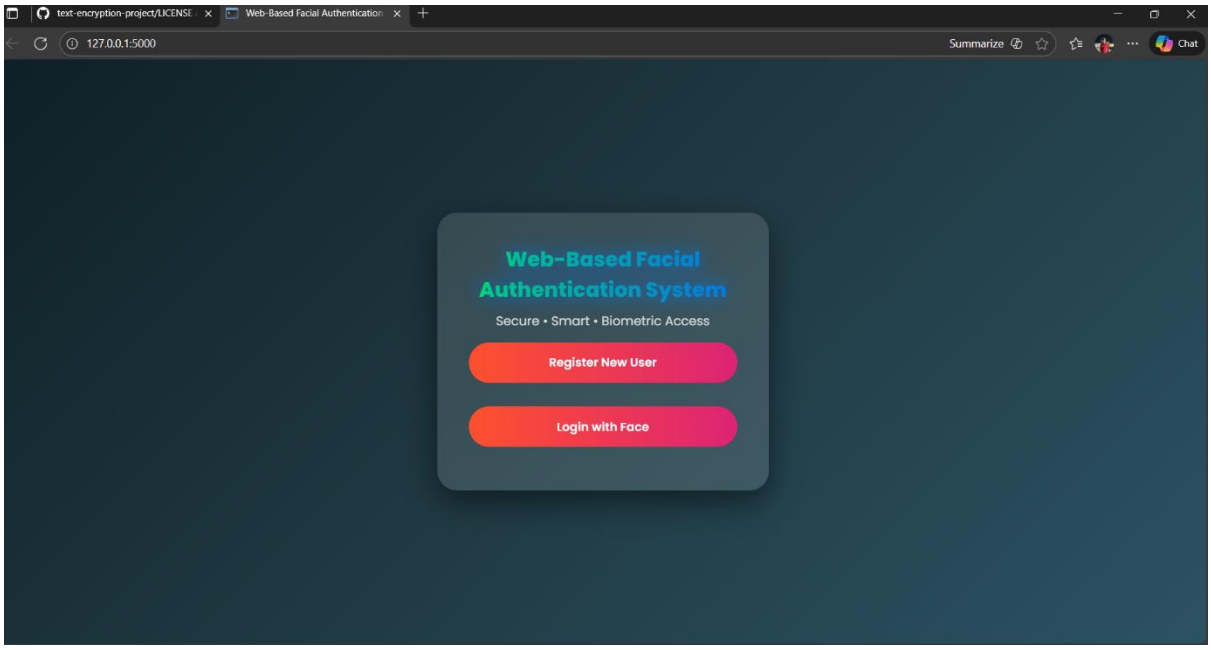


Figure 10.1: Home Page of Web-Based Facial Authentication System

This screen is the landing page of the application. It serves as the main entry point for users and provides clear navigation for system usage.

Key Elements:

- System title: Web-Based Facial Authentication System
- Tagline: Secure • Smart • Biometric Access
- Two primary buttons:
    - Register New User – Navigate to registration module
    - Login with Face – Navigate to authentication module

Functional Significance:
The home page separates the flow for new and existing users, ensuring smooth user interaction and an intuitive interface. The design promotes clarity and simplicity, encouraging secure access.

10.2 User Registration Screen

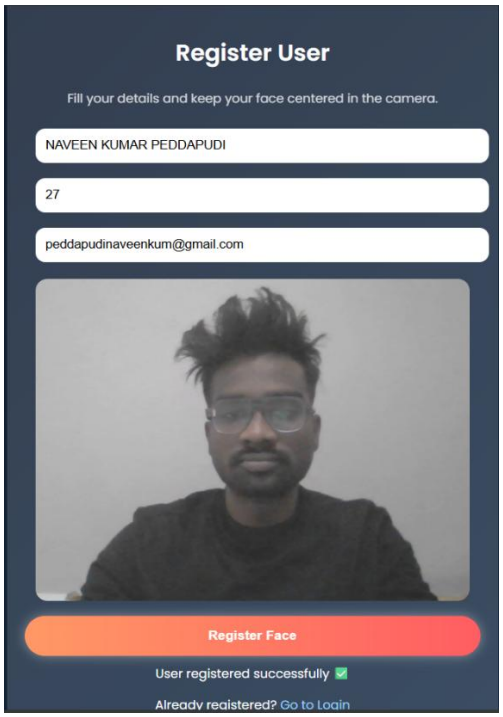


Figure 10.2: User Registration Interface

This screen allows the user to enroll into the system using their facial data.

Visible Components:

- Input fields for:
    - Full Name
    - Age

- Email

- Live webcam preview for face capture
- Register Face button
- Status message: "User registered successfully ✅ "

Operational Function:
This interface captures the user's biometric data and personal information. The face is detected, stored, and used to train the facial recognition model. Proper user guidance ensures accurate capture and improved recognition accuracy.

10.3 Face Login Screen with Liveness Detection

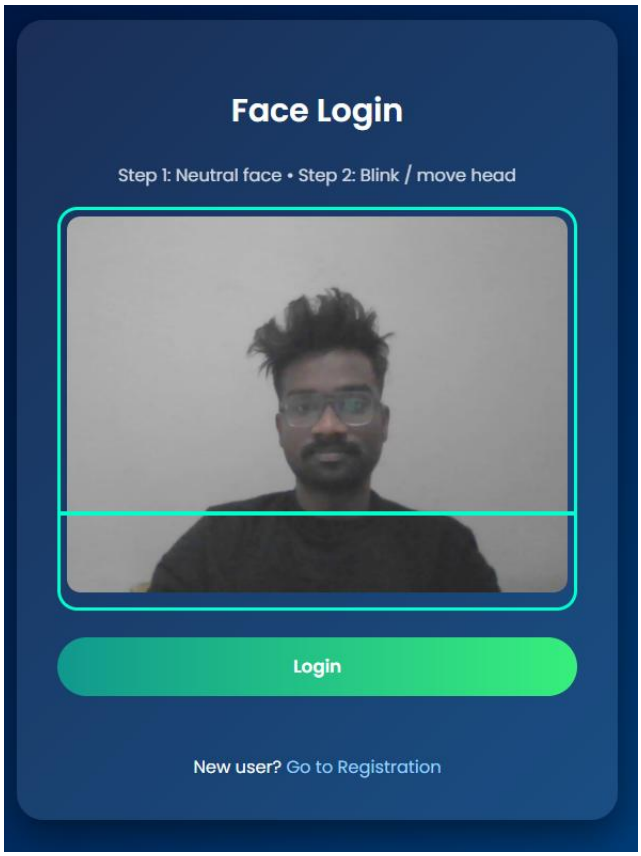


Figure 10.3: Face Login Interface

This screen validates user identity using real-time facial recognition and liveness detection.

Key Features:

- **Step instructions:**
  - Step 1: Neutral face
  - Step 2: Blink / Move head

- Webcam scanner preview
- Login button
- Feedback messages for authentication status

Security Role:
This module prevents spoofing by analyzing movement and confirming the presence of a live person, ensuring genuine authentication.

10.4 Dashboard – Face Verified Successfully

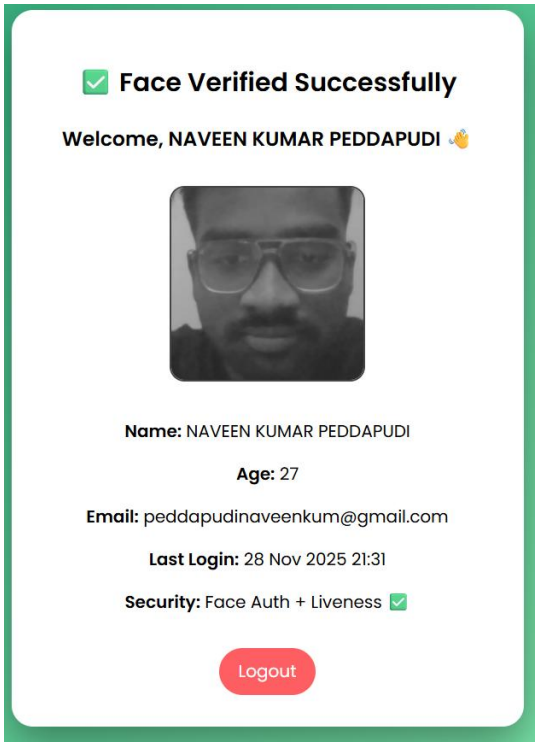


Figure 10.4: Authenticated User Dashboard

This screen confirms successful authentication and displays user information.

Displayed Information:

- Confirmation message
- User profile image
- Name, Age, Email
- Last Login Timestamp
- Security Status
- Logout Button

Security Importance:
This dashboard is protected by session control, ensuring access is granted only to verified users. The logout feature safely terminates the session.

11. TESTING AND VALIDATION

Test cases were performed to verify registration, authentication, and liveness detection accuracy.

12. SECURITY CONSIDERATIONS

- Session management
- Anti-spoofing mechanism
- Controlled data access

13. CONCLUSION

The Web-Based Facial Authentication System fulfills security requirements by integrating facial recognition and liveness detection techniques, providing an efficient and secure authentication solution.

14. FUTURE ENHANCEMENTS

- Integration of deep learning models
- Advanced liveness detection
- Cloud-based storage
- Multi-factor authentication