

A

PROJECT REPORT ON

FaceCrypt

SUBMITTED TO



Maharashtra Education Society's
MES SENIOR COLLEGE, PUNE
Approved by AICTE, New Delhi
&
Affiliated to SAVITRIBAI PHULE PUNE UNIVERSITY

IN PARTIAL FULFILLMENT OF
BACHELOR OF BUSINESS ADMINISTRATION
(COMPUTER APPLICATION)
(Academic Year 2024-25)

SUBMITTED BY
Vivek Dhanipkar (2230014)
Arya Kadam (2230030)
TYBBA-CA (Semester-VI)

UNDER THE GUIDANCE OF

Prof. Neha Kulkarni



MAHARASHTRA EDUCATION SOCIETY'S
(SINCE 1860)

MES SENIOR COLLEGE, PUNE

(BBA, BBA - IB, BBA - CA)

131, Mayur Colony, Ch. Rajaram Maharaj Path, Kothrud, Pune - 411038, Maharashtra, India | Ph.: 020-25463453 / 25440196
E-mail : info.bba@mespune.in | https:// bba.mespune.in

Approved by AICTE, New Delhi & Affiliated to Savitribai Phule Pune University, Pune

Certificate

This is to certify that the Project Report entitled

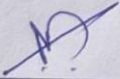
FaceCrypt

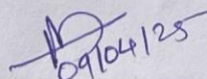
Is prepared by


Virek Dhanipkar & Arya Kadam


Student(s) of TY BBA-CA, Sem-VI for the Academic Year 2024-25 at MES Senior College, Pune.

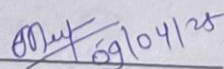
To the best of our knowledge, this is the original study done by the said student(s) and important sources used by him/her/them have been duly acknowledged in this report. The report is submitted in the partial fulfilment of TY BBA-CA, Sem-VI for the Academic Year 2024-25 as per the rules and prescribed guidelines of Savitribai Phule Pune University, Pune.


Project Guide


Head of the Department: BBA-CA


Vice Principal


Internal Examiner


External Examiner

ACKNOWLEDGMENT

I would like to express my sincere gratitude to **MES Senior College, Pune** for providing me with the opportunity to undertake this academic project as part of my **TYBBA-CA Semester VI curriculum**.

I extend my heartfelt thanks to **Prof. Neha Kulkarni**, my project guide, for their invaluable guidance, continuous support, and constructive feedback throughout the project. Their insights and encouragement have been instrumental in the successful completion of this work.

I am also grateful to our **Principal Dr. Ravindra Vaidya, Vice Principal Dr. Poonam Rawat**, and all faculty members of the **MES Senior College, Pune** for their support and motivation during this project.

A special thanks to my peers, friends, and family for their encouragement and assistance throughout the process.

Vivek

Vivek Dhanipkar (2230014)

Arya

Arya Kadam (2230030)

INDEX

Sr. No.	Topic	Page No.
1	CHAPTER 1: INTRODUCTION 1.1 Need of System 1.2 Scope & Feasibility of Work 1.3 Operating Environment – H/w & S/w 1.4 Architecture of system 1.5 Detail Description of Technology Used	1-3
2	CHAPTER 2: PROPOSED SYSTEM 2.1 Proposed System 2.2 Objectives of System	4
3	CHAPTER 3: ANALYSIS & DESIGN 3.1 ERD 3.2 UML Diagrams 3.3 Data Dictionary	5-10
4	CHAPTER 4: OUTPUTS AND REPORTS TESTING 4.1 Test Plan 4.2 Black Box Testing or Data Validation Test Cases 4.3 White Box Testing or Functional Validation Test cases and results	11-14
5.	CHAPTER 5: USER MANUAL 5.1 User Interface Design (Screens etc.) 5.2 Limitations 5.3 Future enhancement BIBLIOGRAPHY ANNEXURE: Sample Program Code	15-18

INTRODUCTION

Need for System:

- Versatility: Integrates with sectors like banking, e-commerce, healthcare, and government.
- Data Security: Protects sensitive information from unauthorized access.
- Identity Theft Prevention: Prevents fraud using facial recognition.
- Regulatory Compliance: Assists in meeting security regulations.
- User Convenience: Provides a simple and secure authentication experience.
- By adopting FaceCrypt, organizations can minimize security risks, ensuring the safety of their data, customers, and reputation.

Scope and Limitations of existing system:

SCOPE: -

- 1) Public Services:
 - Border control and immigration
 - Law enforcement and crime prevention
 - Public safety and surveillance
- 2) Commercial Applications:
 - Retail analytics and marketing
 - Banking and financial security
 - Healthcare identity verification
- 3) Consumer Electronics:
 - Smartphone authentication
 - Smart home device control
 - Gaming console identity verification
- 4) Education and Research:
 - Attendance tracking
 - Behavioral research and development

LIMITATIONS: -

Facial recognition systems face challenges like reliance on traditional authentication methods, vulnerable biometric data storage, and inconsistent accuracy due to lighting, facial expressions, or occlusions. Additionally, they are susceptible to advanced threats like deepfakes, spoofing, and adversarial attacks, compromising system security

Operating Environment – H/w & S/w:

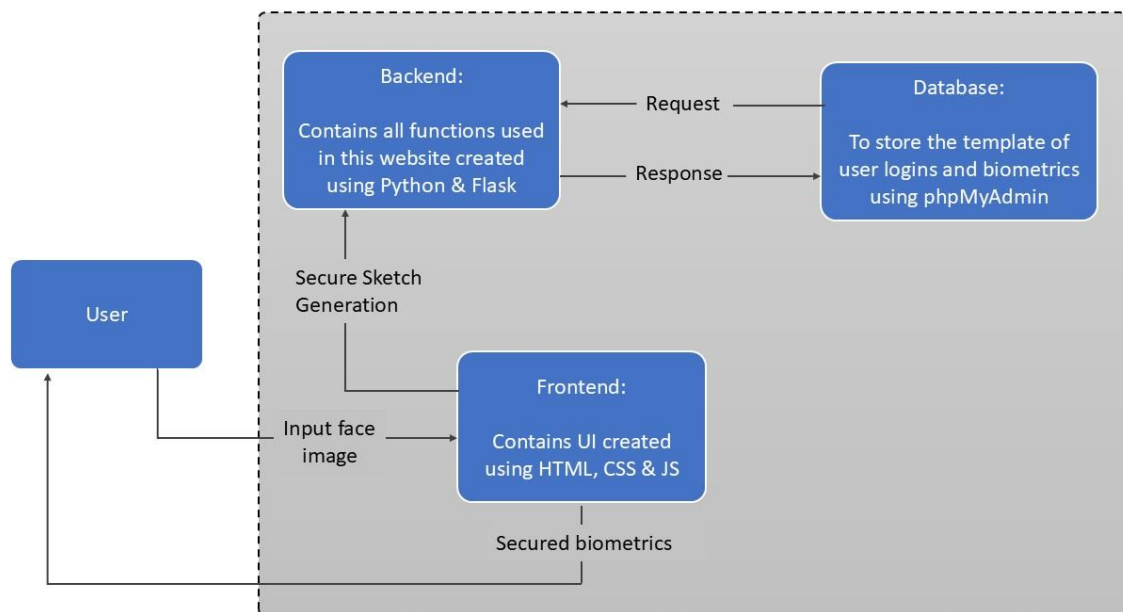
Hardware:

- GB RAM
- 512 GB SSD
- Intel core i5

Software:

- Frontend: HTML, CSS, and JavaScript
- Backend: Python
- Database: phpMyAdmin
- Server: Flask

Architecture of system:



Detailed Description of Technology used:

The FaceCrypt system utilizes the following technologies:

1. HTML, CSS, and JavaScript: Used for developing the frontend of the system.
2. Python: A high-level programming language used for developing the backend of the system.
3. Flask: A lightweight web framework used for developing the backend API.
4. phpMyAdmin: A web-based database management tool used for storing and managing biometric data.

PROPOSED SYSTEM

Proposed System:

This project proposes a secure facial recognition system that utilizes a randomized Convolutional Neural Network (CNN) to generate protected biometric templates. The system integrates user-specific keys to introduce randomness, enhancing template security.

The proposed system operates as follows:

- 1) **Camera Activation:** The camera is opened to capture the user's face image.
- 2) **Face Detection:** The system detects the face in the captured image using facial detection algorithms.
- 3) **Face Alignment:** The detected face is aligned to ensure proper positioning and orientation.
- 4) **Protected Template Generation:** A protected biometric template is generated using the randomized CNN, integrating user-specific keys to introduce randomness.
- 5) **Secure Sketch Generation:** A secure sketch is created from the user-specific key and an intermediate feature, which is stored in the system.

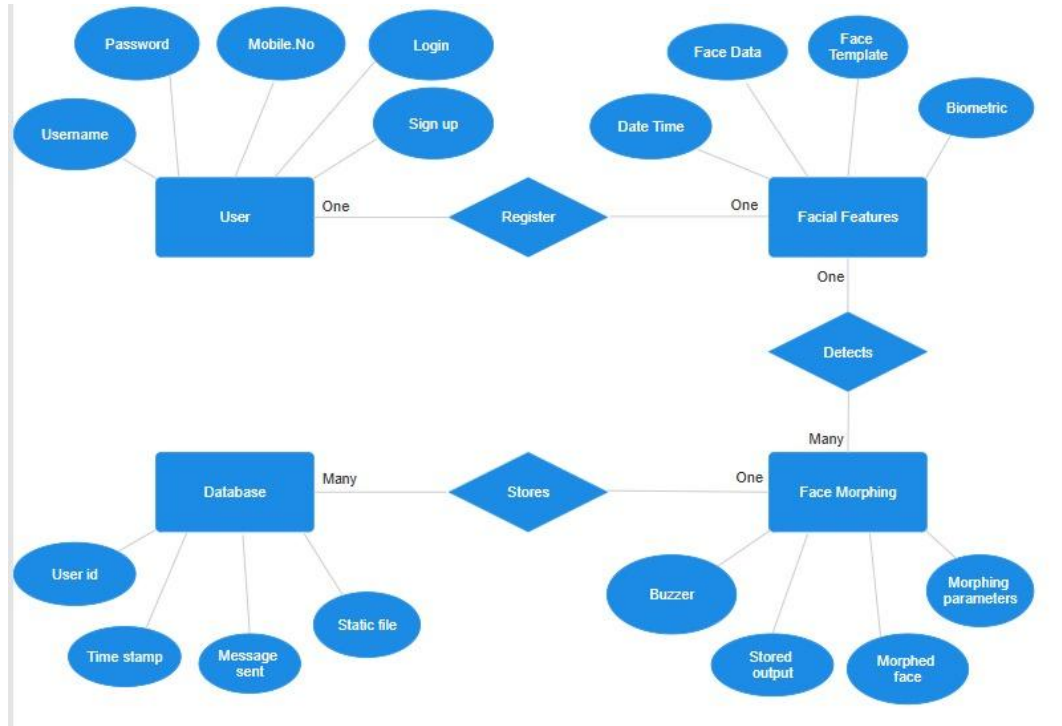
Objectives of System:

The primary objectives of the proposed system are:

- 1) **To develop a secure biometric authentication method:** Using facial recognition and protected template generation to prevent unauthorized access.
- 2) **To ensure template security:** By introducing randomness through user-specific keys and storing secure sketches instead of keys.
- 3) **To construct a protected biometric system:** Whose stored deep templates are non-invertible, cancellable, and discriminative.

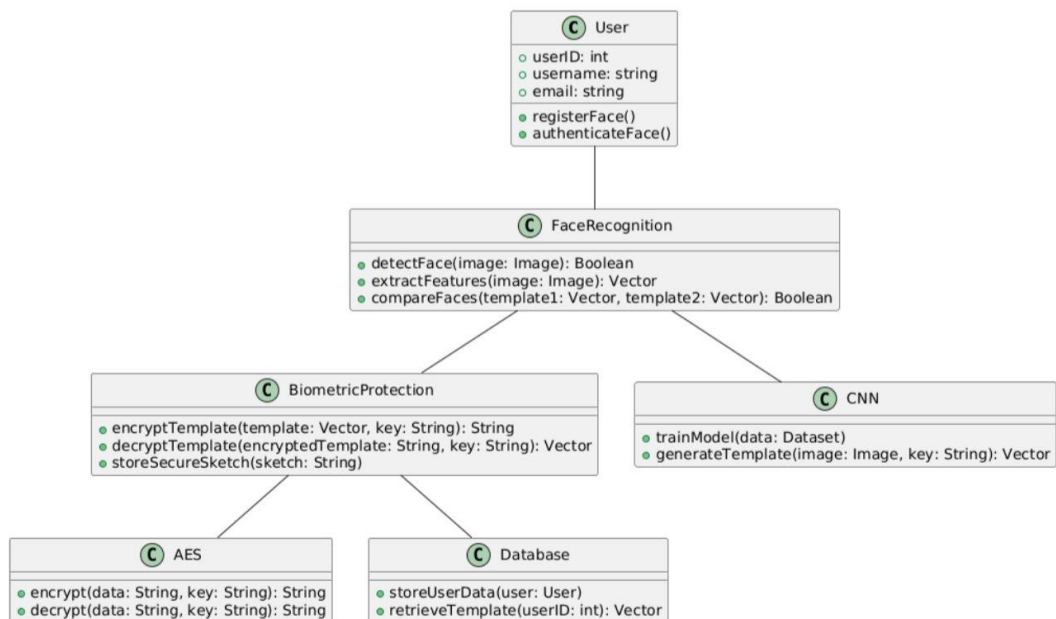
DESIGN

ERD:

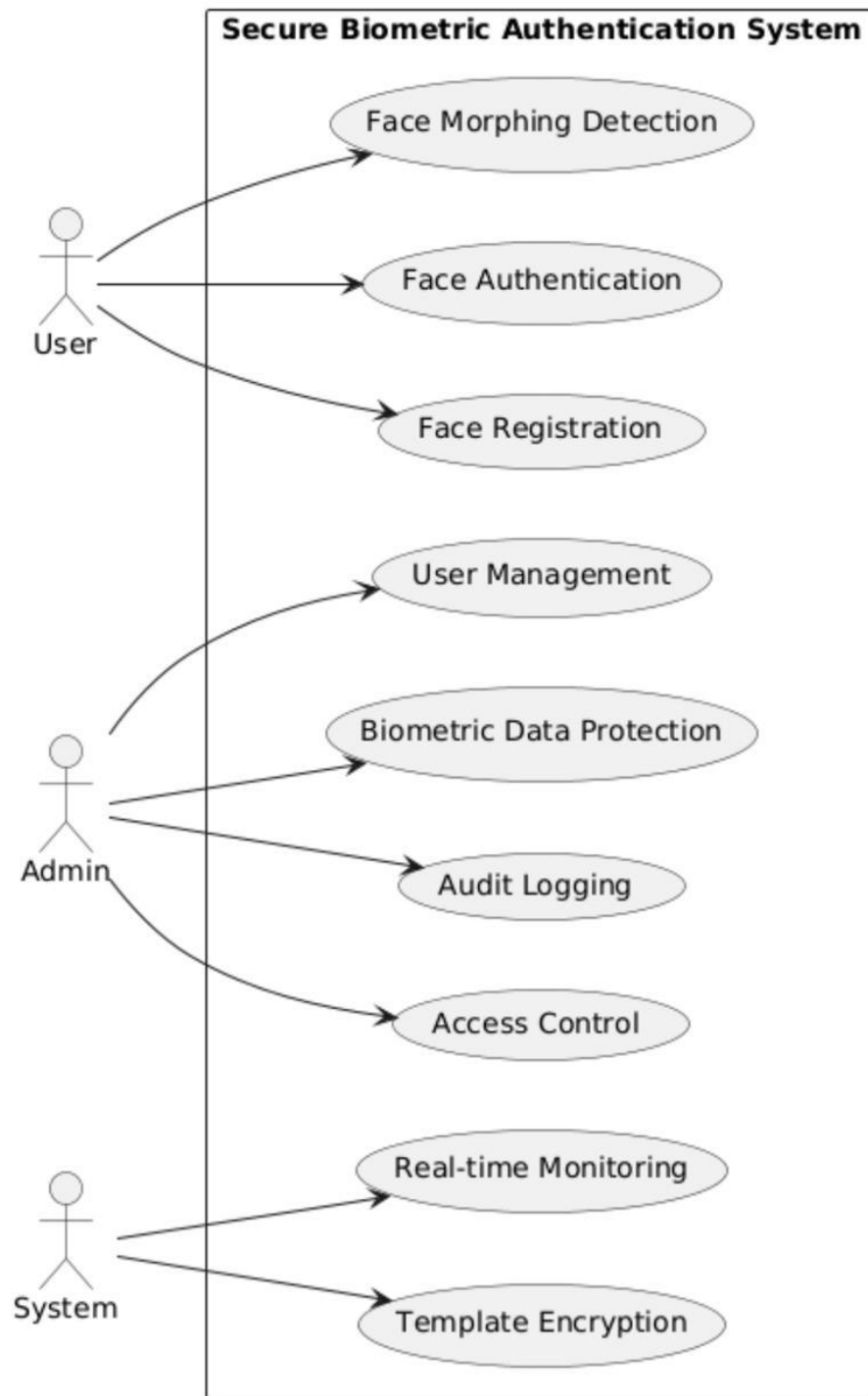


UML:

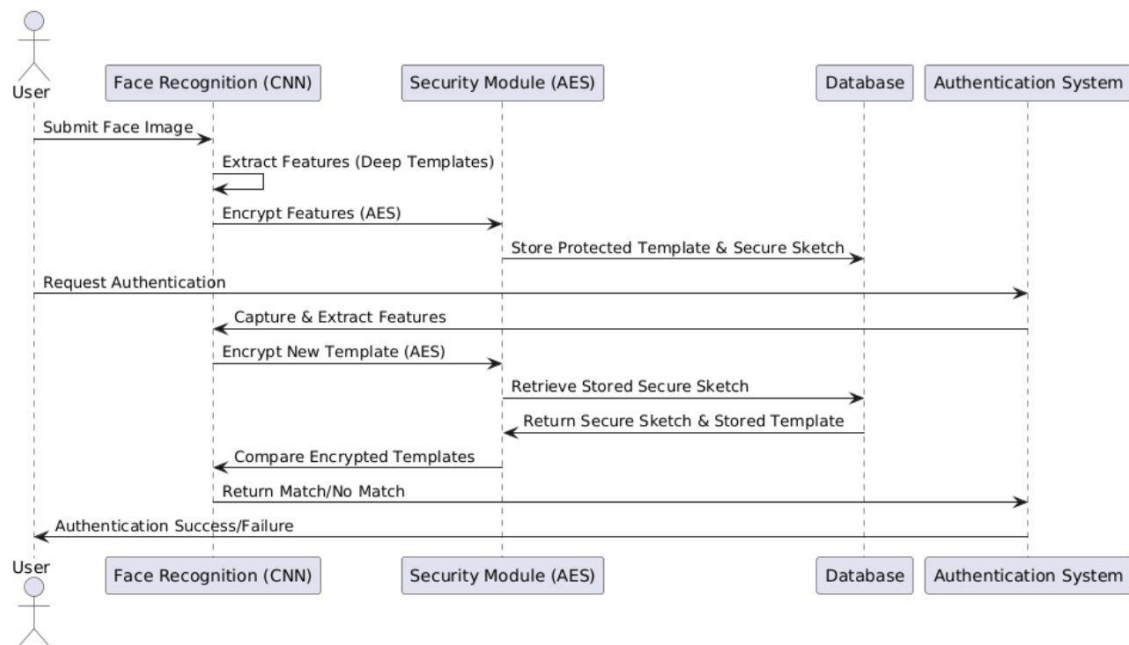
- Use Case Diagram –



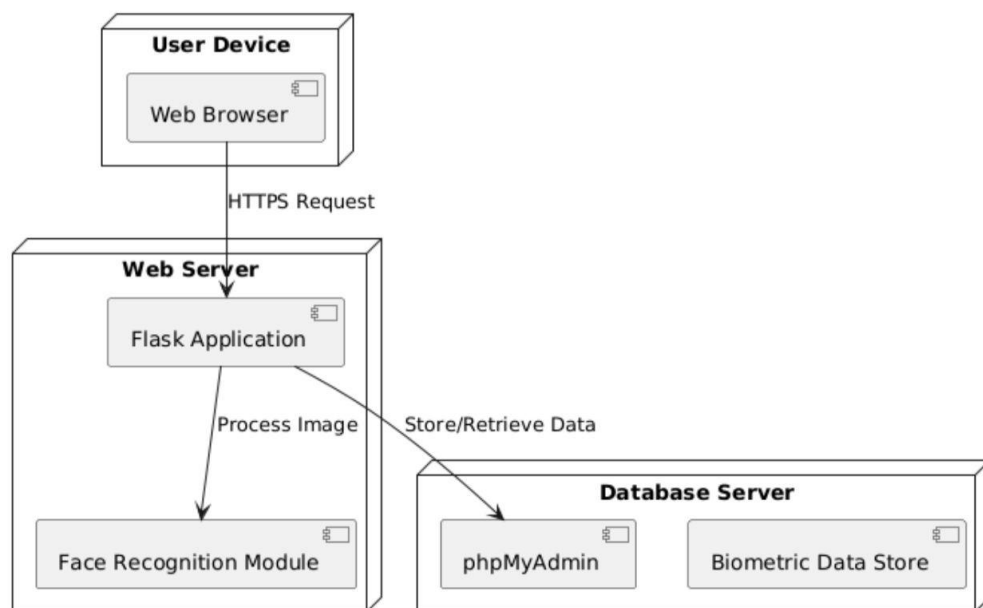
- Class Diagram –



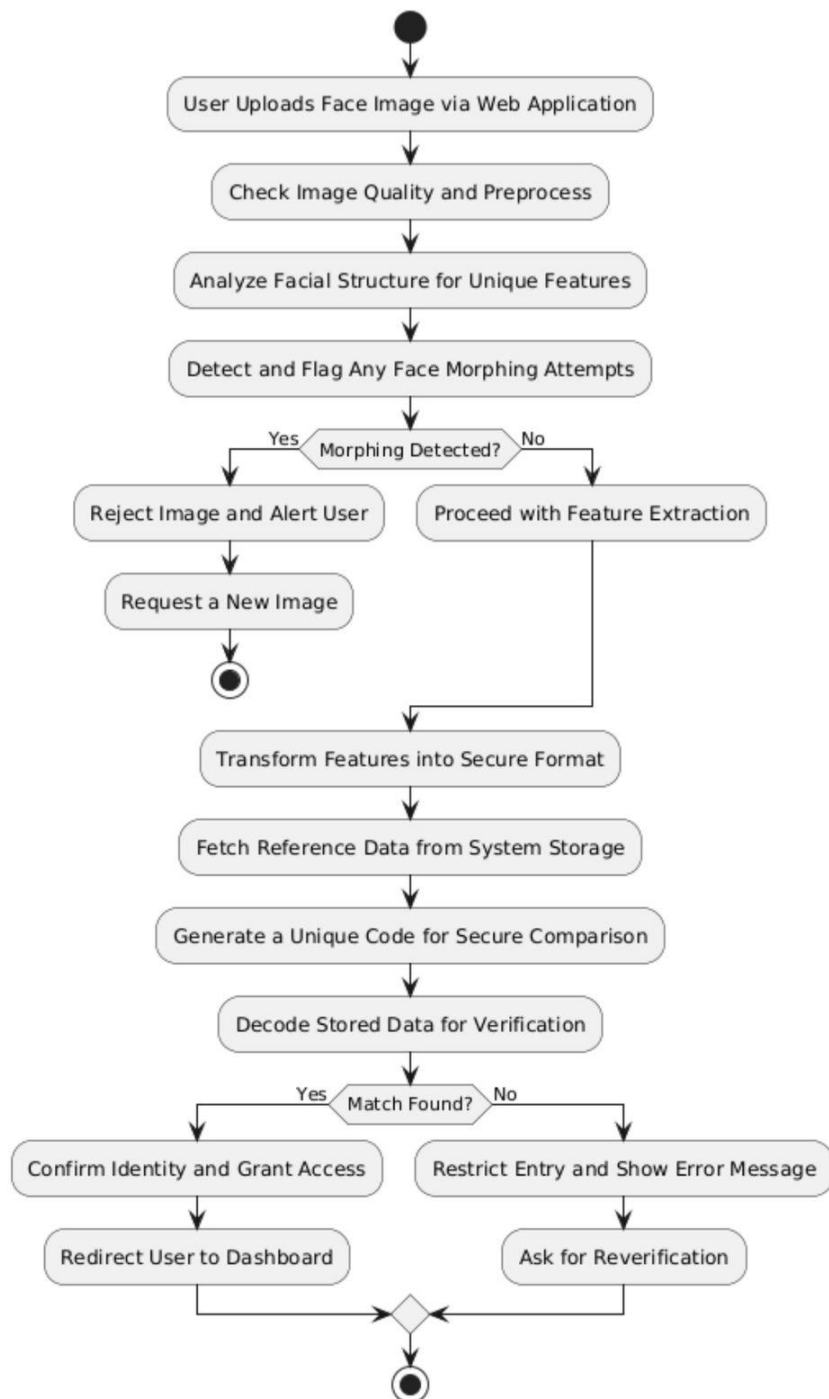
- Sequence Diagram –



- Deployment Diagram –



- Activity Diagram –



DATA DICTIONARY

- User Table –

Field Name	Data Type	Constraints
user_id	INT(primary key,Auto Increment)	Unique,Not Null
username	VARCHAR(100)	Unique,Not Null
email	VARCHAR(255)	Unique,Not Null
password_hash	VARCHAR(255)	Not Null
phone_number	VARCHAR(20)	Not Null
account_status	ENUM('Active','locked')	Default:'Active'
failed_attempts	TINYINT	Default:0
created_at	TIMESTAMP	Default: current Timestamp
updated_at	TIMESTAMP	Default: current Timestamp

- Face Recognition –

Field Name	Data Type	Constraints
Face_id	INT(Primarykey,Auto Increment)	Unique,Not Null
User_id	INT(foreign key)	Not Null
Face_embedding	BLOB	Not Null
Image_hash	VARCHAR(255)	Not Null
Encryption_key	VARCHAR(255)	Not Null
Model_version	VARCHAR(50)	Not Null
Detection accuracy	Float	Not Null
Created_at	TIMESTAMP	Default:Current Timestamp

- Face Authentication Logs Table –

Field Name	Data Type	Constraints
Auth_id	INT(Primarykey,Auto Increment)	Unique,Not Null
User_id	INT(Foreign key)	Not Null
Attempt_Time	TIMESTAMP	Default:Current Timestamp
Device_info	VARCHAR(255)	Not Null
status	ENUM('Success','failure')	Not Null
Failure_reason	VARCHAR(255)	Not Null

OUTPUTS AND REPORTS TESTING

Test Plan:

Introduction

The purpose of this test plan is to define the scope, objectives, approach, and resources required for testing the Secure Face Recognition Authentication System. This plan ensures that all functionalities work correctly and meet business and user requirements.

Scope

This test plan covers functional, usability, performance, security, and compatibility testing for the Secure Face Recognition Authentication System. The primary features to be tested include:

- 1) User authentication (registration, login, logout, password reset)
- 2) Face registration and recognition
- 3) Face morphing detection
- 4) Admin panel for managing users and system settings
- 5) Messaging system
- 6) Biometric data protection

Test Approach

The testing approach includes the following methodologies:

- 1) Manual Testing: Manual testing evaluates the system's functionality, user interface, user experience, and usability to ensure it meets required standards.
- 2) Automated Testing: Automated testing uses test automation tools to perform regression testing, ensuring changes or updates don't break existing functionality.
- 3) Security Testing: Security testing checks the system for vulnerabilities like SQL injection and data breaches to ensure it's secure and protects sensitive data.
- 4) Penetration Testing: Penetration testing simulates real-world attacks to test the system's security defences and identify potential vulnerabilities.

Test Environment

- Operating Systems: Windows, Linux
- Browsers: Chrome, Edge, Firefox
- Devices: Desktop, Laptop, Mobile
- Database: phpMyAdmin
- Backend: Python
- Frontend: HTML, CSS, JavaScript
- Server: Flask
- Modules: Biometric Data Protection, Face Registration, Face Authentication, Face Morphing Detection

Black Box Testing:

- Black Box Testing Test Cases: -

Modules	Test Case	Input	Expected Output
	Register a new user	Valid username, email, password, and face biometric	User registered successfully
Face Registration	Register an existing user	Existing username, email, password, and face biometric	Error message: User already exists
	Register with invalid face biometric	Invalid face biometric (e.g., multiple faces)	Alarm buzzes
	Authenticate with valid credentials	Valid username, password, and face biometric	Authentication successful
Face Authentication	Authenticate with invalid credentials	Invalid username, password, or face biometric	Access denied
	Authenticate with face morphing	Valid username, password, and face biometric with face morphing	Authentication successful only if face morphing actions are performed correctly
	Send a message to a registered user	Valid recipient username and message	Message sent successfully, updated in database with timestamp (e.g., 2023-02-20 14:30:00)
Message Sending	Save a message as draft	Valid message content, click "Save Draft"	Message saved as draft, updated in database with timestamp (e.g., 2023-02-20 14:30:00)
	Attempt to modify a sent message	Select sent message, attempt to delete or edit	Error message: Sent messages cannot be deleted or edited for audit trail purposes

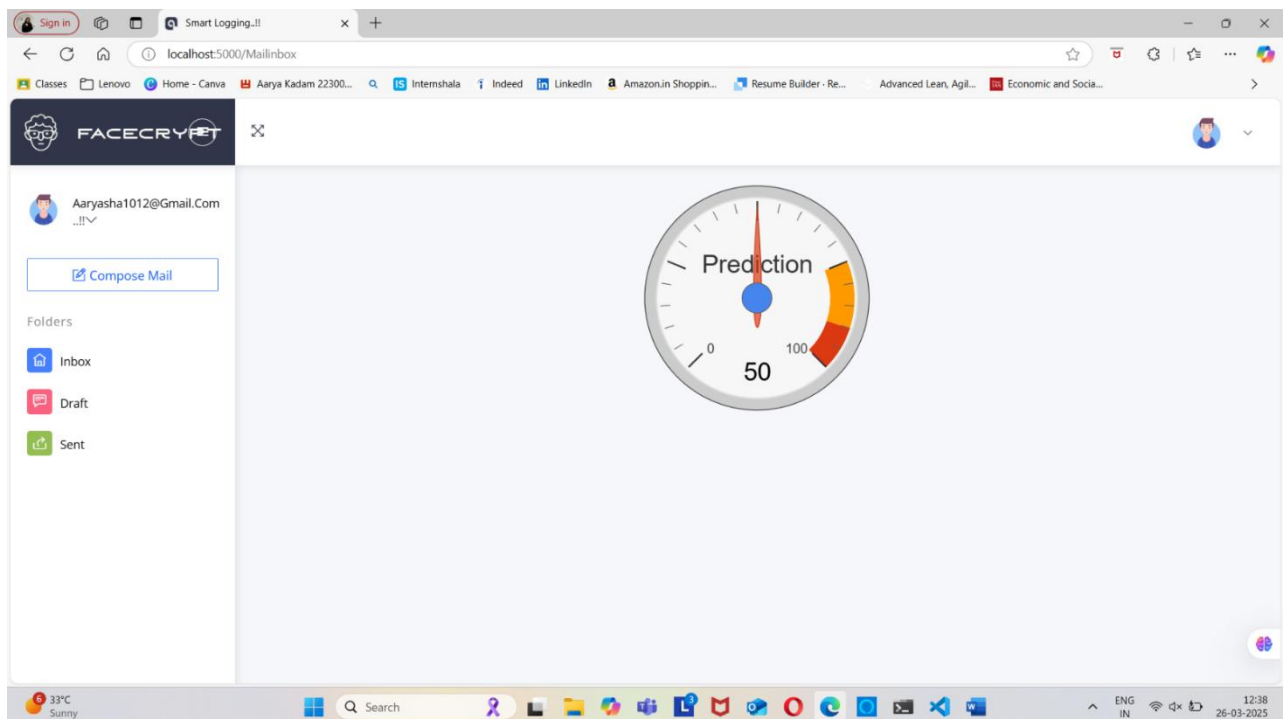
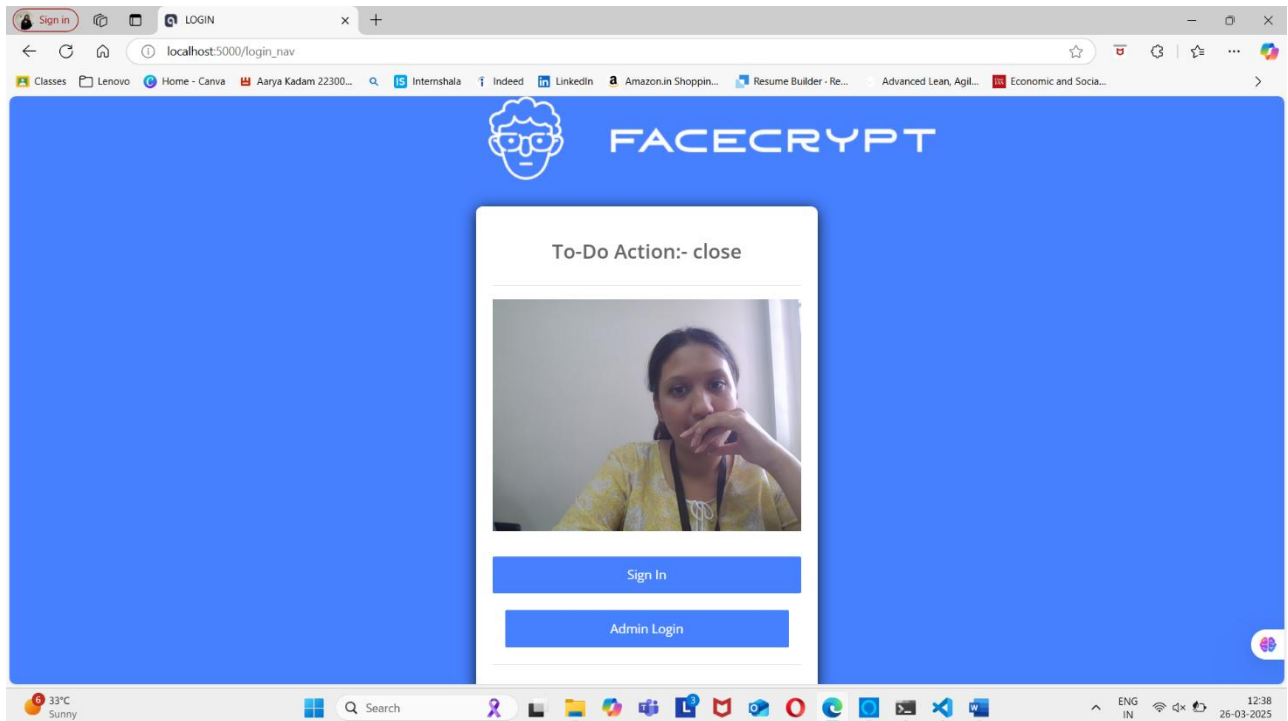
- White Box Testing Test Cases -

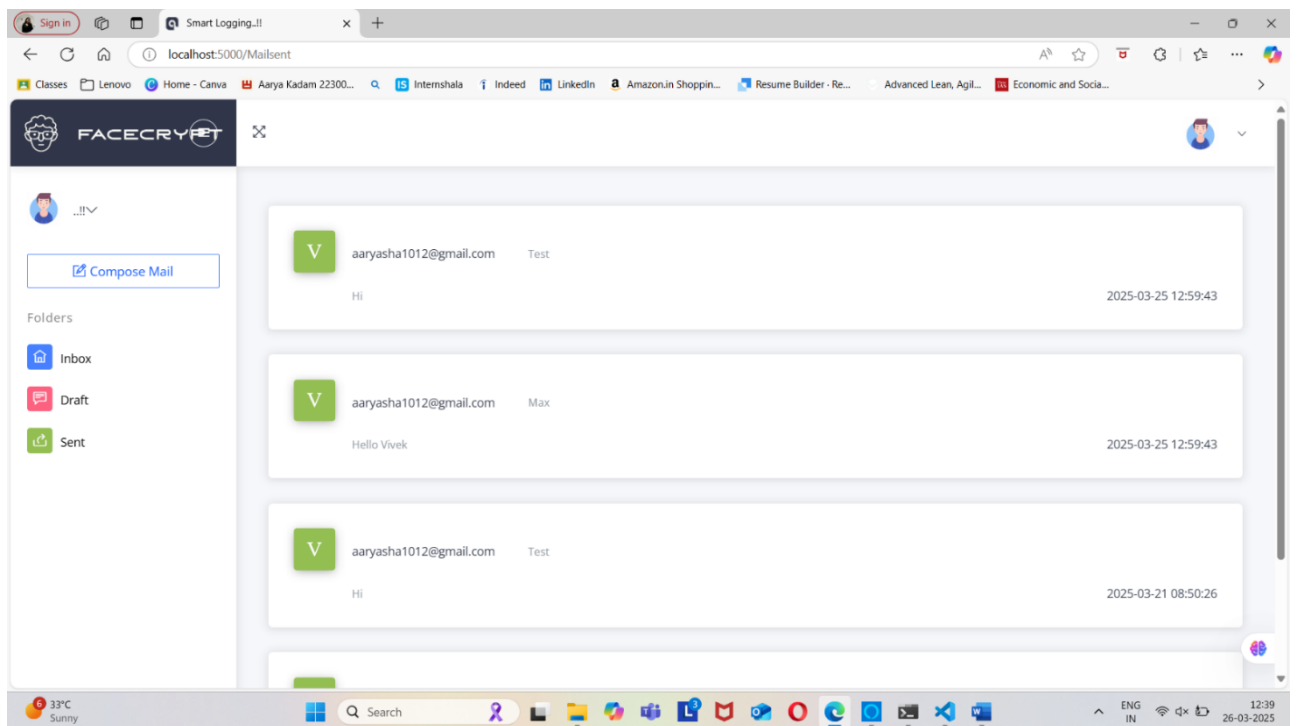
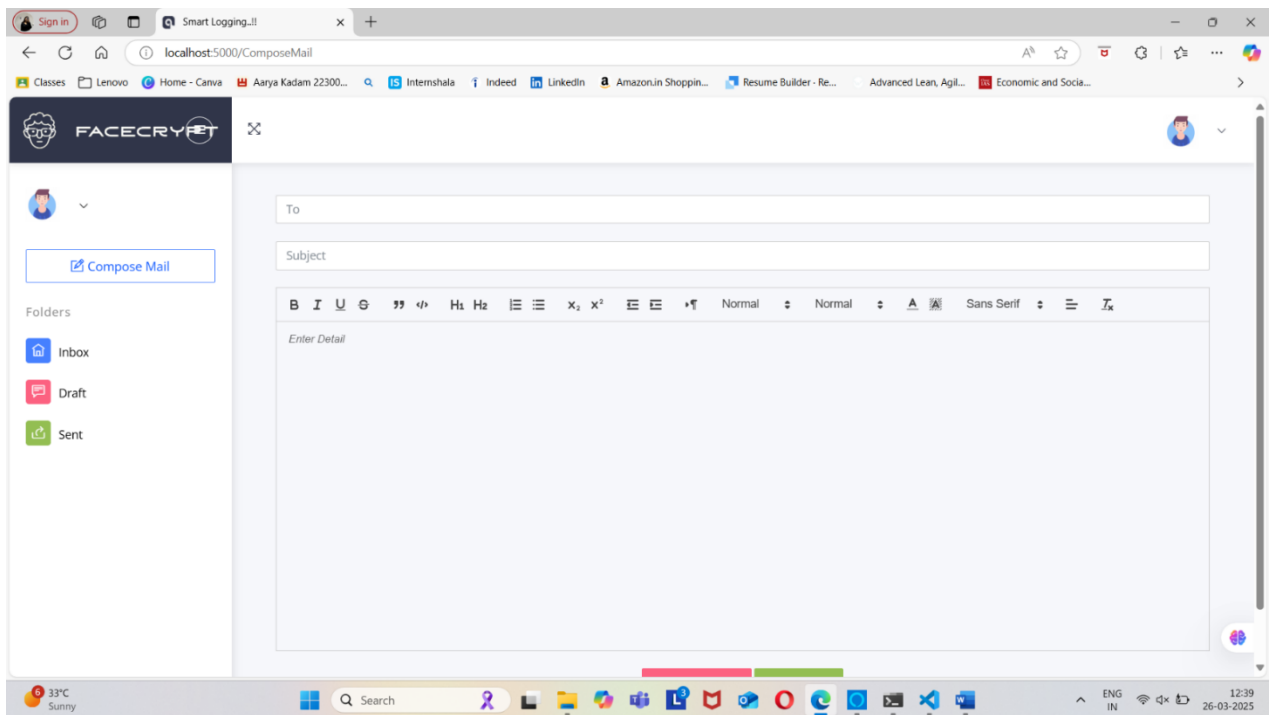
Modules	Test Case	Input	Expected Output	Result
Biometric Data Protection	Validate template protection	Store face biometric template	Template stored securely, non-invertible and cancellable	Pass
	Validate secure sketch generation	Generate secure sketch from user-specific key	Secure sketch generated successfully	Pass
	Validate key regeneration	Regenerate user-specific key from secure sketch	Key regenerated successfully	Pass
Face Registration	Validate face registration	Register a new user with face biometric	Face biometric registered successfully	Pass
	Validate duplicate face registration	Register an existing user with face biometric	Error: "Face biometric already exists"	Fail
	Validate face morphing detection	Register a user with face morphing	Face morphing detected successfully	Pass
Face Authentication	Validate face authentication	Authenticate with valid face biometric	Authentication successful	Pass
	Validate face authentication failure	Authenticate with invalid face biometric	Authentication failed	Fail
	Validate face morphing detection during authentication	Authenticate with face morphing	Face morphing detected successfully	Fail
User Management	Validate user account creation	Create a new user account	User account created successfully	Pass
	Validate user account deletion	Delete a user account	User account deleted successfully	Fail

	Validate user role-based access	Login as a regular user	Admin panel should be restricted	Pass
System Security	Validate SQL injection protection	Input: ' OR '1'='1 in various fields	System should block and log the attempt	Fail
	Validate cross-site scripting (XSS) protection	Input: <script>alert('XSS')</script> in various fields	System should block and log the attempt	Pass
	Validate secure data storage	Store sensitive data (e.g., face biometrics)	Data should be stored securely and encrypted	Pass

USER MANUAL

User Interface Design:





Limitations:

- 1) **Lighting Conditions:** The system's performance may degrade under varying lighting conditions, such as low light or extreme brightness.
- 2) **Facial Expressions and Occlusions:** The system may struggle to recognize faces with extreme facial expressions or occlusions, such as wearing glasses or masks.
- 3) **Database Size and Complexity:** The system's performance may decrease as the database size and complexity increase.
- 4) **Security Threats:** While the system incorporates various security measures, it is not immune to emerging security threats, such as advanced spoofing attacks.
- 5) **Aging and Environmental Factors:** The system may struggle to recognize faces that have changed due to aging or environmental factors.

Future Enhancement:

- 1) **Integration with Other Biometric Modalities:** Integrating face recognition with other biometric modalities, such as fingerprint, iris, or voice recognition, to provide multi-factor authentication.
- 2) **Real-Time Performance Optimization:** Optimizing the system for real-time performance, to enable fast and seamless authentication.
- 3) **Testing and Validation on Larger Datasets:** Testing and validating the system on larger datasets, to ensure its accuracy and reliability.
- 4) **Enterprise Integration:** Integrate the system with existing enterprise infrastructure, such as HR systems, access control systems, and identity management systems.
- 5) **Integration with IoT Devices:** Integrate the system with IoT devices, such as smart door locks, security cameras, and access control systems, to enable seamless and secure authentication.

Bibliography:

- Computer Vision with OpenCV" course by Jose Portilla on Udemy [Python for Computer Vision with OpenCV and Deep Learning | Udemy](#)
- FreeCodeCamp (coding blog and tutorials) [Learn to Code — For Free — Coding Courses for Busy People](#)
- Authors: X. Xu, L. Zhang, and F. Li, Title: "MSSVT: Multi-scale feature extraction for single face recognition"

Annexure :

1. Sample Program Code –

```
@app.route('/register', methods=['GET', 'POST'])
def register():
    if 'username' in session:
        msg = "
        if request.method == 'POST':
            name = request.form['name']
            password = request.form['password']
            email = request.form['email']
            mobile = request.form['contactNo']
            type_ = request.form['type']
            if not re.match(r'^@]+@^[^@]+\.[^@]+', email):
                msg = 'Invalid email address !'
                flash(msg)
            elif not re.match(r'[A-Za-z0-9]+', name):
                msg = 'Username must contain only characters and numbers !'
                flash(msg)
            else:
                try:
                    record_faces(name,password,mobile,email,type_)
                    msg = 'You have successfully registered!'
                    flash(msg)
                    return redirect(url_for('MailinboxAdmin'))
```