Two-Factor Authentication System – A Secure Login System with OTP and Biometric Verification

The **Two-Factor Authentication (2FA) System** enhances user login security by requiring **two-step verification** before granting access. This project protects accounts from unauthorized access by implementing **OTP-based and biometric authentication mechanisms**.

Key Features:

- **Email & SMS OTP Authentication** – Users receive a One-Time Password (OTP) via email or SMS for verification.
- **Biometric Authentication** – Supports **face recognition and fingerprint authentication** for added security.
- **Multi-Device Compatibility** – Works on both desktop and mobile devices.
- **Secure Token-Based Authentication** – Uses **JWT (JSON Web Tokens) or OAuth 2.0** for session management.
- **Brute-Force Attack Prevention** – Implements rate-limiting and CAPTCHA verification to prevent automated login attempts.

The system is built using **Flask/Django, React.js/Vue.js for UI, and Twilio/Google Authenticator for OTP generation**. **Facial recognition and fingerprint authentication** are implemented using **OpenCV and TensorFlow/Keras**.

This project enhances **web security by preventing unauthorized logins**, making it ideal for **banking apps, e-commerce sites, and enterprise authentication systems**.