Visualization

MULTIMODAL AUTHENTICATION SYSTEM

**1. Introduction**

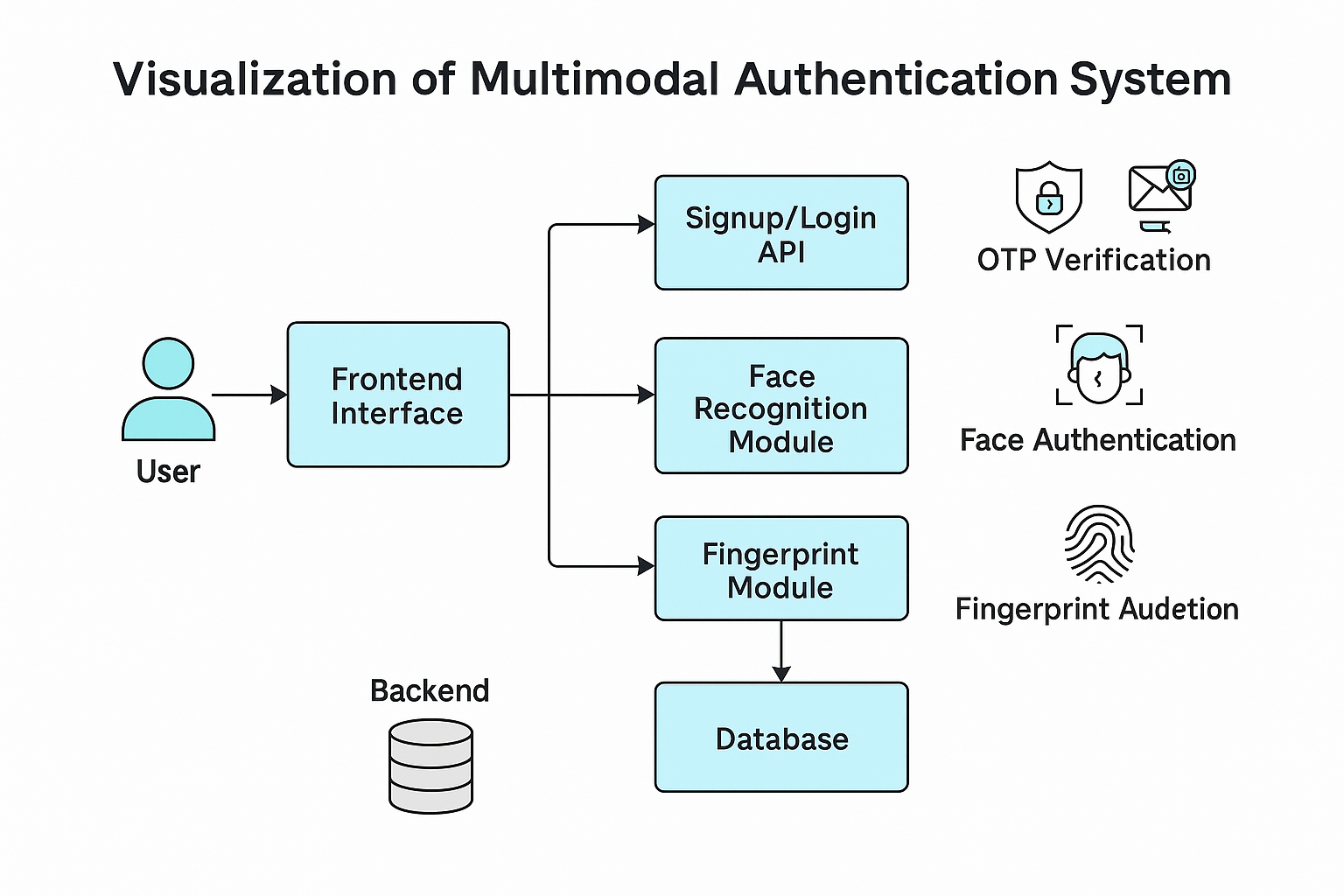
**1.1 Overview of the Project**

This project aims to create a secure and efficient authentication system using both face recognition and fingerprint recognition. The goal is to allow users to register and log in by verifying their face or fingerprint, which provides higher security than traditional password-based systems. By using these biometric methods, the system ensures that only authorized users can access their accounts.

**1.2 Key Features**

The authentication system includes:

* **User Registration**: Users can register by providing their username, email, or capturing their face or fingerprint.
* **User Login**: Users can log in by either matching their face or fingerprint.
* **Admin Dashboard**: Admins can view and manage user data, ensuring proper system maintenance.



**2. Registration Process**

This flow outlines how a new user registers into the system:

* **Enter Credentials:** The user starts by providing required information.
* **Username:** A unique identifier for the user.
* **Email:** Used for communication and verification purposes.
* **Password:** Secured password chosen by the user for future authentication.

**3. Login Flowchart**

This represents how a user logs in to the system:

* **Enter Email:** The user initiates login by entering their registered email.
* **Enter Password/OTP:** They must provide either their password or an OTP (sent via email/SMS).
* **Grant Access:** If the credentials are correct, access to the system is granted.

**4. Face Recognition Process**

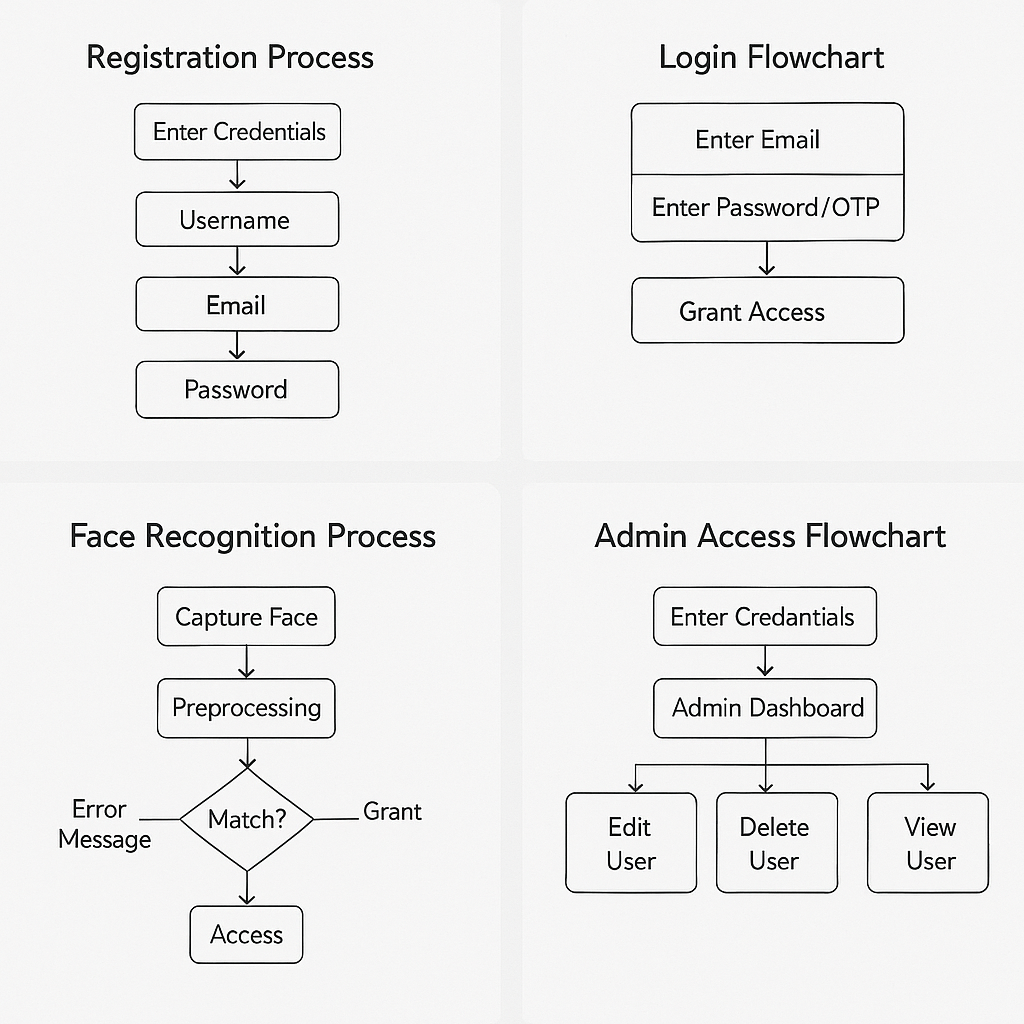
This covers the biometric verification through face recognition:

* **Capture Face:** A live image is captured via webcam or device camera.
* **Enter Username:** The user begins by entering their registered **username**.
* **Preprocessing:** The captured image is resized, normalized, and cleaned for better recognition accuracy.
* **Match?** The processed image is compared with stored face data and the username.
  + If it **matches**, access is **granted**.
  + If there's **no match**, an **error message** is shown.
* **Access:** Granted only when the facial data matches a stored profile

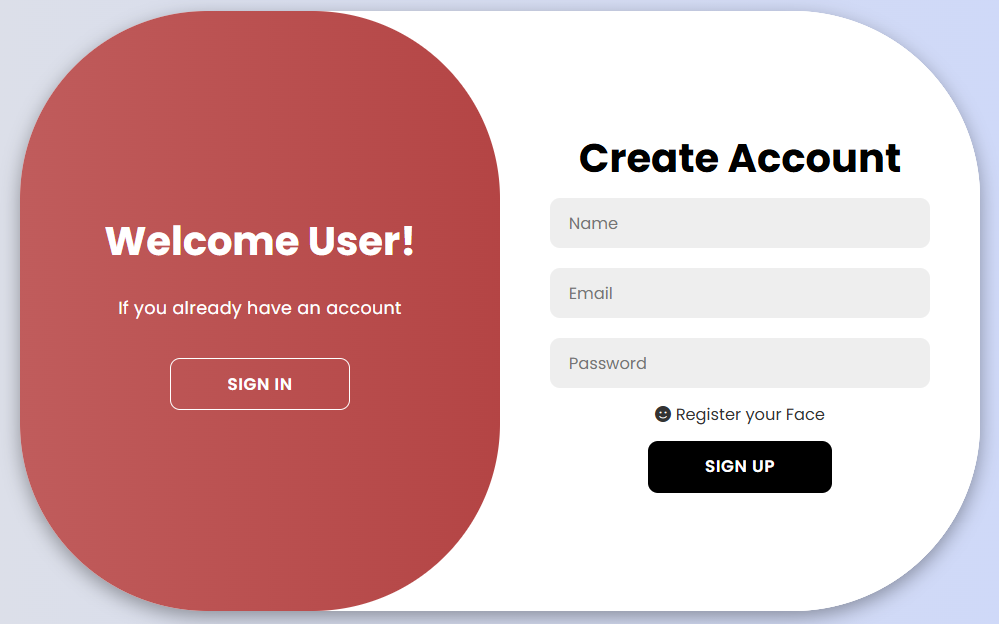
**5. Admin Access Flowchart**

This flow represents how an admin logs in and manages users:

* **Enter Credentials:** The admin enters a username and password (admin-only credentials).
* **Admin Dashboard:** Upon successful login, the admin accesses the dashboard.
* From the dashboard, the admin can:
  + **Edit User:** Modify user information (email, biometric data, etc.).
  + **Delete User:** Remove a user profile from the system.
  + **View User:** View the list of all registered users with their data summaries



REGISTER PAGE:



SIGN IN PAGE

