AVN INSTITUTE OF ENGINEERING & TECHNOLOGY
Accredited by NAAC & NBA
An Autonomous Institute Affiliated to JNTU Hyderabad

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (Cyber Security)

SECURE SENTINEL – A FACIAL RECOGNITION SECURITY SYSTEM FOR ANDROID

PROJECT GUIDE - Mr. K. Krishna Reddy

Group Members:-

- E. Lavanya - 215U1A6216
- Ch. Dhanunjay - 215U1A6212
- P. Pavani - 215U1A6249
- G. Jetin Sairam - 215U1A6220
- G. Madhukar - 215U1A6222

Abstract

The project "Facial Recognition Security System web App" is designed to enhance mobile device security through continuous facial monitoring. The app constantly scans for faces using the device's front camera and cross-references detected faces against a database of registered users. When an unregistered face is detected, the system immediately locks the device screen to prevent unauthorized access.

Simultaneously, the app covertly captures an image of the unregistered individual and securely sends this photo to a predefined email address, enabling the device owner to be promptly alerted of potential security breaches. This solution combines real-time biometric authentication with stealthy intrusion detection, aiming to provide robust, automated protection for Android devices against unauthorized use.

Problem Statement

With the increasing dependence on mobile devices for personal and sensitive information, traditional security methods such as PINs, passwords, and pattern locks are often vulnerable to unauthorized access. These conventional methods can be easily compromised or bypassed, leading to potential privacy breaches and security risks. There is a need for an intelligent and automated security solution that can actively monitor and prevent unauthorized device access in real time without relying solely on manual user intervention.

Aim

The aim of this project is to develop a web application that employs continuous facial recognition to enhance device security. The app will monitor the device's surroundings in real time, identify whether the user is registered or not, automatically lock the screen when an unregistered face is detected, and discreetly capture and send an image of the intruder to a specified email address. This system aims to provide seamless, proactive protection against unauthorized access, ensuring improved security and peace of mind for Android users.

Objective

USER-FRIENDLY INTERFACE

Design a user-friendly interface for easy setup and operation.

FACE RECOGNITION

Develop an Android web application that utilizes facial recognition technology for real-time monitoring of user access.

STEALTH EXECUTION

Integrate a feature to capture and email images of unregistered individuals discreetly.

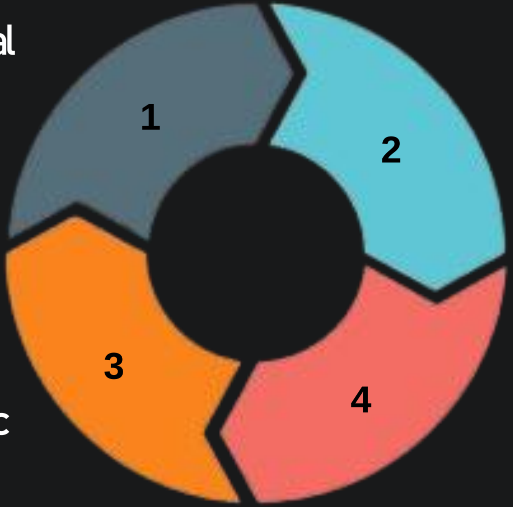
SECURITY & DATA TOOLS

Ensure user privacy and data security throughout the application's functionality.

Scope

Implement accurate facial recognition for user identification.

Provide easy management of registered user face data.



Enable real-time face monitoring with automatic screen locking.

Ensure secure handling of data and captured images.

Existing System

Traditional Security:

Reliance on PINs and passwords, easily bypassed.

Other Apps:

Lack real-time monitoring and automatic responses.

Surveillance Systems:

Fixed-location use, not mobile device solutions.

Biometric Authentication:

Limited to fingerprints, lacking continuous monitoring features.

Limitations of Existing System

Traditional Security:

Reliance on PINs and passwords, easily bypassed.

Limitations:

Vulnerable to theft, guessing, and social engineering attacks.

Other Apps:

Lack real-time monitoring and automatic responses.

Limitations:

Often inaccurate in varied lighting and angles; limited functionality.

Surveillance Systems:

Fixed-location use, not mobile device solutions.

Limitations:

High cost, installation complexity, and lack of mobility for personal use.

Biometric Authentication:

Limited to fingerprints, lacking continuous monitoring features.

Limitations:

Limited to specific features (e.g., fingerprints) and may not work for all users (e.g., injuries).

Proposed System

Real-Time Facial Monitoring

Continuous facial recognition for real-time monitoring.

Secure User Data Management

Secure storage and management of registered user data.

Automatic Screen Lock

Automatic screen lock on detecting unregistered faces.

Instant Email Alert

Email alert with captured image to the device owner.

Stealth Intruder Capture

Silent capture of unrecognized faces without alerting intruders.

User-Friendly Interface

User-friendly interface for easy setup and operation.

Advantages

1. Enhanced Security: Provides a higher level of security compared to traditional methods by using advanced facial recognition technology.

2. Proactive Protection: Automatically locks the device when an unrecognized face is detected, preventing unauthorized access.

3. Intruder Identification: Captures images of potential intruders discreetly, aiding in security investigations.

4. Real-Time Alerts: Sends instant notifications to the device owner, ensuring they are aware of any security breaches.

5. User Management: Allows easy addition and removal of registered users, providing flexibility in user access.

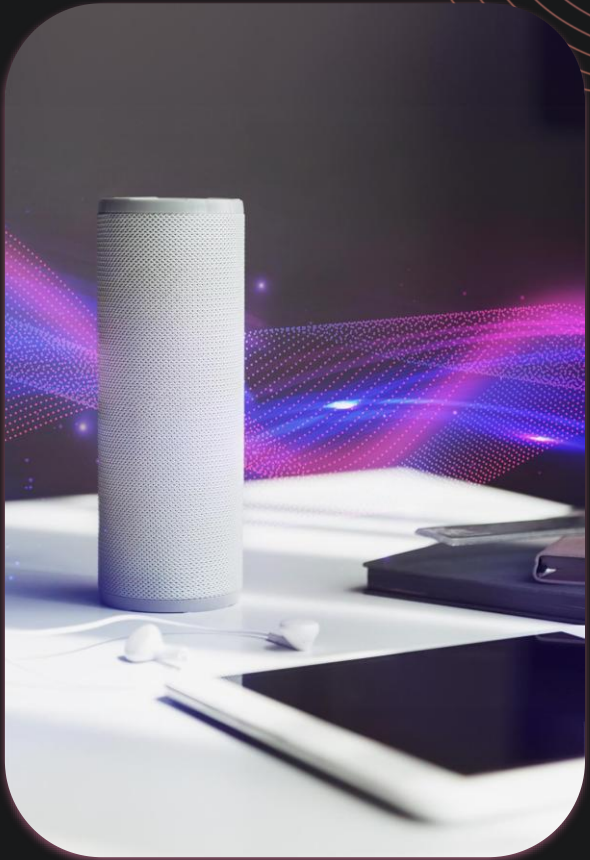
Software & Hardware Requirements

Software required:

- Visual Studio Code
- Android studio
- Python 3.11

Hardware Required:

- PC (Personal Computer)
- Android Device



Requirements Gathering

Functional Requirements

- Continuous face scanning using the front camera.
- Automatic screen lock for unregistered faces.
- Secretly capture photos of unrecognized faces.
- Email captured images to the user.

Non-Functional Requirements

- Efficient battery usage.
- Data encryption for user security.
- Responsive and user-friendly interface.
- Reliable performance in various lighting conditions.

Software Requirement Specifications

- Compatible with Android 14 or later.
- Requires Camera, Display over other apps permission.
- Requires installation of specific libraries for facial recognition (e.g., OpenCV, Dlib).
- Requires a working front camera

Analysis

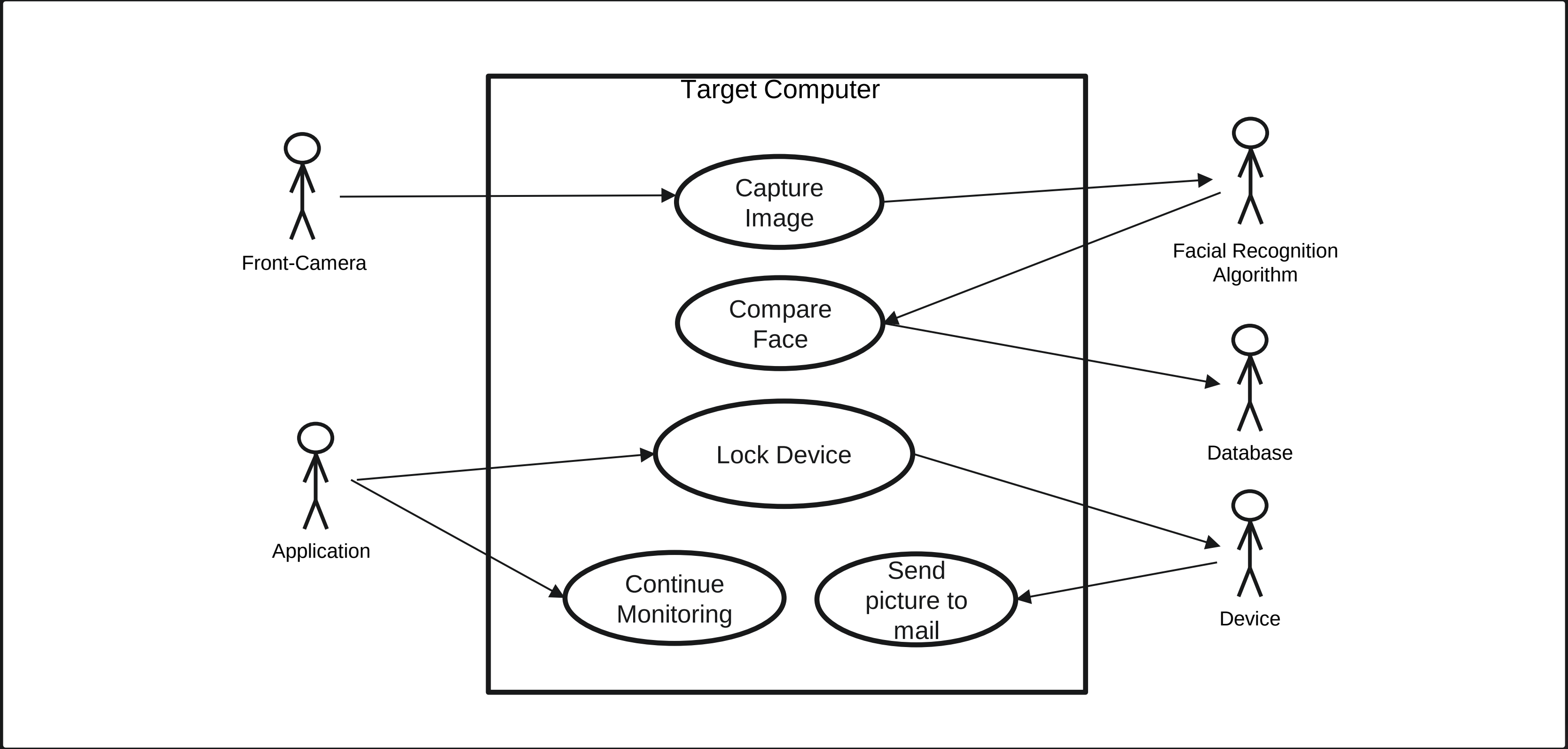
1. Technological Feasibility: Current advancements in facial recognition technology and mobile hardware capabilities make the implementation of this system viable.

2. User Acceptance: The convenience of biometric authentication is likely to be well-received by users, enhancing adoption rates.

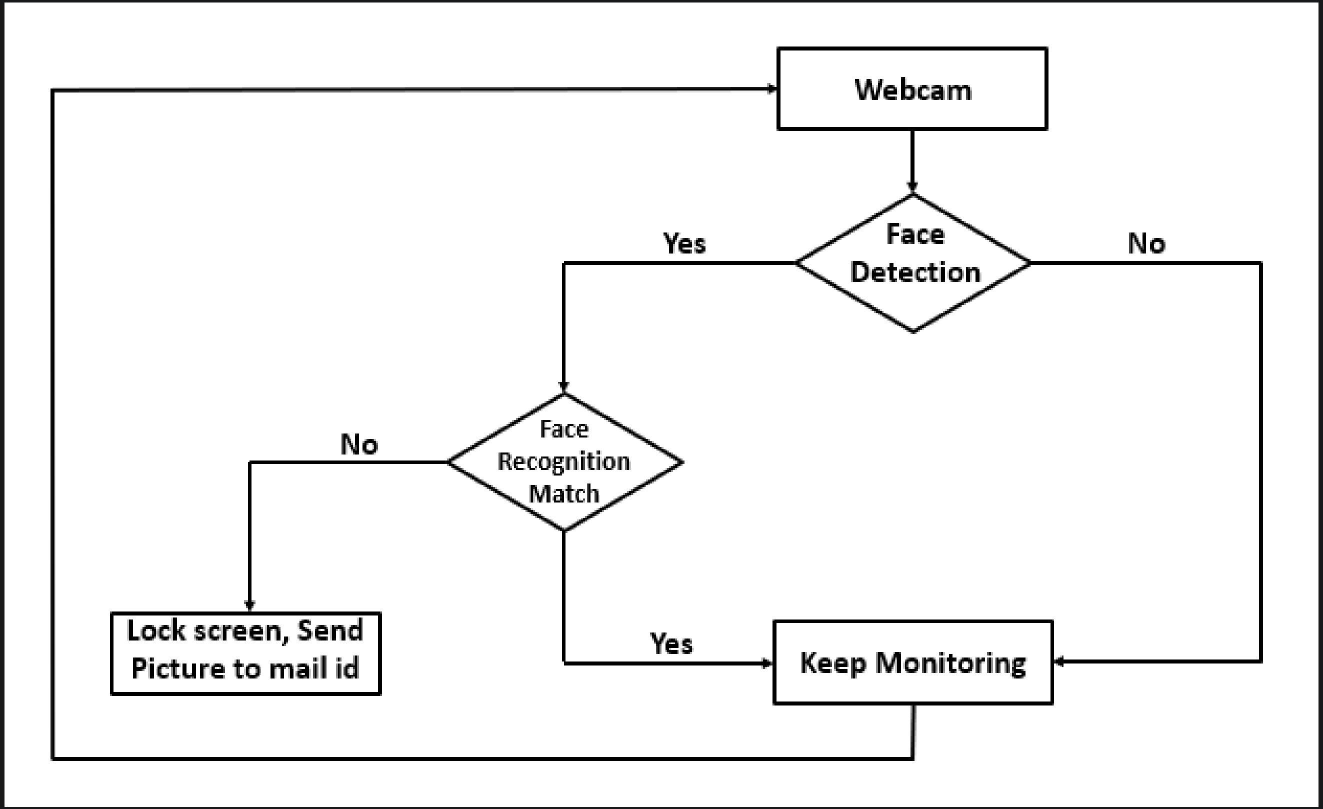
3. Privacy Concerns: Addressing user privacy and data protection will be critical, requiring robust security measures and transparent data handling practices.

4. Cost-Benefit Analysis: Evaluating the costs of development and implementation against the potential benefits in security and user satisfaction will be essential for project viability.

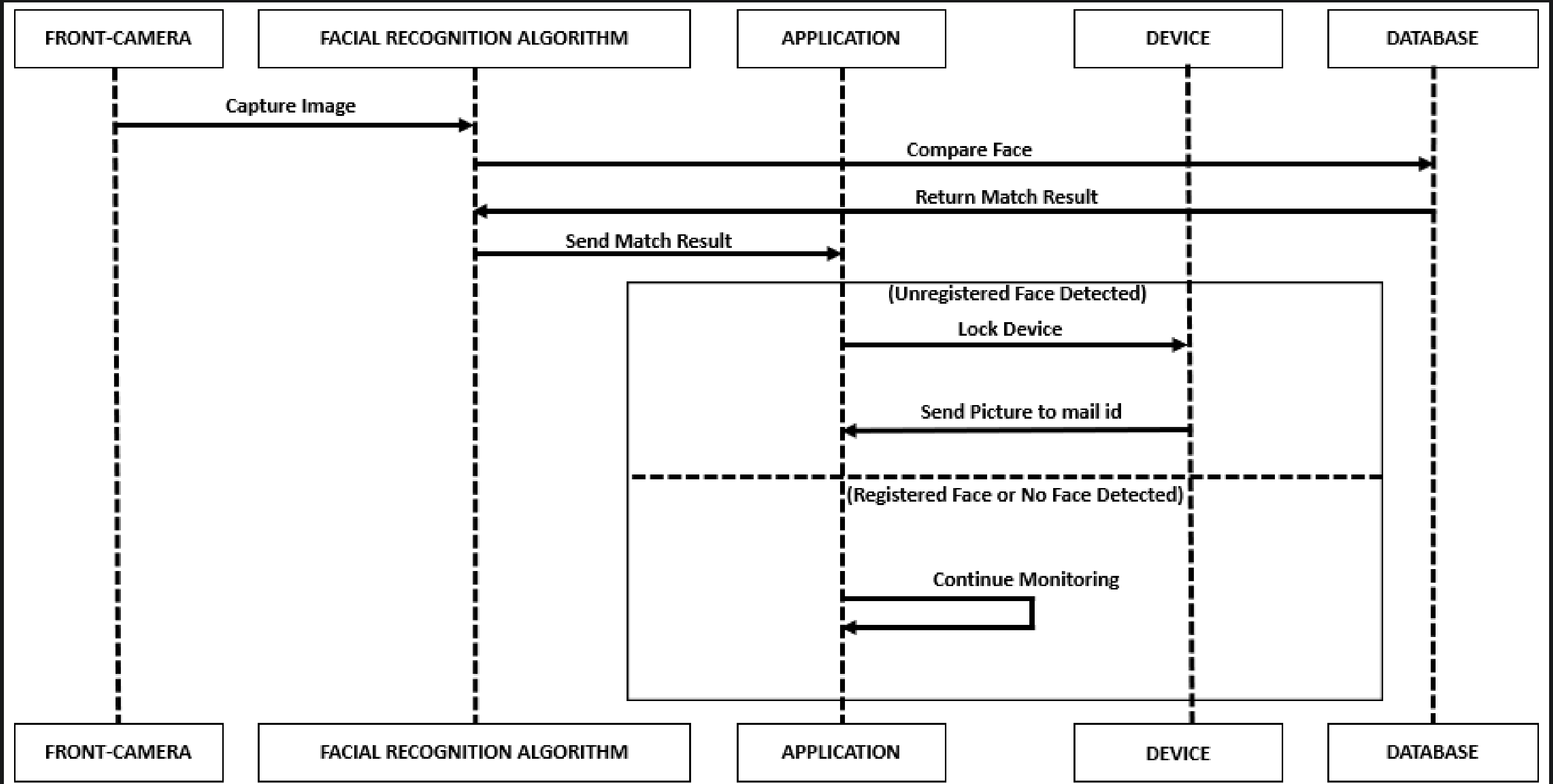
Use-Case Diagram



Flow Chart


Webcam
Face Detection
Yes
No
Face Recognition Match
No
Yes
Lock screen, Send Picture to mail id
Keep Monitoring

UML Sequence Diagram



Test Cases

Test Case ID	Test Cases
TC_01	Registered face detected
TC_02	Unregistered face detected
TC_03	No face detected

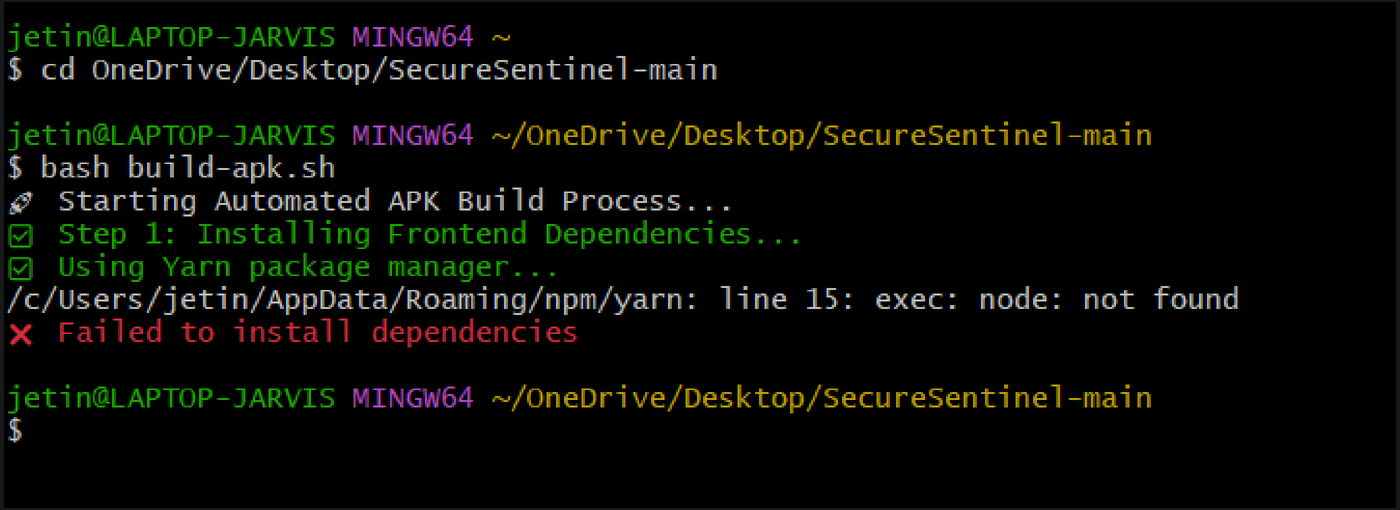
Test Case Scenarios

Project Title	Facial Recognition Security System
Project Name	Secure Sentinel
Project Objective	Using facial Recognition to provide security from unauthorized Physical Access
Test Objective	Testing different possible scenarios for each possible outcome

Test Case Author	Ch. Dhanunjay - 6212
Test Case Reviewer	E. Lavanya -6216
Test Case Version	v3.1.2
Test Execution Date	05-01-2025

Test Case ID	Test Pre-steps	Input Data	Expected Result	Actual Result	Execution Status
TC_01	1) Run the Web application 2) Start the Monitoring	Registered Face	Screen stays ON	Screen stays ON	PASS
TC_02	1) Run the Web application 2) Start the Monitoring	Unregistered Face	Device locks and Email alert is sent	Device locks and Email alert is sent	PASS
TC_03	1) Run the Web application 2) Start the Monitoring	No Faces Detected	Screen stays ON	Screen stays ON	PASS

Bugs & Errors



```
jetin@LAPTOP-JARVIS MINGW64 ~
$ cd OneDrive/Desktop/SecureSentinel-main

jetin@LAPTOP-JARVIS MINGW64 ~/OneDrive/Desktop/SecureSentinel-main
$ bash build-apk.sh
🚀 Starting Automated APK Build Process...
☑ Step 1: Installing Frontend Dependencies...
☑ Using Yarn package manager...
/c/Users/jetin/AppData/Roaming/npm/yarn: line 15: exec: node: not found
✗ Failed to install dependencies

jetin@LAPTOP-JARVIS MINGW64 ~/OneDrive/Desktop/SecureSentinel-main
$
```

ABOUT THE ERROR:

A Runtime Error occurred while Building the web application due to the absence of the dependencies like yarn and MongoDB.

Bugs & Errors

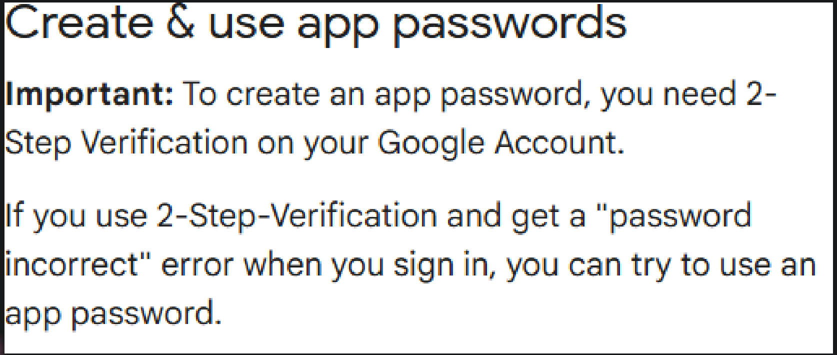
We tried the following:

- Installing the yarn dependencies from MongoDB from the MongoDB.com website and installed it in our system
- Added MongoDB path to the system variables

Outcome:

The build was successfully completed with no runtime errors and the web application was ready for local hosting as a webpage in the browser

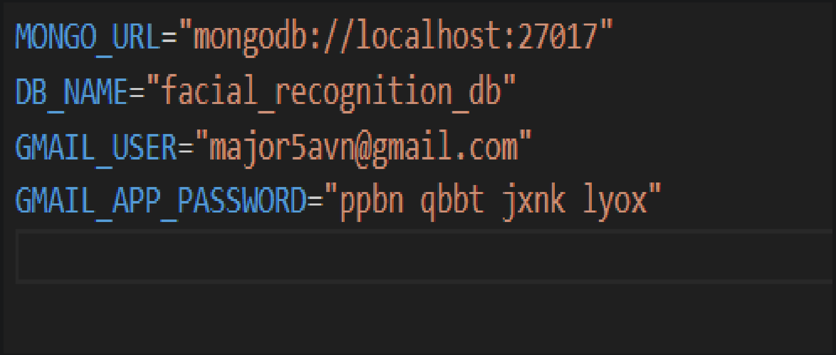
Bugs & Errors



Create & use app passwords

Important: To create an app password, you need 2-Step Verification on your Google Account.

If you use 2-Step-Verification and get a "password incorrect" error when you sign in, you can try to use an app password.



```
MONGO_URL="mongodb://localhost:27017"
DB_NAME="facial_recognition_db"
GMAIL_USER="major5avn@gmail.com"
GMAIL_APP_PASSWORD="ppbn qbbt jxnk lyox"
```

ABOUT THE ERROR:

In order to create custom mail alert, Gmail id passwords were not being accepted into the smtp email service and 2FA was requested for the use of app passwords

Bugs & Errors

We tried the following:

- Enabled 2FA in the common mail id and activated the use of Gmail app passwords
- Utilized the App password (A series of 16-digit alphabetical combination) to act as the mail password instead of the real mail id password

Outcome:

We received the alert mails during testing to custom mail id that was entered in the user interface , and received accurate images of the intruders to the defined mail ID

Conclusion

In conclusion, the proposed facial recognition security system represents a significant advancement in mobile device protection. By integrating continuous monitoring, automatic responses to unauthorized access, and discreet intruder identification, this project addresses the limitations of existing security methods. The combination of enhanced security, user convenience, and real-time alerts ensures that users can confidently safeguard their devices against unauthorized access. As technology continues to evolve, implementing such innovative solutions will be crucial in maintaining personal security in an increasingly digital world. This project not only enhances user experience but also sets a new standard for mobile security, paving the way for future developments in biometric authentication.

THANKS!

Do you have any queries or concerns?