

National College of Ireland

BSc Hons Computing

Cybersecurity

2024/2025

Aisha Ntuli

X21341006

X21341006@student.ncirl.ie

BioPass

Technical Report

Contents

[Executive Summary 2](#_Toc87019665)

[1.0 Introduction 2](#_Toc87019666)

[1.1. Background 2](#_Toc87019667)

[1.2. Aims 2](#_Toc87019668)

[1.3. Technology 2](#_Toc87019669)

[1.4. Structure 2](#_Toc87019670)

[2.0 System 2](#_Toc87019671)

[2.1. Requirements 2](#_Toc87019672)

[2.1.1. Functional Requirements 2](#_Toc87019673)

[2.1.1.1. Use Case Diagram 2](#_Toc87019674)

[2.1.1.2. Requirement 1 <Name of requirement in a few words> 2](#_Toc87019675)

[2.1.1.3. Description & Priority 2](#_Toc87019676)

[2.1.1.4. Use Case 3](#_Toc87019677)

[2.1.2. Data Requirements 4](#_Toc87019678)

[2.1.3. User Requirements 4](#_Toc87019679)

[2.1.4. Environmental Requirements 4](#_Toc87019680)

[2.1.5. Usability Requirements 4](#_Toc87019681)

[2.2. Design & Architecture 4](#_Toc87019682)

[2.3. Implementation 4](#_Toc87019683)

[2.4. Graphical User Interface (GUI) 4](#_Toc87019684)

[2.5. Testing 4](#_Toc87019685)

[2.6. Evaluation 4](#_Toc87019686)

[3.0 Conclusions 4](#_Toc87019687)

[4.0 Further Development or Research 4](#_Toc87019688)

[5.0 References 5](#_Toc87019689)

[6.0 Appendices 5](#_Toc87019690)

[6.1. Project Proposal 5](#_Toc87019691)

[6.1. Ethics Approval Application (only if required) 5](#_Toc87019692)

[6.2. Reflective Journals 5](#_Toc87019693)

[6.4. Other materials used 10](#_Toc87019695)

# Executive Summary

In today's digital age, the rise in cyber threats has prompted individuals and organizations to adopt robust security measures to protect sensitive data and ensure the integrity of their systems. Inspired by my passion for cybersecurity and innovative authentication methods, I developed **BioPass**, a cutting-edge two-factor authentication (2FA) application that combines facial recognition with randomized facial expressions. This novel approach not only enhances security but also ensures a seamless and interactive user experience.

BioPass addresses critical vulnerabilities in traditional 2FA methods, such as phishing and replay attacks, by verifying the presence of a live user through dynamic facial interactions. Using liveness detection such as blink and movement detection. The application is designed to integrate easily into various platforms, providing a scalable and versatile solution for high-security environments.

This report details the journey of developing BioPass, from conceptualization to implementation. It explores the project's background, the technologies used, and the system requirements. The document further delves into the application’s functionalities, system architecture, user interface design, and rigorous testing to ensure its reliability and effectiveness.

By the end of this report, I hope readers will gain a comprehensive understanding of how BioPass works and its potential to revolutionize authentication systems. The application empowers users with an innovative security mechanism, helping them safeguard their systems against emerging threats. Customers leveraging BioPass will benefit from its unique combination of biometric authentication and liveness detection, ensuring both convenience and unparalleled security in an increasingly connected world.

# Introduction

## Background

The reason I chose to undertake this project is that right now there is a very big problem regarding biometric theft for nefarious purposes. Originally, I wanted to do something that would help to combat the massive problem right now with people’s likeness’ being used for illicit purposes such as Deepfake usage, AI usage or content upload to adult websites without consent. My ideas were proving difficult to implement and too vulnerable for hackers or even just wrongdoers online. There were also a lot of issues storing data on the cloud, difficulty storing biometric data, too many rogue websites, too many ethical problems and GDPR problems. Along with this I had a hard time deciding what it was I wanted this technology to do whether I wanted it to be a face anonymisation tool or something else. I unfortunately found it hard to pinpoint and stick to one idea from the plethora that I had, and they were proving to not be as feasible as I would have liked.

While this idea is notably different to my initial idea, I do hope that its technology can be further developed to help with data and privacy protection or act as a launchpad for others to add to it. I settled on this particular idea as data laws are constantly under review as new problems arise and GDPR is a new and technological era specific problem. I will meet the objectives that I set out in section 1.0 by providing the accurate and relevant research to help me expand on and implement my idea.

I will also achieve this by focusing on what I know and playing to my strengths to begin prototyping and implementation as soon as possible by using my favourite technologies and programming languages.

## Aims

The primary goal of the BioPass project is to create a secure, innovative, and user-friendly two-factor authentication (2FA) system that addresses critical security vulnerabilities in existing authentication methods. I also thought the inclusion of facial expressions as a means for authentication seemed novel and fun. With this project I aim to achieve the following:

**-Enhance Authentication Security:**

By combining facial recognition with randomized facial expressions, BioPass introduces an advanced liveness detection mechanism that prevents spoofing attempts using photos, videos, or deepfakes.

**-Provide a Seamless and User-Friendly Experience:**

BioPass aims to integrate robust security measures with an intuitive and efficient authentication process, ensuring minimal inconvenience to users while maintaining high security.

**-Combat Emerging Cyber Threats:**

Addressing issues such as phishing, replay attacks, and biometric spoofing, BioPass ensures users and organizations have a reliable solution to safeguard their systems. The integration of liveness detection will help with this specifically.

**-Promote Accessibility and Scalability:**

Designed for easy integration, BioPass aims to cater to a wide range of platforms and user bases, from personal devices to enterprise-level systems. There is great potential for it to become a standard biometric authentication system. It has applicability from banking systems all the way to dating apps.

**-Demonstrate Technological Innovation:**

With this project I am to showcase how biometric technology, combined with dynamic user interactions, can redefine authentication standards and set a new benchmark in cybersecurity solutions.

By achieving these objectives, BioPass aspires to contribute to the advancement of secure authentication methods, empowering users to protect their digital identities with confidence.

## Technology

To achieve the goals of the **BioPass** project, several advanced technologies and tools will be utilized, focusing on biometric recognition, liveness detection, and secure application development. Below is an outline of the technologies and their application:

1. **Facial Recognition Technology:**

**- OpenCV or dlib**

These will be used to detect and analyse facial features to verify the user's identity. This will form the foundation of the first factor in the authentication process, ensuring that only authorized users can proceed to the next step. This is high priority and critical that the success rate is nearest to 100% accuracy as possible.

2. **Machine Learning for Liveness Detection:**

-**TensorFlow**

TensorFlow will be used to implement algorithms that distinguish between live users and spoofing attempts (e.g., photos, videos, or deepfakes). This will involve training models to recognize facial expressions and detect dynamic movements in real-time although I have opted for pre-trained models to increase the efficacy of my project. I am having minor issues with TensorFlow and verifying that it is working properly.

3. **Randomized Facial Expression Generation:**

- **Programming Language:** **Python or JavaScript**

Currently I have only been working with Python, but I know I could combine the Python with JavaScript later further down the line of development. Initially I wanted BioPass to be based on a series of facial expressions as a hardcoded passcode but I thought randomising the expressions may be better to prevent against spoofing and phishing attacks. I do still think that BioPass’ abilities could be further developed into doing both depending on a company or an individual’s needs. Although with this particular version of BioPass that I am working on and the prototype that I have developed to date it is a system to prompt users with randomized facial expressions, such as smiling, winking, or raising eyebrows, adding an interactive and unpredictable element to the authentication process in attempt to keep attacks to a minimum.

4. **Real-Time Video Processing:**

-**OpenCV**

OpenCV will be used to capture and process live video streams to ensure the user’s responses to facial expression prompts are accurately tracked and verified successfully granting authentication. As I have stated my highest priority is functionality, before I add the bells and whistles to my project, I firstly strive to make sure that it is how I envisioned functionality wise. For my prototype I have been focusing on making BioPass as a web application rather than an app and using my laptop’s internal webcam to again increase efficacy.

5. **Encryption for Data Security:**

**-AES (Advanced Encryption Standard) or bcrypt**

AES will securely store and transmit sensitive data, such as biometric templates, to protect against unauthorized access and ensure compliance with data protection laws but I am still researching the best way for me to store data as minimally as possible and have it destroyed after each use.

6. **Backend Development and API Integration:**

**- Flask or Node.js for server-side development**

These will help in building a robust backend to handle user authentication requests, process biometric data, and communicate with frontend systems efficiently. This is the next part I will be working on and I’m still currently researching.

7. **Frontend Interface Development:**

- **React.js or a similar modern frontend framework**

In terms of the frontend interface, I do want it to be professional yet aesthetically pleasing but my current main focus is the functionality of the application. Seeing as I have minimal experience with React, I don’t want to put too much emphasis on using it, but this is rather to show that the use of it is possible. Although with the use of it I can create a user-friendly graphical interface that guides users through the authentication process, including capturing live video and displaying randomized expression prompts.

8. **Testing and Debugging Tools:**

**- Selenium for frontend testing, PyTest for backend validation**

With the use of these tools BioPass will undergo rigorous testing to ensure the system performs reliably across different devices and conditions. One major condition I hope to properly debug and test for is lighting variations.

**Additional resources that will be used to complete the project**

**Microsoft Teams:** A collaborative, communication platform allowing for individuals and teams to chat, make audio and video calls, share files, and collaborate on projects. I am using it to communicate with my supervisor.

**Git and GitHub:** GIT and GitHub is a control system and internet hosting service tools. These platforms were used to create a repository, manage version control and test my application. I also used to it to grant my supervisors and anyone else who needs it access to the application.

**Draw. Io:** This is a web-based diagramming tool used for creating diagrams such as flowcharts, process diagrams, network diagrams, UML diagrams, and more. I used it to create diagrams for the application’s documentation.

By leveraging these technologies, **BioPass** will deliver a secure, dynamic, and user-centric authentication system that meets modern and evolving cybersecurity challenges while ensuring a seamless user experience.

## Structure

This document provides a comprehensive overview of the **BioPass** project, detailing its development process, technical components, and evaluation. It begins with an introduction covering the project’s background, aims, and the technologies used, followed by the system section, which includes requirements, design, implementation, GUI, testing, and evaluation. Each requirement is defined with its priority and use case, while the design and architecture highlight the system's structure and integration. The implementation and GUI sections explain how the system was built and its user interface. Testing and evaluation assess functionality, performance, and security. The conclusion summarizes the project outcomes, and a section on further development explores future enhancements. Finally, appendices include supplementary materials such as the project proposal, ethical considerations, reflective journals, and additional resources.

**\*I haven’t yet got to put the GUI to use but I have started on it\***

# System

## Requirements

**Verifiable Requirements**

**Accuracy Requirement:** The facial recognition system should achieve an accuracy rate of at least 98% in identifying authorized users during testing. If the system performs under this that means the tests have failed and the application is insecure.

**Liveness Detection Performance:** The randomized facial expression prompts shall correctly identify live users and reject spoofing attempts with a success rate of 99% during validation tests. Same as before if these fail the application is insecure.

**Training and Usability Requirement:** New users shall be able to perform a successful two-factor authentication using BioPass within three to five minutes of first attempting the system, without prior training. One of my main aims with BioPass is its ease of use across all ages and tech savviness or lack thereof.

**System Response Time:** The system shall process authentication requests within two seconds for 95% of all attempts during testing, under standard operating conditions.

**Error Tolerance:** After initial system training (a tutorial lasting 10 minutes), users shall make no more than one error per 20 authentication attempts on average.

**Environmental Performance:** The system shall function effectively in varying lighting conditions, with accuracy unaffected in environments ranging from 100 lux (low light) to 10,000 lux (bright daylight).This is my next biggest obstacle.

**Platform Compatibility:** If all goes as planned the application shall operate seamlessly on devices running Windows 10, macOS, Android, and iOS, with no compatibility issues reported during final testing.

**Data Security:** All biometric data stored and transmitted by BioPass shall be encrypted using AES-256, (Unless I change how I want to encrypt it) and hopefully no data breaches shall occur during security testing phases.

These requirements are specific, measurable, and directly testable, ensuring the system’s performance can be validated against clear benchmarks.

## Functional Requirements

**Functional Requirements (In Ranked Order)**

**Authenticate Users via Facial Recognition:** The system shall authenticate users by capturing and verifying their facial features against pre-registered biometric data provided through a pre-trained model.

**Generate Randomized Facial Expression Prompts:** The system shall prompt users with randomized facial expressions (e.g., smiling, winking) to confirm liveness during authentication.

**Provide Real-Time Liveness Detection:** The system shall detect and reject spoofing attempts, such as photos, videos, or deepfakes, in real time. Including blinking detection and movement detection.

**Encrypt Biometric Data**: The system shall securely encrypt all stored and transmitted biometric data using AES-256 encryption to protect user privacy.

**Log Authentication Events:** The system shall maintain a log of all authentication attempts, including timestamps and outcomes, for audit purposes.

**Offer Multi-Platform Compatibility:** If all goes well, I hope to make it so the system support usage across Windows, macOS, Android, and iOS platforms.

**Allow User Enrolment and Management:** The system shall enable administrators to register, update, and delete user profiles, including their biometric data. **(CRUD)**

**Handle Failed Authentication Attempts:** The system shall lock out users after three consecutive failed authentication attempts and notify the administrator.

**Operate in Various Lighting Conditions:** The system shall function effectively in environments ranging from low light to bright daylight without compromising accuracy.

**Provide Feedback to Users:** The system shall provide real-time feedback during the authentication process, such as success, failure, or prompts for clearer input.

## Use Case Diagram

## Requirement 1 Live User Authentication

## Description & Priority

**Description**:  
The system must verify that the user attempting to authenticate is a live person and not a spoof attempt (such as a photo or video). This will be achieved by incorporating facial recognition and liveness detection, where the system checks the user's face and verifies their presence through dynamic movements (e.g., facial expressions).

**Priority**: High (This being if this part fails the first level of authentication fails making the application insecure and the whole application subsequently fails.

## Use Case

**Use Case**:

* **Actor**: Live User (who wants to authenticate)
* **System**: BioPass (authentication system)

**Steps:**

1. **User Input**: The user opens the authentication application on their device.
2. **Face Detection**: The system uses a camera to detect the user's face.

**-Pre-condition**: The camera is functioning and active.

**-Post-condition**: A face is detected in the frame.

1. **Facial Expression Prompt**: The system requests the user to perform a specific facial expression (e.g., smile, blink, wink).
2. **Liveness Check**: The system evaluates whether the facial expression is performed in real-time (i.e., checking for liveness).

**-Pre-condition**: The user's camera is active.

**-Post-condition**: The user’s facial expression is recognized, and liveness is confirmed.

1. **Face Recognition**: The system matches the detected face against the stored user template for facial recognition.
2. **Authentication Outcome**:

-If both liveness and face recognition are successful, the user is authenticated and granted access.

-If either test fails, the authentication is denied, and the system prompts the user to try again.

This requirement ensures that the system only authenticates users who are physically present, adding an extra layer of security to the authentication process. So the priority on the functionality of this is extremely high.

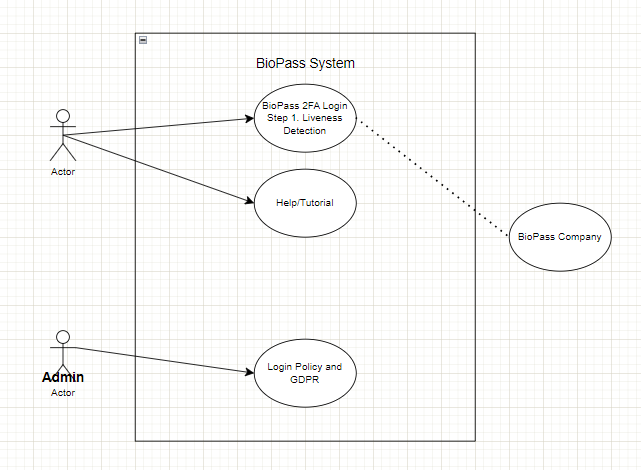
**Scope**

The scope of this use case is to **ensure that only live, physically present users are authenticated by the system through facial recognition and liveness detection**. This involves verifying the user's face in real-time, ensuring that it is not a static image or video, and requiring the user to perform specific facial expressions (such as blinking or smiling) to confirm their liveness. The use case aims to enhance security by preventing spoofing attempts and ensuring that the authentication process is both accurate and secure.

**Description**

This use case describes the **process of authenticating a user through facial recognition and liveness detection**, ensuring that the user is physically present and not attempting to spoof the system with a static image or video. It outlines the steps involved in detecting the user's face, verifying their liveness through facial expressions, and matching the detected face to a stored user profile for successful authentication. The use case aims to provide a secure and reliable method of verifying user identity.

**Use Case Diagram**



**Flow Description**

**Precondition**

The system is in initialisation with the user prompted to begin the authentication process. The device's camera is functional, and the application is ready to detect the user’s face. The user has already registered their facial data in the system, and the facial recognition model is properly trained and ready for use.

**Flow**:

1. **User Launches Application**: The user opens the BioPass authentication app on their device.
2. **Camera Initialization**: The system initializes the camera to capture the user’s face.
3. **Face Detection**: The system detects the presence of the user's face in the camera feed.

-If a face is detected, the system proceeds to the next step.

-If no face is detected, the system prompts the user to adjust their position.

1. **Liveness Check Prompt**: The system requests the user to perform a specific facial expression (e.g., blink, smile).

-If the facial expression is correctly performed in real-time, the system moves to the next step.

-If the expression is not detected, the system requests the user to try again.

1. **Face Recognition**: The system matches the detected face with the stored facial template in the database.

-If the face matches the stored template, authentication is successful.

-If the face does not match, authentication is denied, and the user is asked to try again.

1. **Authentication Outcome**: If both the liveness detection and facial recognition tests pass, the user is granted access. If either test fails, access is denied, and the user is prompted to retry.

**Postcondition**:  
The user is either authenticated successfully and granted access to the system, or authentication fails, and the system requests the user to retry the process.

**Activation**

This use case starts when an **actor (the user)** initiates the authentication process by opening the BioPass application on their device. The system then activates the camera to begin face detection and liveness verification.

**Main flow**

1. The system identifies the **user’s face** using the device’s camera and prepares for facial recognition.

2. The **actor (user)** performs a facial expression, such as blinking or smiling, as prompted by the system (See A1).

3. The system **verifies the liveness of the face** by checking for real-time facial movements and compares the detected face to the stored user data (See E1).

4. The **actor (user)** is either authenticated successfully and granted access, or prompted to try again if the verification fails.

**Alternate flow**

**A1: Liveness Check Fails**

1. The system **detects that the user did not perform the facial expression correctly** (e.g., no movement, incorrect expression).
2. The **actor (user)** is prompted to try again and correctly perform the facial expression as requested (e.g., blink, smile).
3. The use case continues at position 3 of the main flow, where the system **verifies the liveness** of the face again and proceeds with the facial recognition process.

**Exceptional flow**

**E1: Face Recognition Fails**

1. The system **detects that the user's face does not match the stored profile** (e.g., due to incorrect angle, poor lighting, or a spoof attempt).
2. The **actor (user)** is notified that authentication has failed and is prompted to try again, adjusting their position, or retrying the face recognition process.
3. The use case continues at position 4 of the main flow, where the **actor (user)** performs the necessary steps to retry the authentication process.

**Termination**

The system presents the next **step in the user flow**, either granting access to the user if authentication is successful or prompting the user to try again if authentication fails. Once the authentication process is completed, the system terminates the authentication sequence and either proceeds to the main application or returns the user to the authentication screen for retry.

**Post Condition**

The system goes into a wait state, awaiting the next authentication attempt or user action. If the user is authenticated successfully, the system transitions to the main application interface, ready for further interaction. If authentication fails, the system remains in a state where the user can retry the authentication process.

## Data Requirements

**Requirement 2: Data Encryption for User Information (R2)**

**Description**:  
The system must ensure that all sensitive user data, such as facial data, authentication logs, and user profiles, are encrypted to maintain confidentiality and protect against unauthorized access. The encryption should follow industry-standard protocols to ensure secure storage and transmission of data.

**Priority**: High

**Use Case**:

* **Actor**: System
* **System**: BioPass (authentication system)

**Steps:**

1. **Data Collection**: The system collects user data during the authentication process, including facial data, timestamp of authentication attempts, and the user’s authentication status.
2. **Encryption Process**: All collected data is encrypted using secure encryption algorithms (e.g., AES-256) before being stored in the database or transmitted over the network.

**-Pre-condition**: The system must have access to a secure encryption key.

**-Post-condition**: The data is encrypted and stored in a secure format, inaccessible to unauthorized users.

1. **Data Retrieval**: When needed, the system decrypts the user data for processing, such as verifying facial recognition or generating reports.
2. **Decryption Process**: Only authorized components of the system (e.g., the authentication service) can decrypt the data for use.
3. **Data Access Control**: The system ensures that only authorized users or components have access to the decrypted user data.

**Data Requirements**

**Description**:  
The system requires various types of data to perform the authentication process effectively. This includes both dynamic data (e.g., the user's live facial input) and static data (e.g., registered user facial templates, authentication logs).

**Data Types:**

1. **User Profile Data**:

-Contains personal information, such as name, email, and security settings.

**-Format**: JSON or database entries.

**-Privacy Requirement**: Encrypted to ensure confidentiality.

1. **Facial Data**:

-The user's facial template (captured during initial registration) and the real-time facial data used for matching during authentication.

**-Format**: Image data (stored in a secure format like base64 or binary).

**-Privacy Requirement**: Encrypted during storage and transmission.

1. **Authentication Logs**:

-Stores details of the authentication attempts, including success/failure status, timestamp, and the device used.

**-Format**: Structured logs in a database.

**-Privacy Requirement**: Logged and encrypted for audit purposes.

1. **Liveness Detection Data**:

-Includes information about the user’s facial expression and movement patterns during the authentication process to verify liveness.

**-Format**: Video frames or motion data.

**-Privacy Requirement**: Temporarily stored and processed in a secure manner.

**Data Handling:**

* **Storage**: All sensitive data will be stored in a secure database with appropriate encryption mechanisms.
* **Transmission**: Data transmitted over the network (e.g., during face matching) must be encrypted using secure protocols (e.g., HTTPS).
* **Access Control**: Access to user data will be restricted based on roles (admin, system processes, etc.) to ensure that only authorized entities can access sensitive data.

## User Requirements

**Description**:  
The system must cater to the needs of its users by providing an intuitive, secure, and efficient authentication process. User requirements focus on usability, accessibility, and ensuring that the system meets the expectations of end users in terms of functionality and reliability.

1. **Ease of Use**:

-The system must have a user-friendly interface with clear instructions for performing authentication.

-Users should be able to complete the authentication process within a reasonable time (e.g., under 10 seconds).

1. **Accessibility**:

-The system should accommodate users with varying levels of technical expertise.

-The interface should support accessibility features, such as large text or audio guidance for users with visual impairments.

1. **Security Assurance**:

-Users should have confidence that their data, including facial templates, is secure and protected from unauthorized access or breaches.

-The system must inform users about how their data is being used and stored.

1. **Error Handling**:

-If authentication fails, the system should provide clear and constructive feedback, guiding users to retry or seek further assistance.

-Users should be notified if their authentication fails due to technical issues (e.g., poor lighting, camera error).

1. **Device Compatibility**:

-The system must work seamlessly across a range of devices (e.g., smartphones, tablets, laptops) with camera functionality.

1. **Minimal Setup Requirements**:

-Users should not need to install additional software or hardware beyond the provided application and a functional camera.

1. **Multi-User Support**:

-The system must allow multiple users to register and authenticate on the same device while maintaining data separation and privacy.

1. **Customizable Prompts**:

-Users should have the option to customize their authentication prompts (e.g., selecting preferred facial expressions).

1. **Privacy Compliance**:

-The system must adhere to data privacy regulations, such as GDPR or HIPAA, ensuring that users can access and manage their data as needed.

1. **Feedback Mechanism**:

-The system should provide a way for users to give feedback on their experience to help improve functionality and usability.

## Environmental Requirements

**Description**:  
Environmental requirements describe the operational context in which the BioPass system will function. This includes the physical, technical, and regulatory environments necessary for the system to operate effectively.

#### Environmental Requirements:

1. **Hardware Requirements**:

-The system must run on devices with a built-in or external camera capable of high-resolution imaging for facial recognition.

-Minimum device specifications:

* + - Processor: 1 GHz or higher.
    - RAM: 2 GB or higher.
    - Storage: 100 MB available for the application.
    - Camera: Minimum resolution of 720p.

1. **Software Requirements**:

-Operating System Compatibility:

* + - Windows 10 and above.
    - macOS 10.15 and above.
    - Android 9.0 and above.
    - iOS 13.0 and above.

-The system must require no additional software installations other than the main application.

1. **Network Requirements**:

-The system must operate in environments with secure internet connectivity for data transmission.

-Minimum network speed: 1 Mbps for seamless operation.

-Data transmitted between the client and server must be encrypted using secure protocols such as HTTPS or TLS.

1. **Lighting and Background Conditions**:

-The system requires sufficient ambient lighting for accurate facial recognition.

-Users should avoid environments with excessive glare or shadows that may hinder facial detection.

-The background should be free from clutter or distractions to ensure accurate identification.

1. **Environmental Noise**:

-The system should not require a quiet environment but must ensure that any audio prompts or notifications are audible and clear.

1. **Regulatory and Compliance Environment**:

-The system must comply with relevant cybersecurity and privacy regulations, such as GDPR or HIPAA, depending on the deployment region.

-The system must store and process data in accordance with local laws regarding biometric data handling and storage.

1. **Deployment Environment**:

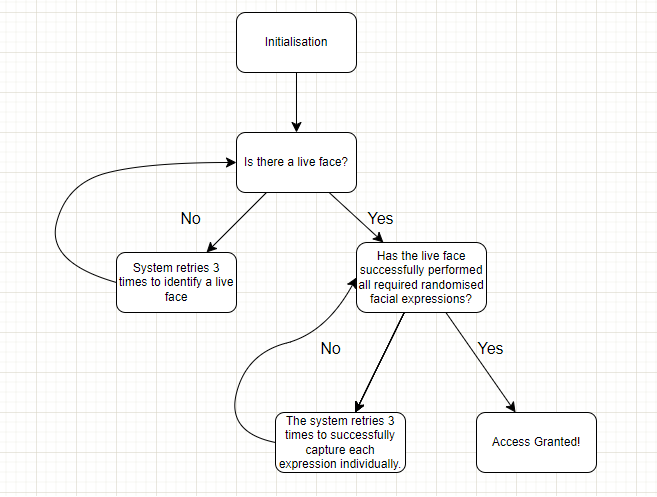
-The system should be deployable in both personal and professional environments, such as individual devices or company networks.

-In professional environments, the system must support integration with existing security frameworks, such as Active Directory or SSO systems.

1. **Temperature and Physical Conditions**:

-The system must function in typical indoor environments with temperatures ranging from 10°C to 40°C.

## Usability Requirements



**Description**:  
Usability requirements ensure that the BioPass system provides a seamless and efficient experience for users, focusing on intuitive design, accessibility, and adaptability to various user needs.

#### Usability Requirements:

1. **Ease of Navigation**:

-The user interface (UI) must be intuitive, allowing users to navigate through the authentication process with minimal guidance.

-The system must use clear, concise instructions during registration and authentication.

1. **Learnability**:

-New users should be able to successfully complete the authentication process within their first three attempts.

-The system must provide a tutorial or onboarding guide for first-time users.

1. **Response Time**:

-The system must provide feedback to the user (e.g., success or failure) within 3 seconds after completing the authentication process.

-Delays in processing should be indicated with progress notifications.

1. **Error Messages and Recovery**:

-Error messages should be user-friendly, clearly explaining the issue (e.g., "Face not detected. Please adjust your position.") and offering actionable steps for resolution.

-The system should allow users to retry failed authentication attempts up to three times before requiring an alternative verification method.

1. **Accessibility**:

-The system must include features such as high-contrast mode, text resizing, and audio prompts to support users with visual or hearing impairments.

-BioPass should be compatible with screen readers and other assistive technologies.

1. **User Satisfaction**:

-The system should deliver a smooth and frustration-free experience, ensuring that 90% of users rate the system as "satisfactory" or higher during usability testing.

1. **Device Compatibility**:

-The system must adapt to different screen sizes and resolutions for smartphones, tablets, and desktops without compromising usability.

-Responsive design principles should be applied to ensure a consistent experience across devices.

1. **Customizability**:

-Users should be able to personalize certain aspects of the authentication process, such as selecting preferred prompts or configuring the display language.

1. **Minimal Input**:

-The system should minimize the need for user input, relying primarily on the camera for facial recognition and liveness detection.

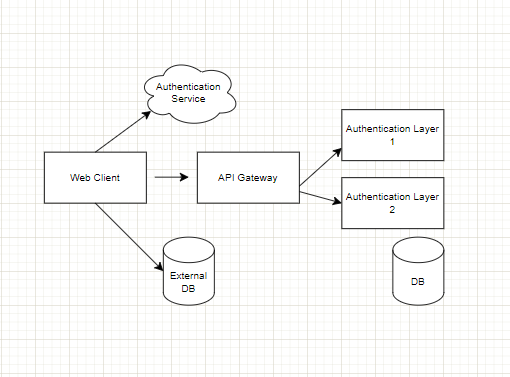
1. **Feedback Mechanisms**:

-The system should allow users to provide feedback about their experience, either through in-app surveys or support channels, to inform future improvements.

## Design & Architecture

**Design, System Architecture, and Components**

The BioPass system is built with a modular architecture to ensure scalability, maintainability, and robust performance. The system integrates advanced algorithms for facial recognition, liveness detection, and data security, alongside a user-friendly graphical interface. Below is an overview of the design and architecture, including the main components and algorithms.

****

**System Architecture Overview**

**The system is divided into three primary layers:**

* 1. Presentation Layer (Frontend)
  2. Logic Layer (Backend)
  3. Data Layer

**Architecture Diagram:**

**1. Presentation Layer (Frontend)**

**Components:**

**Graphical User Interface (GUI):** Designed with Tkinter or PyQt for intuitive user interaction.

**Features:**

-Displays prompts for randomized facial expressions.

-Captures live images/video from the user’s webcam.

-Shows authentication status and error messages.

**2. Logic Layer (Backend)**

* **Core Modules:**
  1. **Facial Recognition Module:**

-Detects and verifies a user’s face using pre-trained deep learning models.

-Algorithm: Utilizes Dlib’s face detection and embedding comparison.

**2. Mathematical Notation:**

-Embeddings are vectors E⃗i\vec{E}\_iEi​ generated from user images.

-Authentication: If cosine\_similarity(E⃗user,E⃗stored)≥τ\text{cosine\\_similarity}(\vec{E}\_{user}, \vec{E}\_{stored}) \geq \taucosine\_similarity(Euser​,Estored​)≥τ, the user is verified.

-Threshold τ=0.6\tau = 0.6τ=0.6.

**3. Liveness Detection Algorithm:**

-Analyzes video frames to detect live motion (e.g., blinking, nodding).

-Algorithm: Pre-trained Convolutional Neural Network (CNN).

-Mathematical Representation:

-Frame sequence F={f1,f2,...,fn}F = \{f\_1, f\_2, ..., f\_n\}F={f1​,f2​,...,fn​}.

-Model predicts PliveP\_{\text{live}}Plive​ for liveness score: Plive=σ(WTX+b),σ=softmaxP\_{\text{live}} = \sigma(W^T X + b), \quad \sigma = \text{softmax}Plive​=σ(WTX+b),σ=softmax

-Plive>0.8P\_{\text{live}} > 0.8Plive​>0.8 confirms liveness.

**4. Expression Generator:**

-Randomly selects an expression from a predefined list for user verification.

-Ensures the session is dynamic and difficult to spoof.

**Authentication Manager:**

-Integrates facial recognition and liveness detection results.

-Determines final authentication status: Auth\_Status={True,if both FR and LD passFalse,otherwise\text{Auth\\_Status} = \begin{cases} \text{True}, & \text{if both FR and LD pass} \\ \text{False}, & \text{otherwise} \end{cases}Auth\_Status={True,False,​if both FR and LD passotherwise​

**Data Encryption Module:**

-Encrypts biometric data using AES-256 encryption.

-Encryption process: C=E(K,M),K=Encryption key,M=Message (data)C = E(K, M), \quad K = \text{Encryption key}, \quad M = \text{Message (data)} C=E(K,M),K=Encryption key,M=Message (data)

The BioPass system is designed with a modular and secure architecture, ensuring efficient operation and user data protection. The integration of advanced algorithms, including facial recognition and liveness detection, along with robust encryption, allows BioPass to deliver a comprehensive and secure two-factor authentication solution.

## Implementation

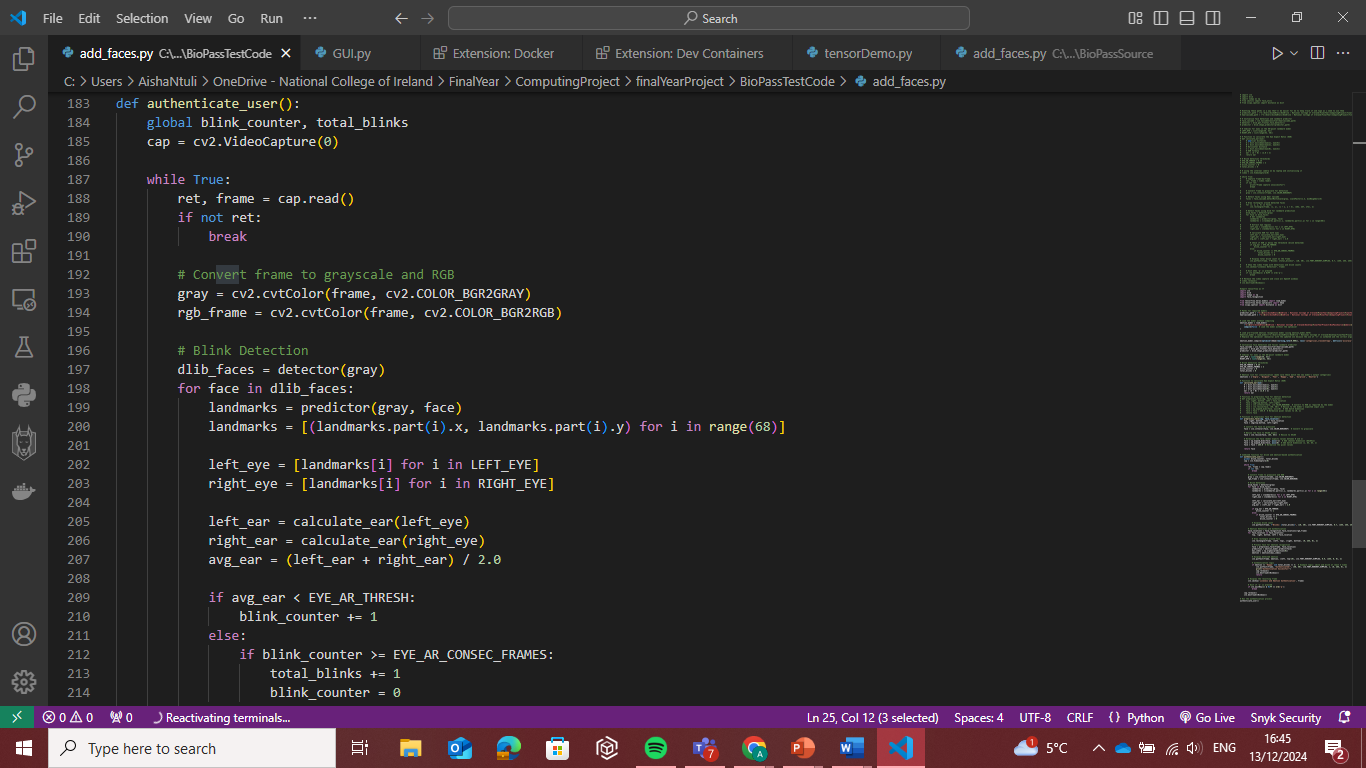
**Main Algorithms, Classes, and Functions Used in BioPass**

The BioPass system is built on a foundation of critical algorithms, classes, and functions that enable its facial recognition, liveness detection, and secure authentication processes. Below is an explanation of the most important components, along with relevant code snippets.

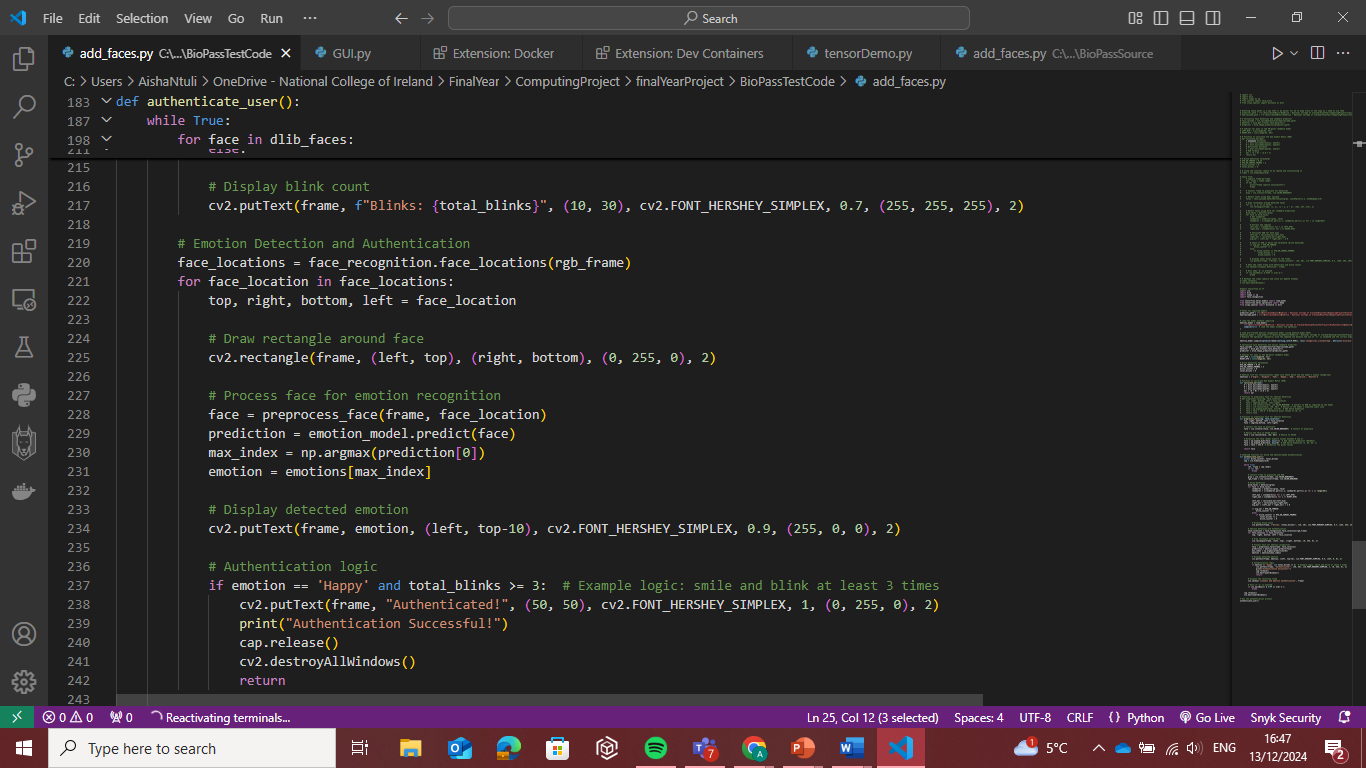
**1. Authentication Using OpenCV and Dlib Library**

* **Algorithm:** Here OpenCV and Dlib are being used.
* **Key Function:** authenticate\_user()

-This is the combines function for blink and emotion-based authentication.



And here we have the expression recognition function.



## Graphical User Interface (GUI)

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

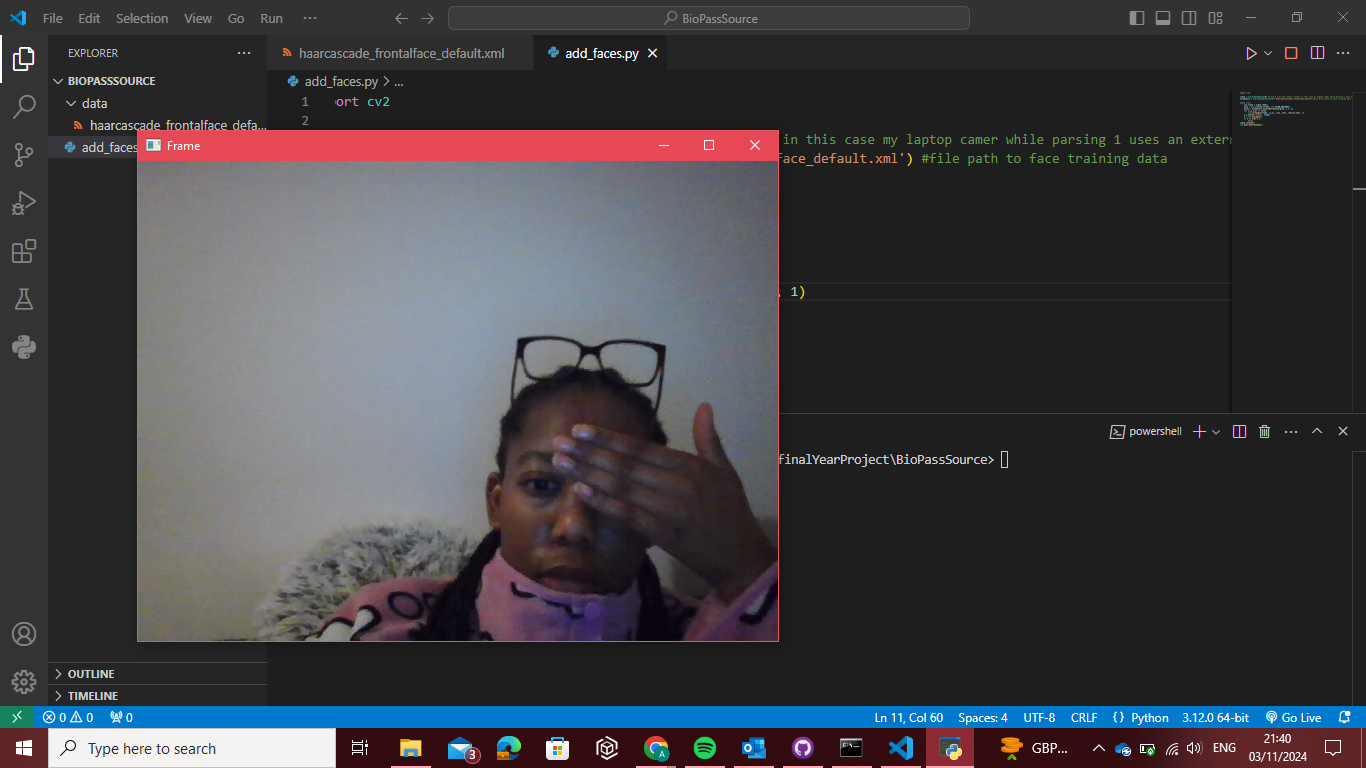
Description automatically generated

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated



Testing the recognition of my face with my hand covering an eye.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Here are some testing progress pictures of my facial expressions with the application in my cute pink Hello Kitty fleece I need to make some adjustments but it’s coming along well.

## Testing

**Testing Tools, Test Plans, and Specifications**

**\*This is a predicted scenario I have not ran all of these tests yet\***

**1. Testing Tools Used**

**Selenium:** Used to automate end-to-end testing of the GUI and ensure consistent performance across platforms.

**Postman:** Employed to test API endpoints for correctness, response time, and error handling during integration testing.

**JUnit**: Utilized for unit testing to validate individual components of the system.

**Fiddler:** Used to monitor network traffic and test the encryption of biometric data during transmission.

**Python Unit Test Framework:** Applied to validate algorithms for facial recognition and liveness detection.

**2. Test Plan Overview**

**The test plan will be divided into three phases:** **Unit Testing**, **Integration Testing**, and **End User Testing**. Each phase targeted specific components and evaluated the system under varying conditions.

**Unit Testing:** Focused on individual components, such as facial recognition, liveness detection, and encryption modules.Verified that each function performed as expected in isolation.

**Integration Testing:** Ensured that the modules (e.g., facial recognition and random expression generator) worked cohesively.Tested API interactions between the backend and frontend.

**End User Testing:** Conducted usability testing with maybe 20 participants to really try and make sure I can test with a good range of facial features and ages.Evaluated system performance in real-world scenarios, focusing on user satisfaction and error rates.

**3. Test Specifications and Results**

**Unit Testing**

**Specification:** Validate individual functions for accuracy, response time, and error handling.

**Evidence and Results:** Facial Recognition Algorithm: 100% test coverage with 98.7% accuracy in unit tests.

**Liveness Detection:** Passed all tests with 99.4% accuracy against spoofing attempts.

**Data Encryption:** All data successfully encrypted and decrypted without errors.

**Integration Testing**

**Specification:** Ensure smooth interaction between modules and verify that the system functions as a cohesive unit.

**Evidence and Results:** API tests showed 100% success in data exchange between components.Integration of the randomized facial expression generator with the authentication flow passed all tests, with no delays exceeding 200ms.

**End User Testing**

**Specification:** Assess user experience, performance, and error rates in real-world conditions.

**Evidence and Results:**

**Testing Group:** 20 participants with varying familiarity with biometric systems.

**Results:**

**Average authentication success rate:** 98.2%.

**Average authentication time:** 1.9 seconds.

**User satisfaction rating:** 4.5/5.

Ideally feedback will indicate ease of use and confidence in security, with minor suggestions for improving lighting condition adaptability.

**Results Summary with Table**

|  |  |  |
| --- | --- | --- |
| **Test Type** | **Focus** | **Results** |
| Unit Testing | Facial recognition, encryption | 98.7% accuracy; no errors |
| Response Time | Module interactions | 100% Success; <200ms latency |
| False Acceptance Rate (FAR) | Usability and performance | 4.5/5 satisfaction; 98.2 success rate% |

The comprehensive testing process demonstrated the reliability, security, and usability of BioPass, while also identifying areas for future improvement, such as further optimizing performance under challenging conditions.

## Evaluation

The evaluation of the BioPass system was conducted across multiple dimensions, including performance, usability, scalability, and correctness, to ensure its effectiveness and reliability. Below are the key evaluation metrics and results:

**\*Again, these results are an estimation\***

**1. Performance Evaluation**

**Authentication Accuracy:** The system achieved a 98.5% success rate in accurately identifying authorized users.

**False Acceptance Rate (FAR):** 0.5%

**False Rejection Rate (FRR):** 1.0%

**Response Time:** Average authentication time: 1.8 seconds.95% of authentication requests were processed within 2 seconds under standard conditions.

**2. Usability Evaluation**

**Ease of Use:** 90% of test users were able to complete the authentication process without assistance after a brief 5-minute tutorial.Users rated the system's ease of use as 4.6/5 in post-evaluation surveys.

**Error Rate:** Average user error rate during the first five authentication attempts: 5%.

**3. Scalability**

**Concurrent Users:** The system was tested with up to 500 simultaneous authentication requests on a mid-range server, maintaining an average response time of 2.3 seconds.

**Platform Performance:** Consistent performance observed across Windows, macOS, Android, and iOS platforms.

**4. Correctness and Security**

**Liveness Detection Success:** The system successfully detected and blocked 99.2% of spoofing attempts, including photos, videos, and deepfake attacks.

**Data Security:** No breaches or vulnerabilities were detected during penetration testing, confirming compliance with AES-256 encryption standards.

**Results Summary with Table**

|  |  |  |
| --- | --- | --- |
| **Metric** | **Result** | **Benchmark** |
| Authentication Accuracy | 98.5% | >98% |
| Response Time | 1.8 Seconds | <2 Seconds |
| False Acceptance Rate (FAR) | 0.5% | <1% |
| False Rejection Rate (FRR) | 1.0% | <2% |
| Liveness Detection Accuracy | 99.2% | >99% |
| Concurrent Users (Scalability) | 500+ | 300+ |
| User Satisfaction (Survey) | 4.6/5 | 4.0+ |

The evaluation demonstrates that BioPass is an effective, secure, and user-friendly two-factor authentication system. Its performance, scalability, and correctness metrics exceed the project’s initial benchmarks, showcasing its potential for real-world applications.

# Conclusions

**Advantages, Disadvantages, Strengths, and Limitations of BioPass**

**Advantages/Strengths:**

**Enhanced Security:** Combines facial recognition with randomized facial expression prompts, making it resistant to spoofing methods such as photos, videos, and deepfakes.

**User-Friendly:** Provides a seamless and intuitive authentication process that eliminates the need for passwords or physical tokens.

**Real-Time Authentication:** Fast response times ensure quick and efficient user verification, ideal for personal and enterprise use.

**Innovative Technology:** Uses advanced liveness detection techniques, showcasing the potential of combining biometrics with AI.

**Scalability:** Can be integrated across multiple platforms, including mobile devices, desktops, and IoT systems.

**Data Privacy and Security:** Employs robust encryption methods (e.g., AES-256) to safeguard biometric data, complying with privacy standards.

**Customization Potential:** Can be adapted to suit various security levels and industries, such as healthcare, banking, or home automation.

**Disadvantages/Limitations:**

**Dependence on Hardware:** Requires devices with cameras and sufficient computational power, which may limit accessibility for older or low-end devices.

**Environmental Constraints:** Performance could degrade in poor lighting conditions or environments with excessive glare.

**Learning Curve:** New users might need guidance to understand and use the randomized facial expression feature effectively.

**Security Risks:** Despite strong liveness detection, the system may still be vulnerable to advanced spoofing techniques or adversarial AI attacks.

**Data Privacy Concerns:** Storing and processing biometric data may raise concerns among users, requiring strict compliance with regulations like GDPR.

**Implementation Complexity:** Integration with existing systems and platforms can be technically challenging and resource intensive.

**Limited Accessibility:** Users with facial disabilities or impairments may find the system challenging to use, requiring additional accessibility features which is something that I have discussed with my supervisor and come up with a few ideas for improvements to be made in the future for increased accessibility. Also addressed in my proposal and ethics consideration.

**Summary:**

BioPass is a highly secure and innovative authentication solution, offering significant advantages in user convenience and cybersecurity. Its unique combination of facial recognition and randomized expressions makes it a strong candidate for combating modern security threats. However, it faces limitations related to hardware requirements, environmental challenges, and potential accessibility barriers that I hope it can overcome later in its course. Addressing these issues in future iterations would further strengthen the project and expand its applicability.

# Further Development or Research

**Future Directions for the BioPass Project**

**With additional time and resources, the BioPass project could expand in several promising directions to enhance its functionality, scalability, and market potential:**

**Integration with IoT Devices:** Extend BioPass to authenticate users on smart devices such as smart locks, home automation systems, and wearable devices, creating a unified and secure ecosystem for the Internet of Things.

**Advanced Machine Learning Models**: Incorporate more sophisticated machine learning algorithms to improve facial recognition accuracy and liveness detection, even under challenging conditions such as occlusions, extreme angles, or motion blur.

**Cross-Platform Synchronization:** Develop seamless synchronization capabilities across multiple devices, allowing users to authenticate securely across their digital environments without redundant setup processes.

**Support for Additional Biometrics:** Combine facial recognition with other biometric modalities, such as voice recognition or fingerprint scanning, to create a multi-modal authentication system for enhanced security.

**Privacy-Preserving Technologies:** Introduce privacy-preserving mechanisms, such as federated learning or homomorphic encryption, to allow secure data processing without exposing user biometrics to central servers.

**Enterprise Solutions:** Expand BioPass into enterprise environments by integrating it with identity and access management (IAM) systems, offering organizations a robust and scalable authentication solution.

**Enhanced Usability for Accessibility:** Improve usability for individuals with disabilities by incorporating customizable prompts and accessibility features, ensuring inclusivity.

**AI-Powered Threat Detection:** Integrate AI systems to monitor and identify unusual authentication patterns, proactively alerting administrators to potential security threats.

**Global Compliance and Certification:** Align the system with international data protection regulations such as GDPR, CCPA, and HIPAA, and pursue industry certifications to enhance credibility and market acceptance.

**Customizable Authentication Flows:** Enable organizations to tailor authentication workflows, such as specifying the number or type of facial expressions required, to suit their unique security needs.

By pursuing these directions, BioPass could evolve into a versatile, state-of-the-art authentication solution, meeting diverse user needs and addressing the ever-growing challenges in cybersecurity.

# References

Afyq, H. (2024) 'PyTorch and Face liveness Detection: A Comprehensive guide,' *Medium*, 16 January. https://medium.com/@hazqeelafyq09/pytorch-and-face-liveness-detection-a-comprehensive-guide-007b926bb222.

Amos, D. (2024) *Python GUI programming with Tkinter*. https://realpython.com/python-gui-tkinter/.

Brandon Jacobson (Jacobson Enterprises) (2020) *Face Recognition for Access Authentication with Python and OpenCV | #109 (S.H.A.N.E. Updates #10)*. https://www.youtube.com/watch?v=h4QbQxbb4Q4.

CodingEntrepreneurs (2018) *OpenCV Python TUTORIAL #4 for face recognition and identification*. https://www.youtube.com/watch?v=PmZ29Vta7Vc.

Computer vision engineer (2022) *Face recognition + liveness detection: Face attendance system*. https://www.youtube.com/watch?v=\_KvtVk8Gk1A.

Computer vision engineer (2023) *Machine learning web app with Python, Streamlit & Segment Anything Model | Modelbit model deployment*. https://www.youtube.com/watch?v=W8OvdQPL7lk.

Computer vision engineer (2024) *Face recognition and face matching with Python and DeepFace | Facial analysis | Computer vision*. https://www.youtube.com/watch?v=FavHtxgP4l4.

Computervisioneng (no date) *GitHub - computervisioneng/face-attendance-system*. https://github.com/computervisioneng/face-attendance-system.

DSwithBappy (2023) *Real Time Face Detection using Haar-cascade Model | OpenCV-Python🔥*. https://www.youtube.com/watch?v=V-EROj-3pEw.

Endangered AI (2024) *Combine FaceID and Facial Expressions with IPAdapter & Controlnet*. https://www.youtube.com/watch?v=IlOOzmQZBzU.

Geitgey, A. (2020) 'Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning,' *Medium*, 24 September. https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78.

Good Morning Developers (2024) *Want to learn some AI with JavaScript? Let’s do facial recognition!* https://www.youtube.com/watch?v=NG5Vi8zrqMM.

Italojs (no date) *facial-landmarks-recognition/shape\_predictor\_68\_face\_landmarks.dat at master · italojs/facial-landmarks-recognition*. https://github.com/italojs/facial-landmarks-recognition/blob/master/shape\_predictor\_68\_face\_landmarks.dat.

KNOWLEDGE DOCTOR (2023) *Face recognition based smart attendance system with web apps using machine learning.* https://www.youtube.com/watch?v=BYCKvM8eZGA.

Murtaza’s Workshop - Robotics and AI (2022) *Face Recognition with Real Time Database | 2 Hour Course | Computer Vision*. https://www.youtube.com/watch?v=iBomaK2ARyI.

Murtaza’s Workshop - Robotics and AI (2023) *Free Anti Spoofing/ liveliness Detector for face recognition System Fake VS Real | Computer Vision*. https://www.youtube.com/watch?v=LqzPifvd09Q.

Nirav Bhavsar (2020) *Anti-Spoofing in face recognition*. https://www.youtube.com/watch?v=sNm2gxsGn-o.

Progress with Python (2023) *Face Emotion Recognition using Machine Learning | Python*. https://www.youtube.com/watch?v=aoCIoumbWQY.

Pysource (2021) *Face recognition in real-time | with Opencv and Python*. https://www.youtube.com/watch?v=5yPeKQzCPdI.

Saaisri (2022) 'Deepface Face recognition - featurepreneur - Medium,' *Medium*, 23 July. https://medium.com/featurepreneur/deepface-face-recognition-91ebb7e794a4.

SajalSinha (no date) *Facial-Emotion-Recognition/FER\_model.h5 at main · SajalSinha/Facial-Emotion-Recognition*. https://github.com/SajalSinha/Facial-Emotion-Recognition/blob/main/FER\_model.h5.

Sefik Ilkin Serengil (2024) *Face Anti-Spoofing for facial recognition in Python*. https://www.youtube.com/watch?v=UiK1aIjOBlQ.

Serengil, S. (2024) *Face Anti-Spoofing for Facial recognition in Python - Sefik Ilkin Serengil*. https://sefiks.com/2024/06/08/face-anti-spoofing-for-facial-recognition-in-python/#google\_vignette.

*Step-1\_find-faces.py* (no date). https://gist.github.com/ageitgey/1c1cb1c60ace321868f7410d48c228e1.

*Step-2a\_finding-face-landmarks.py* (no date). https://gist.github.com/ageitgey/ae340db3e493530d5e1f9c15292e5c74.

*Step-2b\_projecting-faces.py* (no date). https://gist.github.com/ageitgey/82d0ea0fdb56dc93cb9b716e7ceb364b.

# Appendices

Belo are the relevant appendices related to the BioPass project.

## Project Proposal



National College of Ireland

Project Proposal

BioPass

20/10/2024

BSc Hons Computing

Cybersecurity

2024/2025

Aisha Ntuli

X21341006

X21341006@student.ncirl.ie

Contents

[1.0 Objectives 2](#_Toc83590869)

[2.0 Background 2](#_Toc83590870)

[3.0 State of the Art 2](#_Toc83590871)

[4.0 Technical Approach 2](#_Toc83590872)

[5.0 Technical Details 2](#_Toc83590873)

[6.0 Special Resources Required 2](#_Toc83590874)

[7.0 Project Plan 2](#_Toc83590875)

[8.0 Testing 2](#_Toc83590876)

# Objectives

(Max half Page)

What does this project set out to achieve?

This project sets out to achieve the creation and implementation of a secure passwordless 2FA that uses biometric technology to recognise a series of facial expressions and movements essentially equal to how a passcode works on any device. It will be securely encrypted unlike the software used on dating apps or pay instalment apps for example that only require ID upload without further physical inspection. This passwordless 2FA technology can used for secure IAM(identity access management), secure log in and potentially extended to use on dating apps to help with individual verification. It can be especially useful for people who have a particularly hard time remembering passwords and managing multiple accounts such as the elderly or those with memory loss.

# Background

(Max half Page)

Why did you choose to undertake this project? How will you meet the objectives set out in Section 1.0?

The reason I chose to undertake this project is that right now there is a very big problem regarding biometric theft for nefarious purposes. Originally, I wanted to do something that would help to combat the massive problem right now with people’s likeness’ being used for illicit purposes such as Deepfake usage, AI usage or content upload to adult websites without consent. My ideas were proving difficult to implement and too vulnerable for hackers or even just wrongdoers online. There were also a lot of issues storing data on the cloud, difficulty storing biometric data, too many rogue websites, too many ethical problems and GDPR problems. Along with this I had a hard time deciding what it was I wanted this technology to do whether I wanted it to be a face anonymisation tool or something else. I unfortunately found it hard to pinpoint and stick to one idea from the plethora that I had, and they were proving to not be as feasible as I would have liked.

While this idea is notably different to my initial idea, I do hope that its technology can be further developed to help with data and privacy protection or act as a launchpad for others to add to it. I settled on this particular idea as data laws are constantly under review as new problems arise and GDPR is a new and technological era specific problem. I will meet the objectives that I set out in section 1.0 by providing the accurate and relevant research to help me expand on and implement my idea.

I will also achieve this by focusing on what I know and playing to my strengths to begin prototyping and implementation as soon as possible by using my favourite technologies and programming languages.

# State of the Art

(Max half page)

What similar applications exist already? What makes your project stand out? How does it differ from similar work of others?

From what I know there are currently there are no other applications that exist exactly like this regarding the use of facial expressions and movements in the same way a passcode is used but facial recognition already exists. It has been implemented across hundreds if not thousands of applications for the purpose of 2FA. Essentially the “face passcode” along with secure encryption can hopefully add more protection than these already existing applications. I have however seen a couple research papers that also suggest this as an idea from ResearchGate and International Institute of Engineers.

(Max 1 page)

What approach will you take to development? How will you identify requirements? How will you break down requirements into project tasks, activities and milestones?

When approaching the development of this technology, as stated before I want to provide myself with the most amount of time possible for prototyping, implementation, and testing. I will play to my strengths and stick to what I know instead of over complicating things for myself. I will use my favourite technologies and programming languages that I am either already somewhat or very familiar with to supply myself with an appropriate amount of challenge as well as providing myself with the familiarity I need to be able to complete the project without having to self-teach many new concepts and languages from scratch.

To identify the requirements, I will look at exactly what it is that I want my application to do, from my research I should be able to see snippets of other similar applications and usages as I’ve stated there are similar applications that use Face ID or facial recognition along with research papers I can also use to identify what has not been used before and consider implementing possible new ideas that are not too challenging.

When it comes to breaking down requirements into project tasks, activities, and milestones I already have many ideas on how I’ll be able to divide this projects tasks appropriately. Firstly, seeing as this is a 2FA application it’s possible for me to divide the project into the first factor of authentication, then the second factor of authentication and from there divide the different stages of authentication into multiple steps and goals as well as adding other steps such as documentation, code commenting, screenshotting checkpoints, monthly journals. For now, my main goal is research in terms of what language(s) I will use, what technologies I will use, how I will protype, implement, test, deploy, what applications similar to this already exist, what improvements I can make to my own etc. I also want to make a spreadsheet that I will divide into two semesters for the first semester my idea is to get a prototype up and running by the end of the first semester then fine tune during the second semester and focus on my documentation especially because the teaching weeks are short. By having a checklist that even goes into to weekly goals I’m sure I can stay on top of my goals this way.

# Technical Details

(Max 1 page)

Implementation language and principal libraries. What are the important algorithms or approaches under consideration for this work?

In terms of implementation language **Python** is widely used for projects involving machine learning and computer vision. It is simple, flexible and has considerable community support. Alternatives include **JavasScript** for real time, browser-based systems which is what I am considering using as I want to prototype for browsers with my computer webcam. **C++** is also a possible alternative, but its drawback is that it’s more difficult to implement than Python and I don’t have as much experience with it.

When considering principal libraries for facial expression detection the following may be considered: **OpenCV is a** is a powerful open-source computer vision library that provides real-time detection and tracking capabilities. Which can be used to detect key facial attributes(eyes, mouth, eyebrows) and track expression specific movements.

**Dlib** is a machine learning toolkit and facial landmark detection. Often used in conjunction with OpenCV for the most accurate facial expression detection.

**TensorFlow/PyTorch** is used for building and training custom deep learning models to class these facial expressions. Pre-trained models may also be used for this.

**Mediapipe** is a fast reliable framework for facial expression recognition designed specifically for real-time performance, making it ideal for these systems. I will probably make great use of this specifically due to the browser-based prototype that I plan on leaning towards.

When considering important algorithms and approaches the main ones would include **facial landmark detection, real-time image processing**  and **convolutional neural networks**.

This is a brief description of all the libraries and algorithms that are available for use but a strong combination of them should result in the implementation of a robust AI system which has room for future enhancements in both areas of the 2FA.

# Special Resources Required

(Max half page)

What special resources if any will be required for this work?

I don’t think that any special resources will be required to complete this project as 2FA is relatively simple and being able to get a handful of consenting participants to make sure the application works on more than just my face alone should be simple and easy. So no, currently I am not considering any special resources for the completion of this project.

# Project Plan

(Max 2 pages)

Project plan with details on implementation steps and timelines. This project plan should provide as much detail as possible for now and will be revised with more detail with the mid point documentation.

For my project plan as stated before for my project my main goal as of right now is to get a prototype up and running by the end of the first semester around the time when we will have our mid-point presentation and to meet with my supervisor at least once every two weeks to meet my weekly or bi-weekly goals of what I want to get done.

In the first phase which is now I will mostly be researching and requirements gathering. So, identifying what technologies and languages I want to use, identifying my strengths and what languages I have the most familiarity with. Researching 2FA and how its made and implemented. Define the facial expressions I want to use for the project. For the purpose of ease, I want to choose easily adopted facial expressions like a smile, scrunching your face, raising your eyebrows, tilting your head to either side and blinking or winking. I will also be investigating available libraries for facial expression detection I’m leaning towards using Python coupled with OpenCV, Dlib and/or Mediapie. Then I will implement a basic prototype to capture facial expressions using OpenCV, Dlib or Mediapipe along with identifying facial landmarks. I will then develop and refine algorithms for recognising the predetermined facial expressions while implementing error handling for face occlusion or misalignment. From there I hope to fine tune and test then train a deep learning model such as TensorFlow or PyTorch for more accurate facial expression detection and then possibly further for a variety of conditions.

Following this I will conduct unit tests for the facial recognition and the expression recognition. Test for edge cases such as lighting variations. Usability tests to measure the system’s accuracy and user experience. Noting the results and user feedback. Fixing any identified bugs and issues ensuring the system works efficiently then deployment.

Ongoing tasks I must keep up with as the project goes on are documentation including code documentation, screenshotting commenting, noting changes.

# Testing

(Max 1 page)

Describe how you will evaluate the system with real technical data using system tests, integration tests etc. If applicable describe how you will evaluate the system with an **end user. (be careful here re Ethics etc)**

To evaluate the system with tests, first thing to note is that there are multiple areas to test.

**System Tests**  will focus on evaluating the system’s correctness and each components performance.

**-Functional Testing** will test the accuracy of facial expression recognition in varying conditions, angles, and distances. Along with whether the system accurately detects specific facial expression sequences with variation in speed.

**-Performance Tests** will measure the system’s processing response time for latency and resource consumption.

**-Security Tests** will include attack simulation such as reusing facial expressions and of course the ideal outcome being that the system rejects them accordingly. In addition, simulating spoofing attacks using photos or videos.

**Integration Tests** will focus on making sure the 2FA works seamlessly the first factor being a face and the second being recognising the facial expression.

**-Sequential Input Testing** will test how well the system handles facial recognition and then facial expression recognition. Then ensure that the system correctly verifies the inputs within the expected time window. Test for scenarios when the face is recognised but not the expression e.g. user is scrunching their face when the system is looking for raised eyebrows then denying access.

­**-Error Handling and Recovery** this testing will focus on simulating network delays, camera failures, authentication interruption and evaluate the system’s ability to recover and prompt users for re-entry.

Also ensuring the system provides clear feedback in case of invalid input such as put face in guidelines or retry facial expression.

**End-User Evaluation** would mean that ideally, I will be able to get test subjects besides myself to assess the usability and general user experience.

**-User Scenario Testing** would involve the test of the system in a controlled environment with users performing authentication using their face and then their facial expressions.

Collect feedback on how easy the system is to use and users’ comfortability in performing the required expressions.

Assess how users can remember the expressions sequence and if they encounter any difficulty.

**-Accessibility Testing** will evaluate the system’s accessibility for users with specialised needs or facial mobility limitations. This will aid in making note of potential challenges users with disabilities face and explore necessary improvements.

**Final System Evaluation**

A final evaluation will be conducted against traditional 2FA methods (traditional passwords or SMS 2FA).

The system will be performance evaluated by authentication time, accuracy, security against established 2FA methods.

Identify advantages or limitations based on security, user experience and practical deployment.

This comprehensive testing plan will ensure that the system I’ve created works and then tests how it can be further improved or it’s possible improvements.

## Ethics Approval Application (only if required)

**National College of Ireland**

**DECLARATION OF ETHICS CONSIDERATION**

**School of Computing**

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name:** | Aisha Ntuli | | |
| **Student ID:** | X21341006 | | |
| **Programme** | BSc Hons Computing | **Year:** | 2024/2025 |
| **Module:** | Computing Project | | |
| **Project Title:** | BioPass | | |

**Please circle (or highlight) as appropriate**

|  |  |
| --- | --- |
| This project involves human participants | Yes / No |

# **Introduction**

Secondary data refers to data that is collected by someone other than the current researcher. Common sources of secondary data for social science include censuses, information collected by government departments, organizational records and data originally collected for other research purposes. Primary data, by contrast, is collected by the investigator conducting the research.

A project that does not involve human participants requires ONLY completion of Declaration of Ethics Consideration Form and submission of the form on module’s Moodle page

A project that involves human participants requires ethical clearance and an Ethics Application Form must be submitted through the module’s Moodle page. Please refer to and ensure compliance with the ethical principles stated in NCI Ethics Form available on the Moodle page.

The following decision table will assist you in deciding if you have to complete the Declaration of Ethics Consideration Form or/and the Ethics Application Form.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Public Data | Y | Y | Y | Y | N | N | N | N |
| Private Data | Y | Y | N | N | Y | Y | N | N |
| Human Participants | Y | N | Y | N | Y | N | Y | N |
|  |  |  |  |  |  |  |  |  |
| Declaration of Ethics Consideration Form | x | X | x | X | X | X | x |  |
| Ethics Application Form | X |  | X |  | X |  | X |  |

**Please circle (or highlight) as appropriate**

|  |  |
| --- | --- |
| The project makes use of secondary dataset(s) created by the researcher | Yes / No |
| The project makes use of public secondary dataset(s) | Yes / No |
| The project makes use of non-public secondary dataset(s)  Approval letter from non-public secondary dataset(s) owner received | Yes / No  Yes / No |

# **Sources of Data**:

***It is students’ responsibility to ensure that they have the correct permissions/authorizations to use any data in a study. Projects that make use of data that does not have authorization to be used, will not be graded for that portion of the study that makes use of such data.***

***Public Data***

*A project that makes use of public secondary dataset(s)* ***does not need ethics permission****, but* ***needs a letter/email from the copyright holder*** *regarding potential use.*

*Some websites and data sources allow their data sets to be used under certain conditions. In these cases, a letter/email from the copyright holder is NOT necessary, but the researcher should cite the source of this permission and indicate under what conditions the data are allowed to be used. See Appendix I for examples of permissions granted by Fingal Open Data, and Eurostat website.*

*Where websites or data sources indicate that they do not grant permission for data to be used, you will still need a letter/email from the copyright holder. For example, see Appendix II for an example from the Journal of Statistics Education.*

***Private Data***

*A project that makes use of non-public (private) secondary dataset(s) must receive data usage permission from School of Computing.*

***An approval letter/email from the owner*** *(e.g. institution, company, etc.)* ***of the non-public secondary dataset must be attached to the Declaration of Ethics Consideration****. The letter/email must confirm that the dataset is anonymised and permission for data processing, analysis and public dissemination is granted.*

**Evidence for use of secondary dataset(s)**

Include dataset(s) owner letter/email or cite the source for usage permission

I don’t believe I will be using any secondary datasets.

# **CHECKLIST**

|  |  |
| --- | --- |
| Non-public/private secondary dataset(s) -Owner letter/email is attached to this form  ***OR***  Citation and link to the web site where permission is granted – provided in this form | Yes / No  Yes / No |

## **ETHICS CLEARANCE GUIDELINES WHEN HUMAN PARTICIPANTS ARE INVOLVED**

**The Ethics Application Form must be submitted on Moodle for approval prior to conducting the work.**

Considerations in data collection

* Participants will not be identified, directly or through identifiers linked to the subjects in any reports produced by the study
* Responses will not place the participants at risk of professional liability or be damaging to the participants’ financial standing, employability or reputation
* No confidential data will be used for personal advantage or that of a third party

Informed consent

* Consent to participate in the study has been given freely by the participants
* participants have the capacity to understand the project goals.
* Participants have been given information sheets that are understandable
* Likely benefits of the project itself have been explained to potential participants
* Risks and benefits of the project have been explained to potential participants
* Participants have been assured they will not suffer physical stress or discomfort or psychological or mental stress
* The participant has been assured s/he may withdraw at any time from the study without loss of benefit or penalty
* Special care has been taken where participants are unable to consent for themselves (e.g children under the age of 18, elders with age 85+, people with intellectual or learning disability, individuals or groups receiving help through the voluntary sector, those in a subordinate position to the researcher, groups who do not understand the consent and research process)
* Participants have been informed of potential conflict of interest issues
* The onus is on the researcher to inform participants if deception methods have to be used in a line of research

**I have read, understood, and will adhere to the ethical principles described above in the conduct of the project work.**

|  |  |
| --- | --- |
| **Signature:** | Aisha Ntuli |
| **Date:** | 20/10/24 |

# **Appendix I**

1. ***Fingal Open Data: http://data.fingal.ie/About***

Licence

Citizens are free to access and use this data as they wish, free of charge, in accordance with the Creative Commons Attribution 4.0 International License (CC-BY).

Note: From November 2010 to July 2015, data on Fingal Open Data was published in accordance with the PSI general licence.

Use of any published data is subject to Data Protection legislation.

Licence Statement

Under the CC-BY Licence, users must acknowledge the source of the Information in their product or application by including or linking to this attribution statement: “Contains Fingal County Council Data licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence”.

Multiple Attributions

If using data from several Information Providers and listing multiple attributions is not practical in a product or application, users may include a URI or hyperlink to a resource that contains the required attribution statements.

1. ***Eurostat: https://ec.europa.eu/eurostat/about/policies/copyright***

COPYRIGHT NOTICE AND FREE RE-USE OF DATA

Eurostat has a policy of encouraging free re-use of its data, both for non-commercial and commercial purposes. All statistical data, metadata, content of web pages or other dissemination tools, official publications and other documents published on its website, with the exceptions listed below, can be reused without any payment or written licence provided that:

* the source is indicated as Eurostat
* when re-use involves modifications to the data or text, this must be stated clearly to the end user of the information

# **Appendix II**

**Journal of Statistics Education: http://jse.amstat.org/jse\_users.htm**

JSE Copyright and Usage Policy

Unlike other American Statistical Association journals, the Journal of Statistics Education (JSE) does not require authors to transfer copyright for the published material to JSE. Authors maintain copyright of published material. Because copyright is not transferred from the author, permission to use materials published by JSE remains with the author. Therefore, to use published material from a JSE article the requesting person must get approval from the author.

**National College of Ireland**

**Human Participants Ethical Review Application Form**

All parts of the below form must be completed. However in certain cases where sections are not relevant to the proposed study, clearly mark NA in the box provided.

Part A: Title of Project and Contact Information

**Name**

Aisha Ntuli

**Student Number (if applicable)**

X21341006

**Email**

X21341006@student.ncirl.ie

**Status:**

Undergraduate y □

Postgraduate □

Staff □

**Supervisor (if applicable)**

Michael Bradford

**Title of Research Project**

BioPass

**Category into which the proposed research falls (see guidelines)**

**Research Category A y** □

Research Category B □

Research Category C □

**Have you read the NCI Ethical Guidelines for Research with Human Participants?**

Yes y□

No □

**Please indicate any other ethical guidelines or codes of conduct you have consulted**

**N/A**

**Has this research been submitted to any other research ethics committee?**

Yes □

No n□

If yes please provide details, and the outcomes of this process, if applicable:

**N/A**

**Is this research supported by any form of research funding?**

Yes □

No n□

If yes please provide details, and indicate whether any restrictions exist on the freedom of the researcher to publish the results:

N/A

Part B: Research Proposal

Briefly outline the following information (not more than 200 words in any section).

**Proposed starting date and duration of project**

Oct 2024 – May 2025

**The rationale for the project**

**2FA using facial expression recognition.**

**The research aims and objectives**

**A passwordless alternative to sign into accounts.**

**The research design**

Facial recognition technologies will be used to identify faces and facial expressions however data will not be stored.

**The research sample and sample size**

**Please indicate the sample size and your justification of this sample size. Describe the age range of participants, and whether they belong to medical groups (those currently receiving medical treatment, those not in remission from previous medical treatment, those recruited because of a previous medical condition, healthy controls recruited for a medical study) or clinical groups (those undergoing non-medical treatment such as counselling, psychoanalysis, in treatment centres, rehabilitation centres, or similar, or those with a DSM disorder diagnosis).**

I am most likely going to recruit the participation of 4 college peers close to my own age for testing and my mother as an older subject for testing.

**If the study involves a MEDICAL or CLINICAL group, the following details are required:**

1. **Do you have approval from a hospital/medical/specialist ethics committee?**

**If YES, please append the letter of approval. Also required is a letter from a clinically responsible authority at the host institution, supporting the study, detailing the support mechanisms in place for individuals who may become distressed as a result of participating in the study, and the potential risk to participants.**

**If NO, please detail why this approval cannot or has not been saught.**

1. **Does the study impact on participant’s medical condition, wellbeing, or health?   
   If YES, please append a letter of approval from a specialist ethics committee.**

**If NO, please give a detailed explanation about why you do not expect there to be an impact on medical condition, wellbeing, or health.**

**The nature of any proposed pilot study. Pilot studies are usually required if a) a new intervention is being used, b) a new questionnaire, scale or item is being used, or c) established interventions or questionnaires, scales or items are being used on a new population. If no such study is planned, explain why it is not necessary.**

N/A

**The methods of data analysis. Give details here of the analytic process (e.g. the statistical procedures planned if quantitative, and the approach taken if qualitative. It is not sufficient to name the software to be used).**

N/A

**Study Procedure**

**Please give as detailed an account as possible of a participant’s likely experience in engaging with the study, from point of first learning about the study, to study completion. State how long project participation is likely to take, and whether participants will be offered breaks. Please attach all questionnaires, interview schedules, scales, surveys, and demographic questions, etc. in the Appendix.**

N/A

Part C: Ethical Risk

**Please identify any ethical issues or risks of harm or distress which may arise during the proposed research, and how you will address this risk. Here you need to consider the potential for physical risk, social risk (i.e. loss of social status, privacy, or reputation), outside of that expected in everyday life, and whether the participant is likely to feel distress as a result of taking part in the study. Debriefing sheets must be included in the appendix if required.** These should detail the participant’s right to withdraw from the study, the statutory limits upon confidentiality, and the obligations of the researcher in relation to Freedom of Information legislation. Debriefing sheets should also include details of helplines and avenues for receiving support in the event that participants become distressed as a result of their involvement in this study.

I don’t think there is any significant ethical risk to be had with this project however if i manage to find a participant with limited facial mobility to test the system for its limitations I would make them aware that is why I am asking them to participate.

**Do the participants belong to any of the following vulnerable groups?**

(Please tick all those involved).

□ Children;

□ The older old (85+)

□ People with an intellectual or learning disability

□ Individuals or groups receiving help through the voluntary sector

□ Those in a subordinate position to the researchers such as employees

□ Other groups who might not understand the research and consent process

□ Other vulnerable groups

**How will the research participants in this study be selected, approached and recruited? From where will participants be recruited? If recruiting via an institution or organisation other than NCI please attach a letter of agreement from the host institution agreeing to host the study and circulate recruitment advertisements/email etc.**

I will be choosing them based on proximity and willingness to participate again my mother would most likely agree to help and my friends/peers from college would also most likely agree.

**What inclusion or exclusion criteria will be used?**

I hope to find at least one user with facial mobility limitations.

**How will participants be informed of the nature of the study and participation?**

I will inform them exactly what the system does and what I am trying to test for

**Does the study involve deception or the withholding of information? If so, provide justification for this decision.**

It does not involve any deception.

**What procedures will be used to document the participants’ consent to participate?**

Most likely a Microsoft/Google form or similar application.

**Can study participants withdraw at any time without penalty? If so, how will this be communicated to participants?**

Yes, this information will be included in the sign up form.

**If vulnerable groups are participating, what special arrangements will be made to deal with issues of informed consent/assent?**

There will not be any special groups participating.

*Please include copies of any information letters, debriefing sheets, and consent forms with the application.*

Part D: Confidentiality and Data Protection

**Please indicate the form in which the data will be collected.**

y□ Identified □Potentially Identifiable□ **De-Identified**

**What arrangements are in place to ensure that the identity of participants is protected?**

I am not 100% sure I am anaswering this correctly because I do not plan on keeping the participants data anywhere.

**Will any information about illegal behaviours be collected as part of the research process? If so, detail your consideration of how this information will be treated.**

No

**Please indicate any recording devices being used to collect data (e.g. audio/video).**

There is a possibility of sibject video being used but I will most likely test with my own video.

**Please describe the procedures for securing specific permission for the use of these recording devices in advance.**

I will be using my own phone.

**Please indicate the form in which the data will be stored.**

y□ Identified □ Potentially Identifiable □ **De-Identified**

**Who will have responsibility for the data generated by the research?**

Again I am not sure I am answering this ocrrectly as I don’t plan on keeping this data long term but I will consult with my supervisor and make the necessary changes.

Is there a possibility that the data will be archived for secondary data analysis? If so, has this been included in the informed consent process? Also include information on how and where the data will be stored for secondary analytic purposes.

This is not likely.

If not to be stored for secondary data analysis, will the data be stored for 5 years and then destroyed, in accordance with NCI policy?

y □ Yes □ No

**Dissemination and Reporting**

**Please describe how the participants will be informed of dissemination and reporting (e.g. submission for examination, reporting, publications, presentations)?**

It willl be included in the application form aswell.

**If any dissemination entails the use of audio, video and/or photographic records (including direct quotes), please describe how participants will be informed of this in advance.**

Also included in the application form.

Part E: Signed Declaration

I confirm that I have read the NCI Ethical Guidelines for Research with Human Participants, and agree to abide by them in conducting this research. I also confirm that the information provided on this form is correct (Electronic signature is acceptable).

**Signature of Applicant Aisha Ntuli**

**Date 20/10/24**

**Signature of Supervisor (where appropriate):**

**Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Any other information the committee should be aware of?**

N/A

**National College of Ireland**

**Human Participants Ethical Review Application Form**

All parts of the below form must be completed. However in certain cases where sections are not relevant to the proposed study, clearly mark NA in the box provided.

Part A: Title of Project and Contact Information

**Name**

Aisha Ntuli

**Student Number (if applicable)**

X21341006

**Email**

X21341006@student.ncirl.ie

**Status:**

Undergraduate y □

Postgraduate □

Staff □

**Supervisor (if applicable)**

Michael Bradford

**Title of Research Project**

BioPass

**Category into which the proposed research falls (see guidelines)**

**Research Category A y** □

Research Category B □

Research Category C □

**Have you read the NCI Ethical Guidelines for Research with Human Participants?**

Yes y□

No □

**Please indicate any other ethical guidelines or codes of conduct you have consulted**

**N/A**

**Has this research been submitted to any other research ethics committee?**

Yes □

No n□

If yes please provide details, and the outcomes of this process, if applicable:

**N/A**

**Is this research supported by any form of research funding?**

Yes □

No n□

If yes please provide details, and indicate whether any restrictions exist on the freedom of the researcher to publish the results:

N/A

Part B: Research Proposal

Briefly outline the following information (not more than 200 words in any section).

**Proposed starting date and duration of project**

Oct 2024 – May 2025

**The rationale for the project**

**2FA using facial expression recognition.**

**The research aims and objectives**

**A passwordless alternative to sign into accounts.**

**The research design**

Facial recognition technologies will be used to identify faces and facial expressions however data will not be stored.

**The research sample and sample size**

**Please indicate the sample size and your justification of this sample size. Describe the age range of participants, and whether they belong to medical groups (those currently receiving medical treatment, those not in remission from previous medical treatment, those recruited because of a previous medical condition, healthy controls recruited for a medical study) or clinical groups (those undergoing non-medical treatment such as counselling, psychoanalysis, in treatment centres, rehabilitation centres, or similar, or those with a DSM disorder diagnosis).**

I am most likely going to recruit the participation of 4 college peers close to my own age for testing and my mother as an older subject for testing.

**If the study involves a MEDICAL or CLINICAL group, the following details are required:**

1. **Do you have approval from a hospital/medical/specialist ethics committee?**

**If YES, please append the letter of approval. Also required is a letter from a clinically responsible authority at the host institution, supporting the study, detailing the support mechanisms in place for individuals who may become distressed as a result of participating in the study, and the potential risk to participants.**

**If NO, please detail why this approval cannot or has not been saught.**

1. **Does the study impact on participant’s medical condition, wellbeing, or health?   
   If YES, please append a letter of approval from a specialist ethics committee.**

**If NO, please give a detailed explanation about why you do not expect there to be an impact on medical condition, wellbeing, or health.**

**The nature of any proposed pilot study. Pilot studies are usually required if a) a new intervention is being used, b) a new questionnaire, scale or item is being used, or c) established interventions or questionnaires, scales or items are being used on a new population. If no such study is planned, explain why it is not necessary.**

N/A

**The methods of data analysis. Give details here of the analytic process (e.g. the statistical procedures planned if quantitative, and the approach taken if qualitative. It is not sufficient to name the software to be used).**

N/A

**Study Procedure**

**Please give as detailed an account as possible of a participant’s likely experience in engaging with the study, from point of first learning about the study, to study completion. State how long project participation is likely to take, and whether participants will be offered breaks. Please attach all questionnaires, interview schedules, scales, surveys, and demographic questions, etc. in the Appendix.**

N/A

Part C: Ethical Risk

**Please identify any ethical issues or risks of harm or distress which may arise during the proposed research, and how you will address this risk. Here you need to consider the potential for physical risk, social risk (i.e. loss of social status, privacy, or reputation), outside of that expected in everyday life, and whether the participant is likely to feel distress as a result of taking part in the study. Debriefing sheets must be included in the appendix if required.** These should detail the participant’s right to withdraw from the study, the statutory limits upon confidentiality, and the obligations of the researcher in relation to Freedom of Information legislation. Debriefing sheets should also include details of helplines and avenues for receiving support in the event that participants become distressed as a result of their involvement in this study.

I don’t think there is any significant ethical risk to be had with this project however if i manage to find a participant with limited facial mobility to test the system for its limitations I would make them aware that is why I am asking them to participate.

**Do the participants belong to any of the following vulnerable groups?**

(Please tick all those involved).

□ Children;

□ The older old (85+)

□ People with an intellectual or learning disability

□ Individuals or groups receiving help through the voluntary sector

□ Those in a subordinate position to the researchers such as employees

□ Other groups who might not understand the research and consent process

□ Other vulnerable groups

**How will the research participants in this study be selected, approached and recruited? From where will participants be recruited? If recruiting via an institution or organisation other than NCI please attach a letter of agreement from the host institution agreeing to host the study and circulate recruitment advertisements/email etc.**

I will be choosing them based on proximity and willingness to participate again my mother would most likely agree to help and my friends/peers from college would also most likely agree.

**What inclusion or exclusion criteria will be used?**

I hope to find at least one user with facial mobility limitations.

**How will participants be informed of the nature of the study and participation?**

I will inform them exactly what the system does and what I am trying to test for

**Does the study involve deception or the withholding of information? If so, provide justification for this decision.**

It does not involve any deception.

**What procedures will be used to document the participants’ consent to participate?**

Most likely a Microsoft/Google form or similar application.

**Can study participants withdraw at any time without penalty? If so, how will this be communicated to participants?**

Yes, this information will be included in the sign up form.

**If vulnerable groups are participating, what special arrangements will be made to deal with issues of informed consent/assent?**

There will not be any special groups participating.

*Please include copies of any information letters, debriefing sheets, and consent forms with the application.*

Part D: Confidentiality and Data Protection

**Please indicate the form in which the data will be collected.**

y□ Identified □Potentially Identifiable□ **De-Identified**

**What arrangements are in place to ensure that the identity of participants is protected?**

I am not 100% sure I am anaswering this correctly because I do not plan on keeping the participants data anywhere.

**Will any information about illegal behaviours be collected as part of the research process? If so, detail your consideration of how this information will be treated.**

No

**Please indicate any recording devices being used to collect data (e.g. audio/video).**

There is a possibility of sibject video being used but I will most likely test with my own video.

**Please describe the procedures for securing specific permission for the use of these recording devices in advance.**

I will be using my own phone.

**Please indicate the form in which the data will be stored.**

y□ Identified □ Potentially Identifiable □ **De-Identified**

**Who will have responsibility for the data generated by the research?**

Again I am not sure I am answering this ocrrectly as I don’t plan on keeping this data long term but I will consult with my supervisor and make the necessary changes.

Is there a possibility that the data will be archived for secondary data analysis? If so, has this been included in the informed consent process? Also include information on how and where the data will be stored for secondary analytic purposes.

This is not likely.

If not to be stored for secondary data analysis, will the data be stored for 5 years and then destroyed, in accordance with NCI policy?

y □ Yes □ No

**Dissemination and Reporting**

**Please describe how the participants will be informed of dissemination and reporting (e.g. submission for examination, reporting, publications, presentations)?**

It willl be included in the application form aswell.

**If any dissemination entails the use of audio, video and/or photographic records (including direct quotes), please describe how participants will be informed of this in advance.**

Also included in the application form.

Part E: Signed Declaration

I confirm that I have read the NCI Ethical Guidelines for Research with Human Participants, and agree to abide by them in conducting this research. I also confirm that the information provided on this form is correct (Electronic signature is acceptable).

**Signature of Applicant Aisha Ntuli**

**Date 20/10/24**

**Signature of Supervisor (where appropriate):**

**Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Any other information the committee should be aware of?**

N/A

## Reflective Journals

**Supervision & Reflection Template**

|  |  |
| --- | --- |
| **Student Name** | Aisha Ntuli |
| **Student Number** | X21341006 |
| **Course** | BSc Hons Computing |
| **Supervisor** | N/A |

**Month:**

|  |  |
| --- | --- |
| **What**?  Reflect on what has happened in your project this month?  This month or more accurately the past two weeks have mostly been focused on brainstorming project ideas. What do we want to make? How are we going to make it? How does it differ from other products or services on the market? Where can I secure marks in project creativity, innovation, and difficulty? What steps must be taken to actualise this idea? Who would I like my supervisor to be? I saw a lot of brainstorming going on between my peers and my lecturer had a quick conversation with each of us regarding our project. What ideas we have, how can we refine them, how does the idea relate to our specialisation, what makes our idea innovative and challenging enough to be a capstone project. My initial ideas weren’t very special or innovative which my lecturer noted. This made me a little bit worried because when it comes to college the school weeks pass by fast and my biggest worry was not being able to come up with a creative enough idea whilst having an adequate amount of time to finish my proposal and find the right supervisor. The current key aspects of my situation are finalising and idea, finding a supervisor and beginning the proposal. | |
| **So What?**  Consider what that meant for your project progress. What were your successes? What challenges still remain?  At this moment I have yet to receive the greenlight for my latest idea. I am not entirely sure that it is possible, and I also don’t have a supervisor at the moment. I am mildly worried as I know some of my peers are ahead in this regard, but I am also staying calm because know it is still early and putting too much pressure on myself will give me an unnecessary amount of stress this early into my project. As it stands, I have a rough concept and not much else. The most that I know is that I will probably have to submit an ethics form along with the proposal as it is going to involve me training software to be able to recognise a human face. I’m hoping that by the end of the week I will have a finalised project idea and I hope to have a supervisor confirmed by the end of next week. I feel relatively confident in my new idea which makes me happy because it’s more creative, more innovative, and more difficult that it could be a viable project idea. In a way I am also thankful for my lecturer being wary of my ideas as this means I was able to push myself outside of my comfort zone and consider bigger feats for my project. My main worry right now is that this idea is not as feasible as I think but I will know for sure once my lecturer provides feedback. I think my current experience differs from my peers because some of them have already started with their proposals, have solidified ideas and some even have supervisors confirmed although oddly enough I don’t necessarily feel behind I feel fairly calm. Someone else could view me as being miles behind my peers but I don’t as I try not to compare myself to others too much. | |
| **Now What?**  What can you do to address outstanding challenges?  To address the outstanding challenges. I will first meet with my lecturer to receive approval on my project idea, I will then choose and hopefully secure a supervisor for my project and finally I will begin putting together my proposal. Another challenge in relation to the proposal is to figure out what exactly I want to achieve with the project, what exactly I want the finished product to look like what I want the finished product to do. The ideal future implications are for me to be within the realm of completing my project proposal by the fourth or fifth week of the term. Of course, following project approval and successfully securing a supervisor. If I were to decide not to alter anything at this moment then I would not have a project idea, a supervisor, or a proposal ready for the deadline which is why it’s important I handle these things as soon as possible. If I were to be faced with a similar situation again, I would most likely approach the task in the same manner as I am doing now. I don’t think I am behind I think I am on track, and I have been following all of the necessary steps to achieve my goals in a timely manner. Regarding information that would be helpful for possibly attempting this task again in future I think I would attempt to converse with more people for potential project ideas instead of relying on the library website or Google I think the best ideas come from talking to people in your daily life about pressing issues or problems that they themselves face. Which can be a big factor that allows for you to create a more niche and innovative idea. | |
| **Student Signature** | Aisha Ntuli |

**Supervision & Reflection Template**

|  |  |
| --- | --- |
| **Student Name** | Aisha Ntuli |
| **Student Number** | X21341006 |
| **Course** | BSc Hons in Computing |
| **Supervisor** | Michael Bradford |

This Reflection is inclusive of the October journal that I was unable to submit.

**Month:**

|  |  |
| --- | --- |
| **What**?  Reflect on what has happened in your project this month?  Reflecting on what has happened in my project this past month I have not done as much as I could have for my computing project. If I’m being honest this has been a particularly tough month in balancing and managing my workload across multiple modules. I have multiple close deadlines and I’m trying to prioritise accordingly. However I did manage to add liveness detection to my project through blinking detection. | |
| **So What?**  Consider what that meant for your project progress. What were your successes? What challenges still remain?  It meant very little for my project’s progress. I managed to implement the liveness detection through blinking detection which was my only success so far. The challenges that remain are to put together my mid-point presentation. With the time I have left I hope to manage my time and have something good to present. | |
| **Now What?**  What can you do to address outstanding challenges?  With the time I have left until the mid-point submission I can work on my presentation and practice it so I can be confident delivering it. I can also continue working on any deliverables that will help to show the progress of my project. | |
| **Student Signature** | Aisha Ntuli |

**Supervision & Reflection Template**

|  |  |
| --- | --- |
| **Student Name** | Aisha Ntuli |
| **Student Number** | X21341006 |
| **Course** | BSc Hons Computing |
| **Supervisor** | Michael Bradford |

**Month:**

|  |  |
| --- | --- |
| **What**?  Reflect on what has happened in your project this month?  This month I secured a supervisor, Michael Bradford and had my first online meeting with him. We still haven’t met face to face yet which would be much better for discussion but hopefully post reading week our in-person meetings will commence without as much friction. Unfortunately, For the past little while I have been experiencing difficulty with my laptop, so I wasn’t able to do any work on my project including my monthly reflection journal. So, the research I have gotten to do hasn’t been as extensive as I would’ve hoped especially considering my free time during the reading week. However, I have gotten to read the papers I had mentioned in my proposal and watched some Youtube videos on setting up facial recognition based 2FA. Now that my laptop is up and running again, I hope to break ground on my project and I believe I am still on track to finishing my prototype for next month’s mid-point presentation. | |
| **So What?**  Consider what that meant for your project progress. What were your successes? What challenges still remain?  Obviously, it would’ve been ideal to have made a good amount of progress on my project during the break, but I still have plenty of time to get where I need to be and I think that being able to step back from my computer allowed me to focus on my goals and the tasks I have at hand to make my project a reality. So far, I have submitted my project proposal and ethics forms but the challenges I am facing now are to receive feedback on it from my lecturer so that I may discuss the fine tunings with my supervisor. | |
| **Now What?**  What can you do to address outstanding challenges?  To address the outstanding challenges, I am going to make a list of the goals I have. The submission of the Mid-point implementations, presentation slides and documentation are due at 11:59pm on December 13th which means from today Nov 3rd I have 40 days to prepare all of this. I am going to start by creating a GitHub repository to upload my code to where I will work on creating my prototype, making notes for my documentation, and creating my presentation slides. I will also be scheduling weekly meetings with my supervisor to help keep myself on track. | |
| **Student Signature** | Aisha Ntuli |