

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Real-time Deepfake Detection System for Video Streaming Platforms



Student Introduction

Project ID :F24PROJECT3AEBE

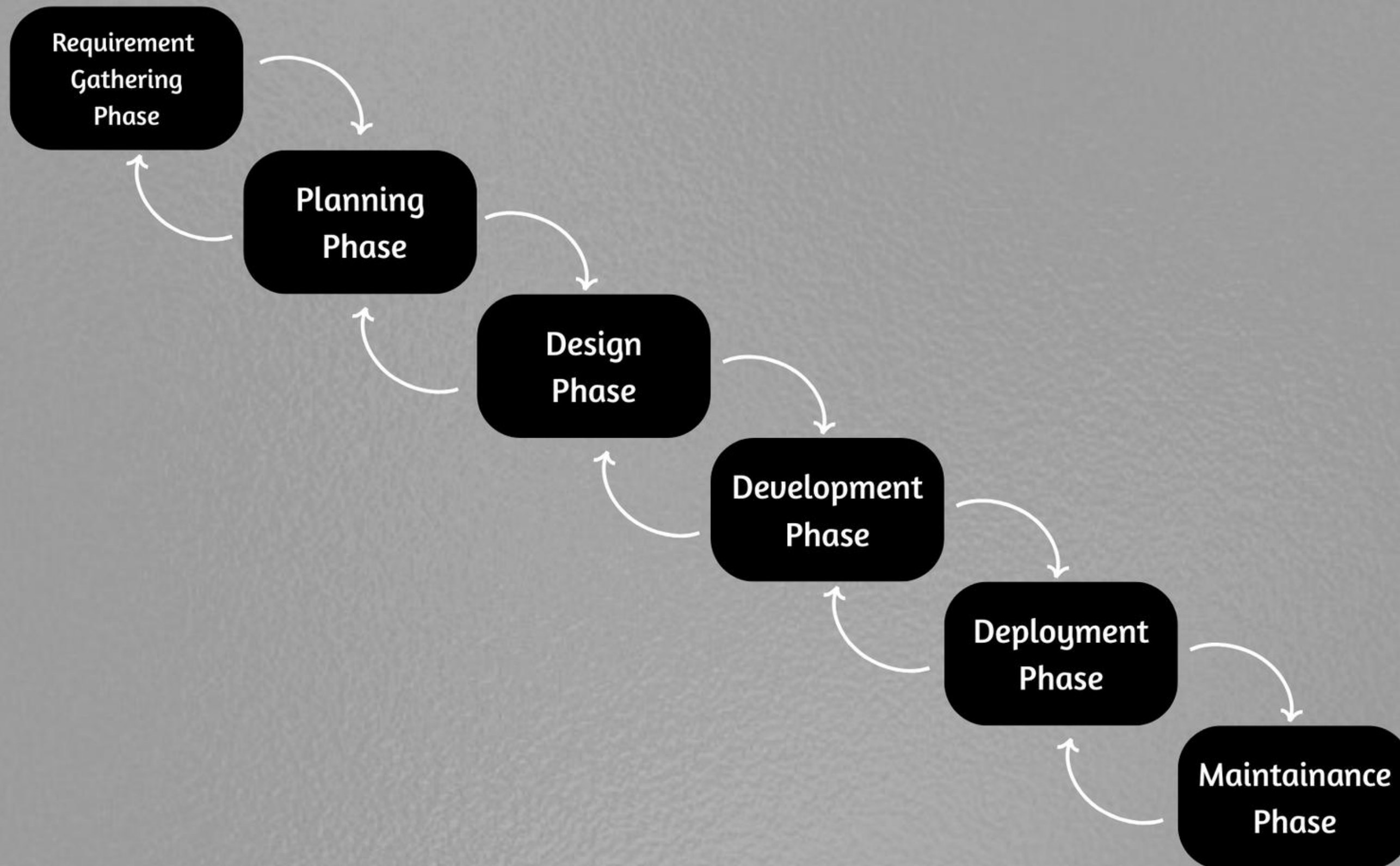
Student Name: Bisma Azeem

Student ID: BC220422952

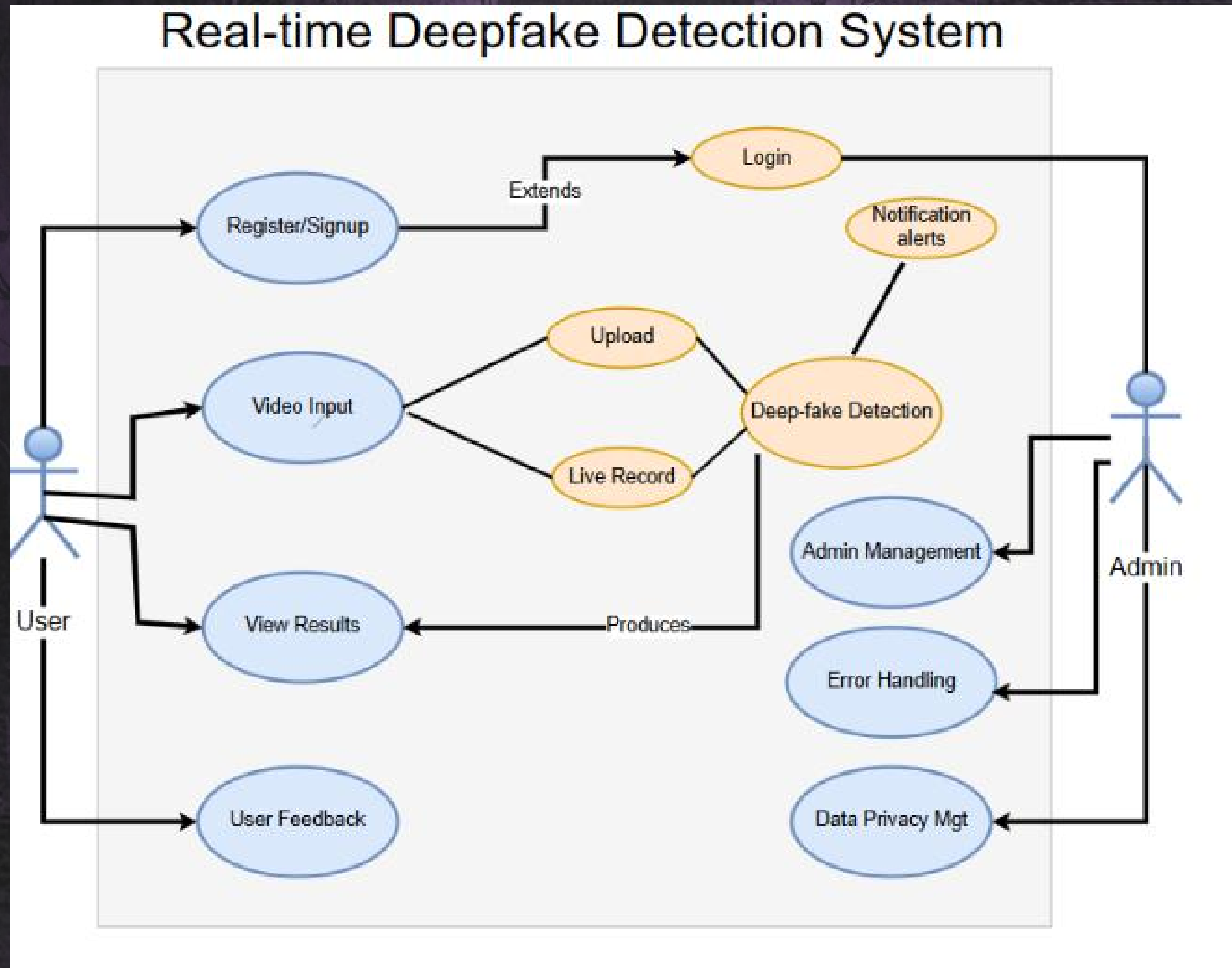
Project Introduction

The increasing sophistication of deep-fake technology has brought about a critical challenge in maintaining authenticity and trust in digital video communication. With the surge in video-based platforms—be it live streaming, online meetings, or uploaded content—there arises an urgent need for systems that can distinguish between genuine and manipulated media in real time. This project aims to develop an intelligent, real-time web-based system that proactively detects deep-fake content across various video platforms, empowering users to verify the authenticity of visual media with confidence.

Process Diagram



Use Case Diagram



Business Rules Catalog

1. User Authentication and Authorization:

- Users will be able to create accounts by providing necessary information.
- Authenticated users will be able to log in to the system using their credentials.
- Users can recover passwords via password recovery mechanism
- The system will implement role-based access control to restrict access to specific functionalities.
- The system will enforce strong password policies.
- Optional 2FA can be implemented for enhanced security.

2. Video Input and Processing:

- The system will support integration with live streaming and video conferencing platforms.
- The users can upload recorded videos in supported formats for analysis.
- The system will validate video file formats and sizes to prevent malicious uploads.
- The system will extract individual frames from input videos for analysis.

3. Deepfake detection:

- The system will utilize advanced deep learning models to process frames in real-time.
- The system will extract relevant features from video frames, such as facial landmarks, eye-movements, lip syncing or motion patterns.
- The system will classify the input video as either fake or real based on the extracted features.

Business Rules Catalog

4. Visualizations and Alerts:

- The system will also display the detected frames along with a confidence score for each classification.
- The system, in real-time, will notify the users and administrators via alerts when a deep-fake content is detected.
- For uploaded videos, the system will provide a detailed report with visualizations of detected deep-fake segments.

5. User Feedback:

- Users can give feedback on the accuracy of the system's detection.
- User feedback will be used to improve the performance of the system.

6. Error Handling:

- The system will gracefully handle errors, such as invalid video input, model loading failures, processing delays and network issues.
- The error messages will be informative and user-friendly.

7. User Privacy and Data Handling:

- The system will process video data locally.
- The system will ensure end-to-end encryption to maintain user privacy.
- The system will obtain explicit user consent before processing and storing any video data.

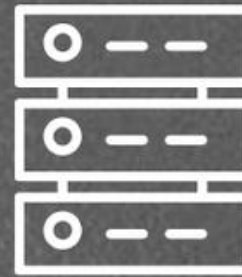
Architecture Diagram

Presentation Layer



- UI Components
- Authorization
- WebRTC Integration

Application Layer



- Authorization
- Data Processing
- Deepfake Detection

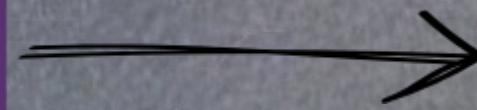
Data Layer



- NoSQL Database
- Encryption

Team Structure

**Ma'am
Sonia
Salman**



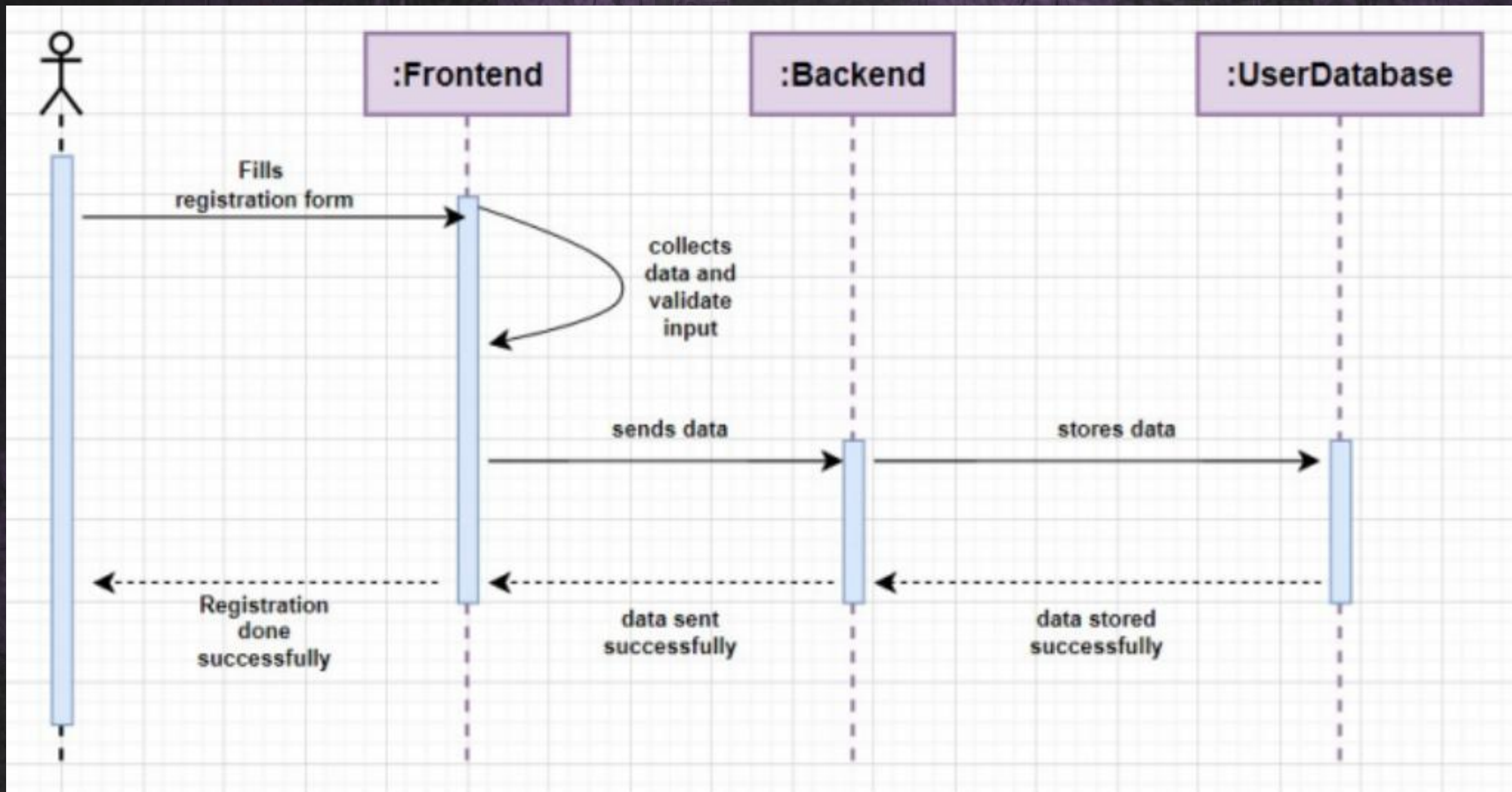
**Bisma
Azeem**

Project Schedule

WBS NUMBER	TASK TITLE	START DATE	DUE DATE	DURATION	November					December					January					February					March					April					May				
					W1	W2	W3	W4	W5	W1	W2	W3	W4	W5	W1	W2	W3	W4	W5	W1	W2	W3	W4	W5	W1	W2	W3	W4	W5	W1	W2	W3	W4	W5					
1	SRS Document	11/12/2024	12/8/2024	26																																			
1.1	Scope	11/12/2024	11/12/2024	0																																			
1.2	Functional Requirements	11/13/2024	11/14/2024	1																																			
1.3	Non Functional Requirements	11/15/2024	11/15/2024	0																																			
1.4	Usecase Diagram	11/16/2024	11/18/2024	2																																			
1.5	Usage Scenarios	11/19/2024	11/24/2024	5																																			
1.6	Adopted Methodology	11/25/2024	11/30/2024	5																																			
1.7	Work Plan	12/1/2024	12/3/2024	2																																			
2	Design Document	12/9/2024	3/3/2025	84																																			
2.1	Introduction	12/21/2024	12/24/2024	3																																			
2.2	ERD	12/25/2024	12/31/2024	6																																			
2.3	Sequence Diagram	1/1/2025	1/11/2025	10																																			
2.4	Architecture Design Diagram	1/12/2025	1/22/2025	10																																			
2.5	Class Diagram	1/23/2025	1/31/2025	8																																			
2.6	Database Diagram	2/1/2025	2/6/2025	5																																			
2.7	Interface Diagram	2/7/2025	2/19/2025	12																																			
2.8	Test Cases	2/20/2025	2/28/2025	8																																			
3	Prototype	3/4/2025	3/17/2025	13																																			
3.1	Problem Statement	3/4/2025	3/5/2025	1																																			
3.2	Design	3/6/2025	3/8/2025	2																																			
3.3	Development	3/9/2025	3/15/2025	6																																			
3.4	Final Prototype	3/16/2025	3/17/2025	1																																			
4	Final	3/18/2025	5/9/2025	51																																			
4.1	Model Design	3/18/2025	3/23/2025	5																																			
4.2	Web App Layout	3/24/2025	3/27/2025	3																																			
4.3	Web App Development	3/28/2025	3/31/2025	3																																			
4.4	Coding	4/1/2025	4/15/2025	14																																			
4.5	Testing	4/16/2025	4/23/2025	7																																			
4.6	Final Development	4/24/2025	4/30/2025	6																																			
4.7	Final Report	5/1/2025	5/9/2025	8																																			

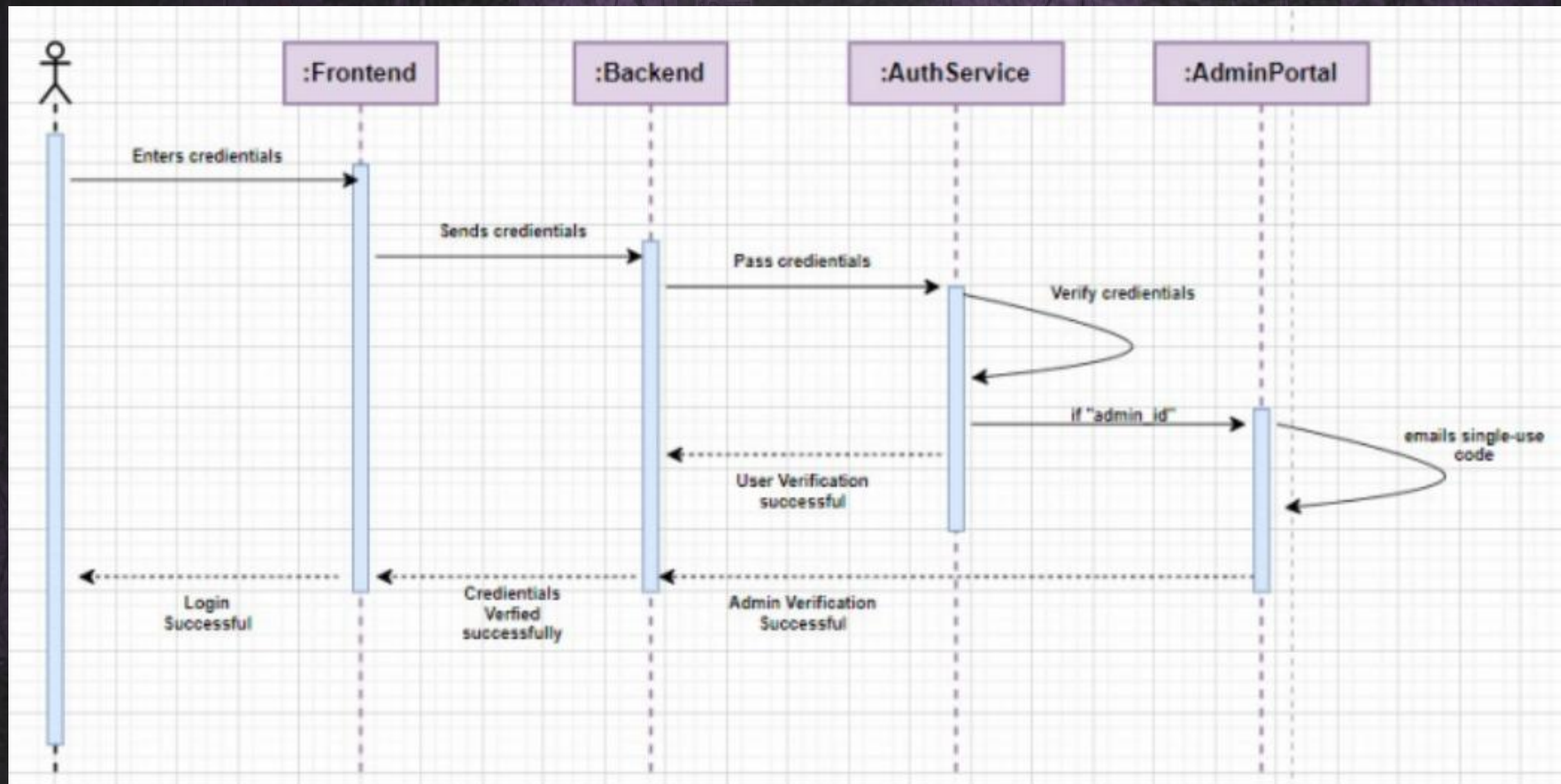
Sequence Diagrams

Register:



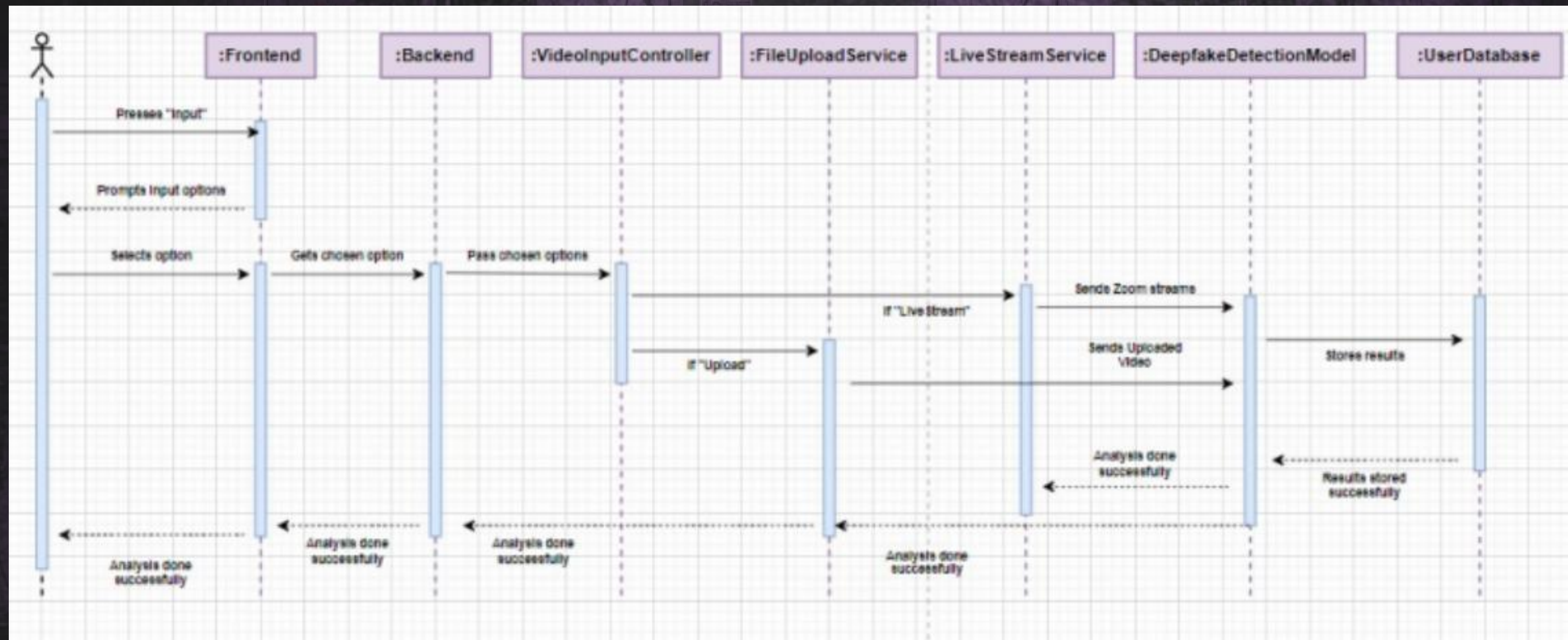
Sequence Diagrams

Login:



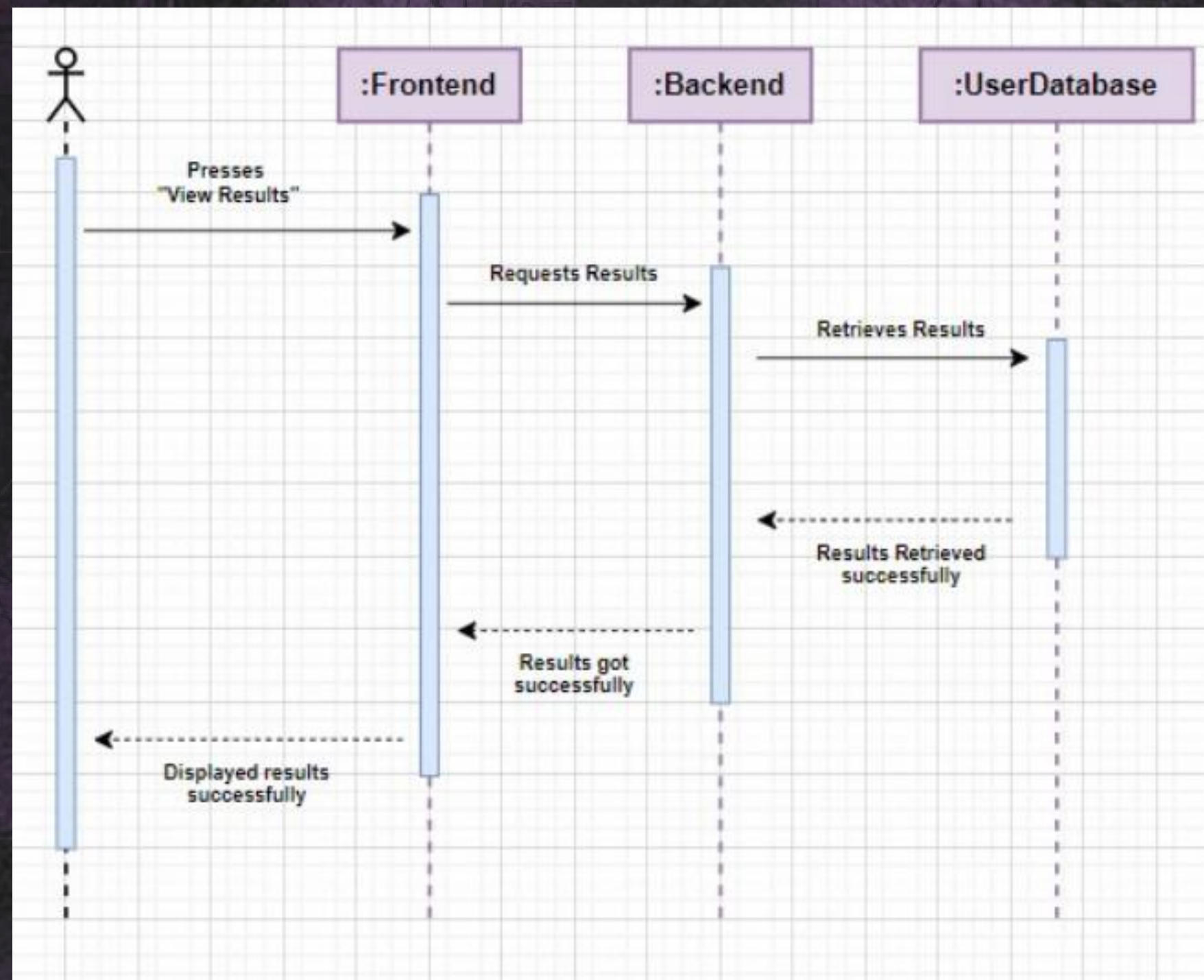
Sequence Diagrams

Video Input and Processing:



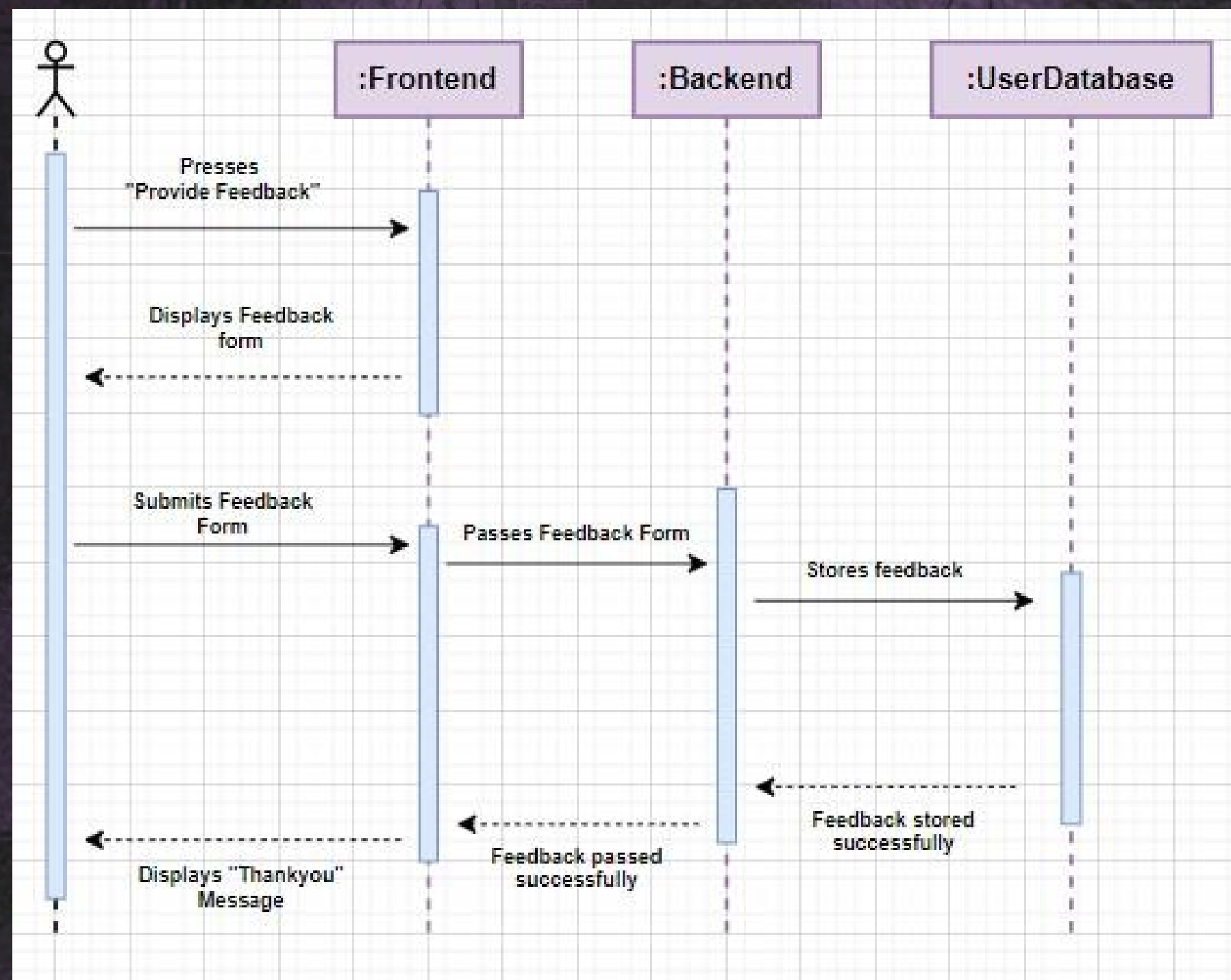
Sequence Diagrams

View Results:



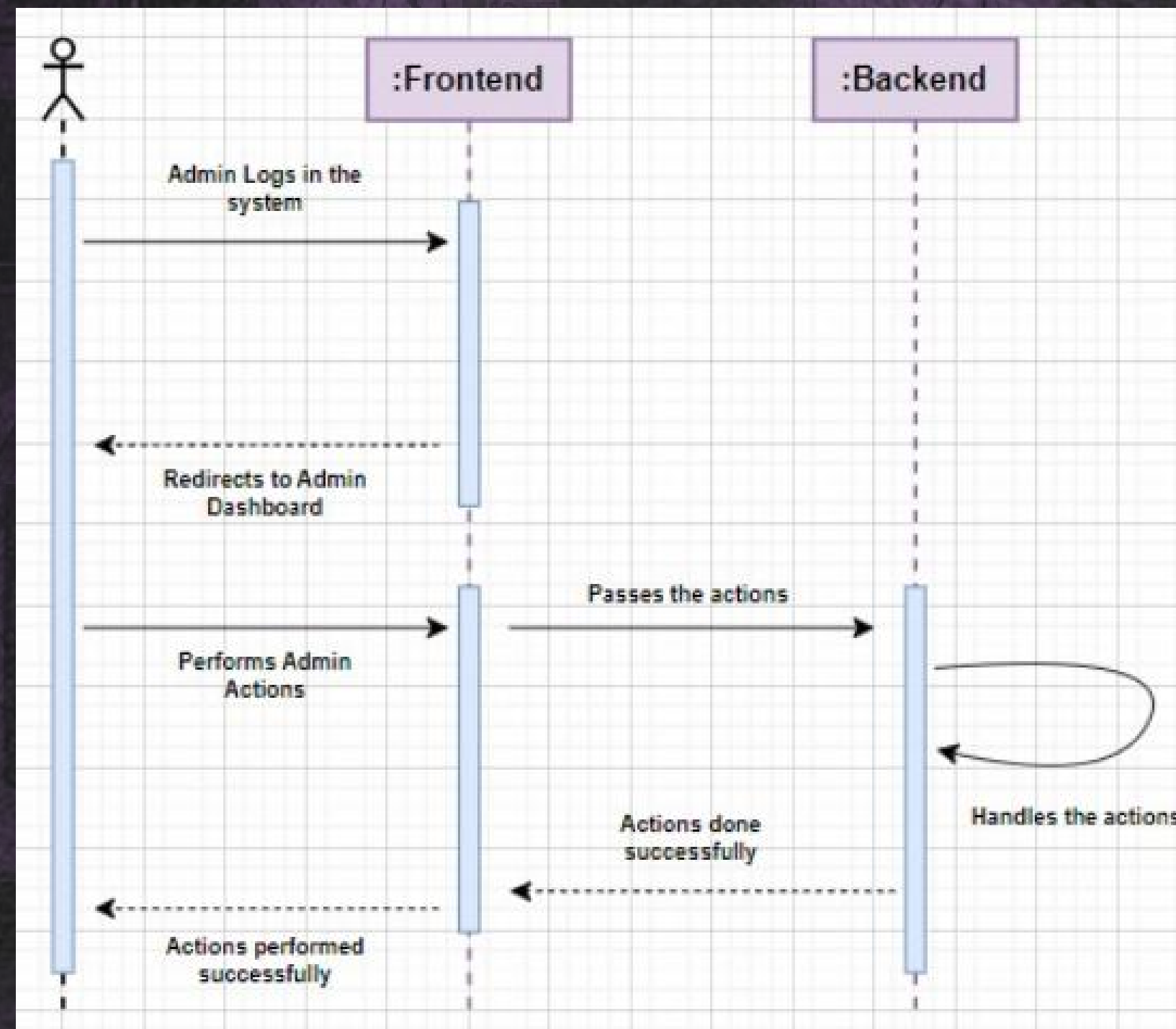
Sequence Diagrams

User Feedback:



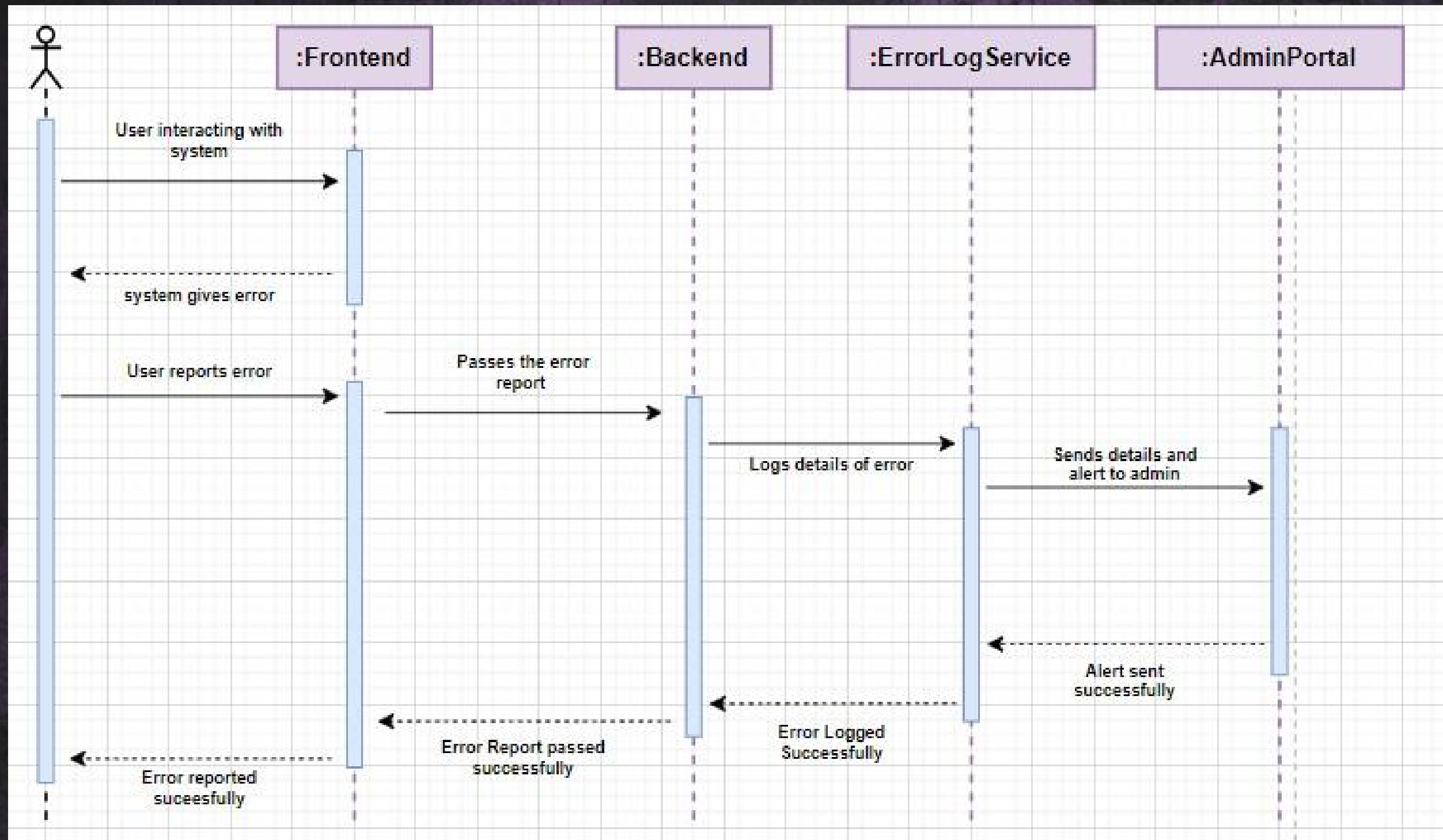
Sequence Diagrams

Admin Management:



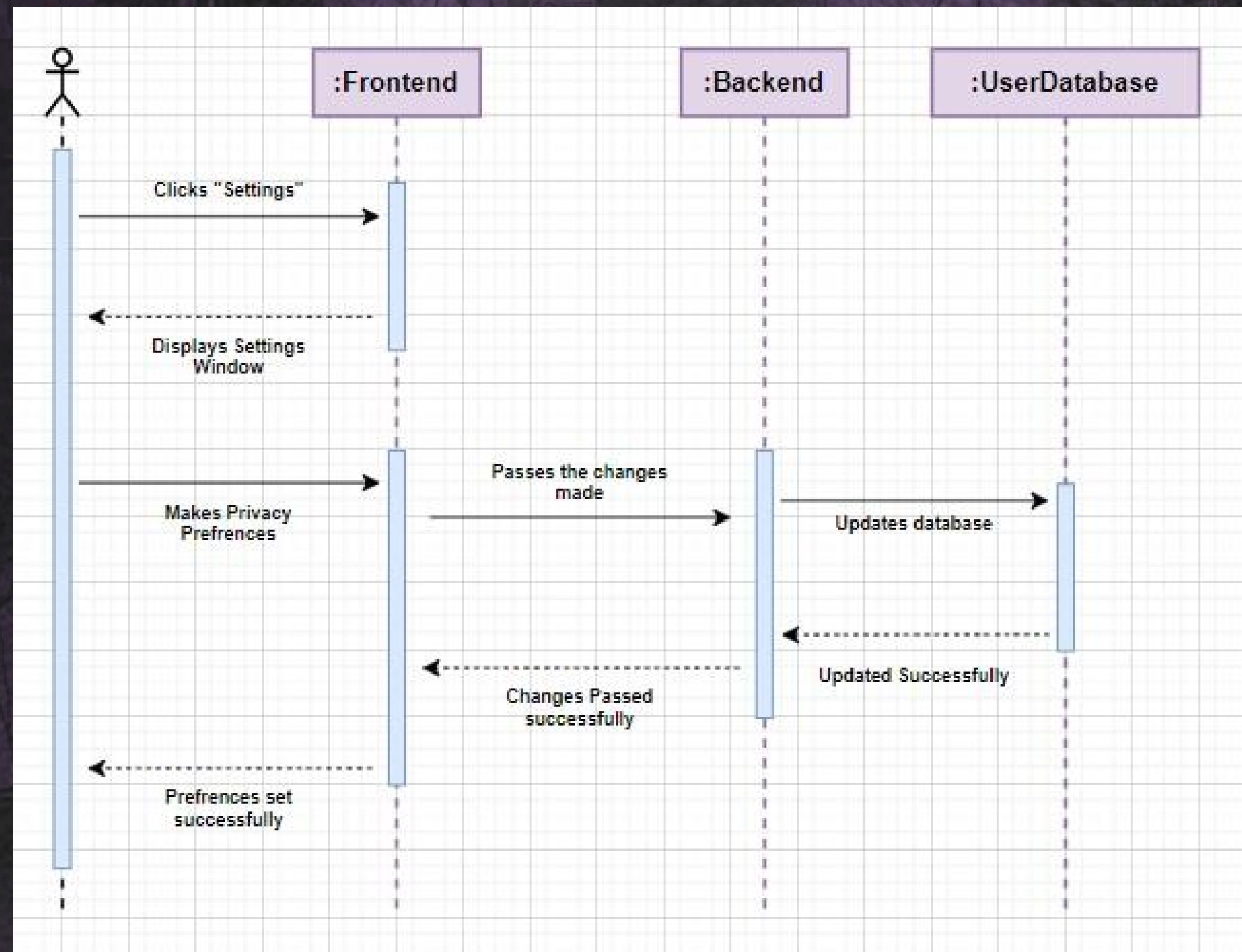
Sequence Diagrams

Error Handling:

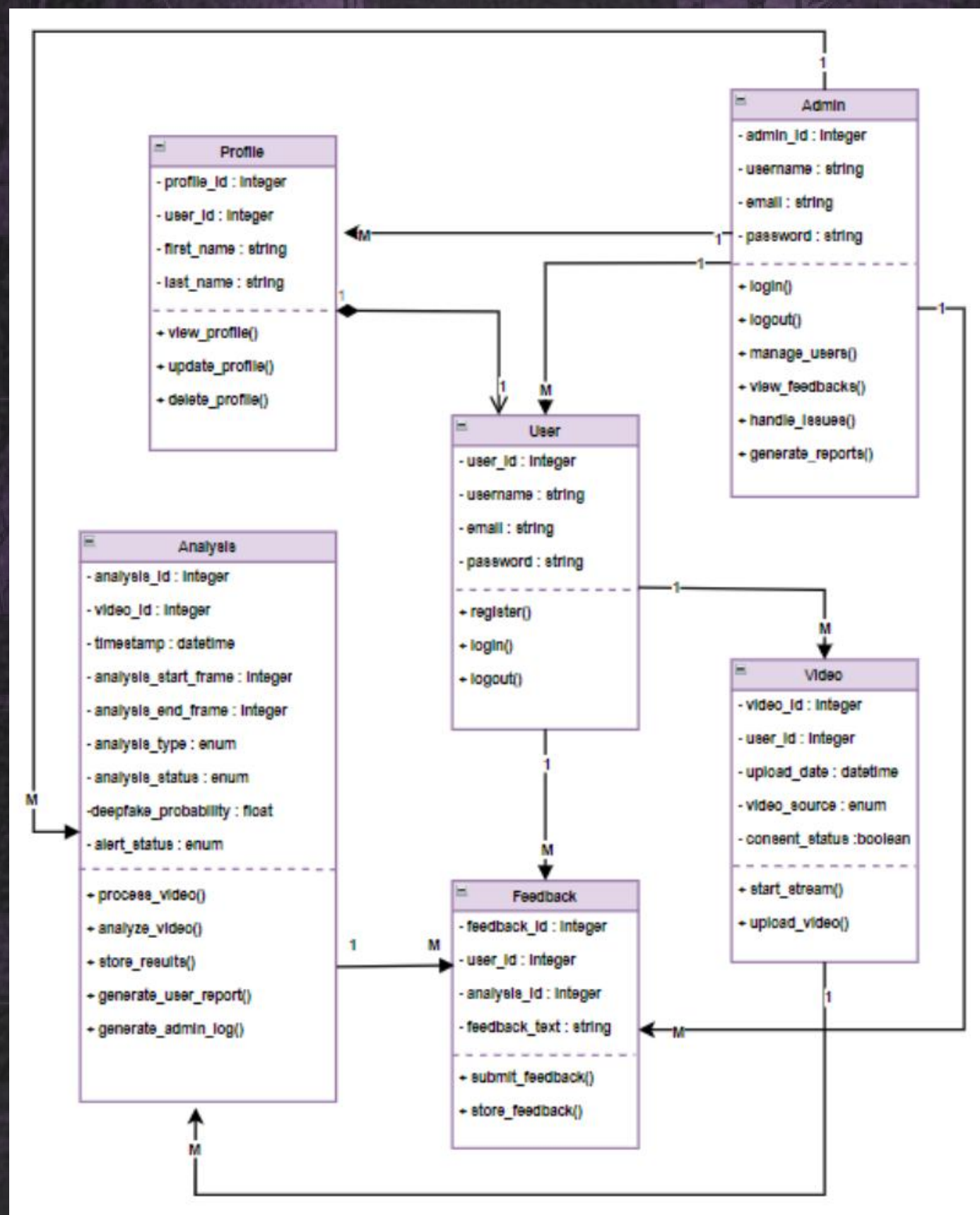


Sequence Diagrams

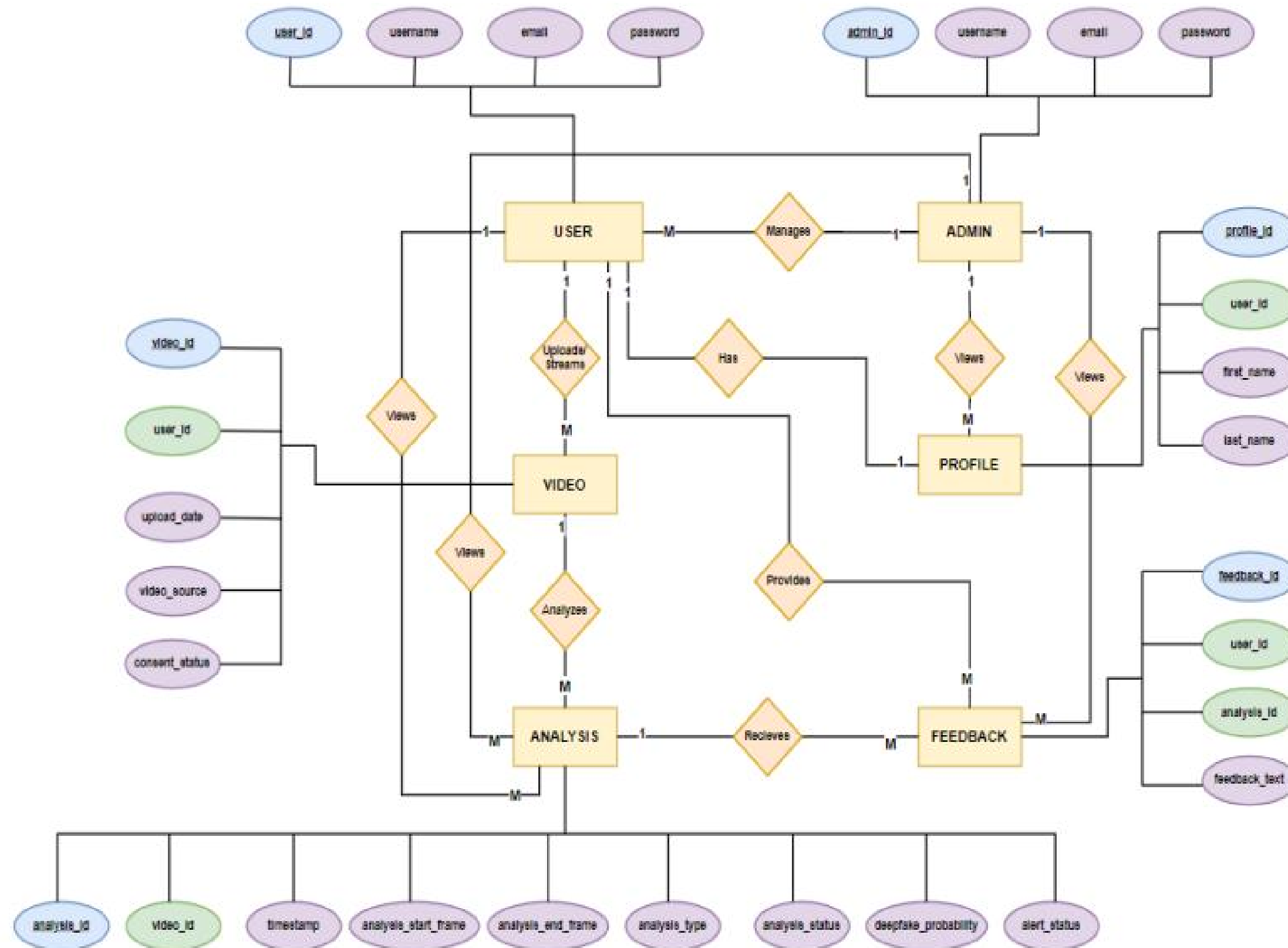
Data Privacy Management:



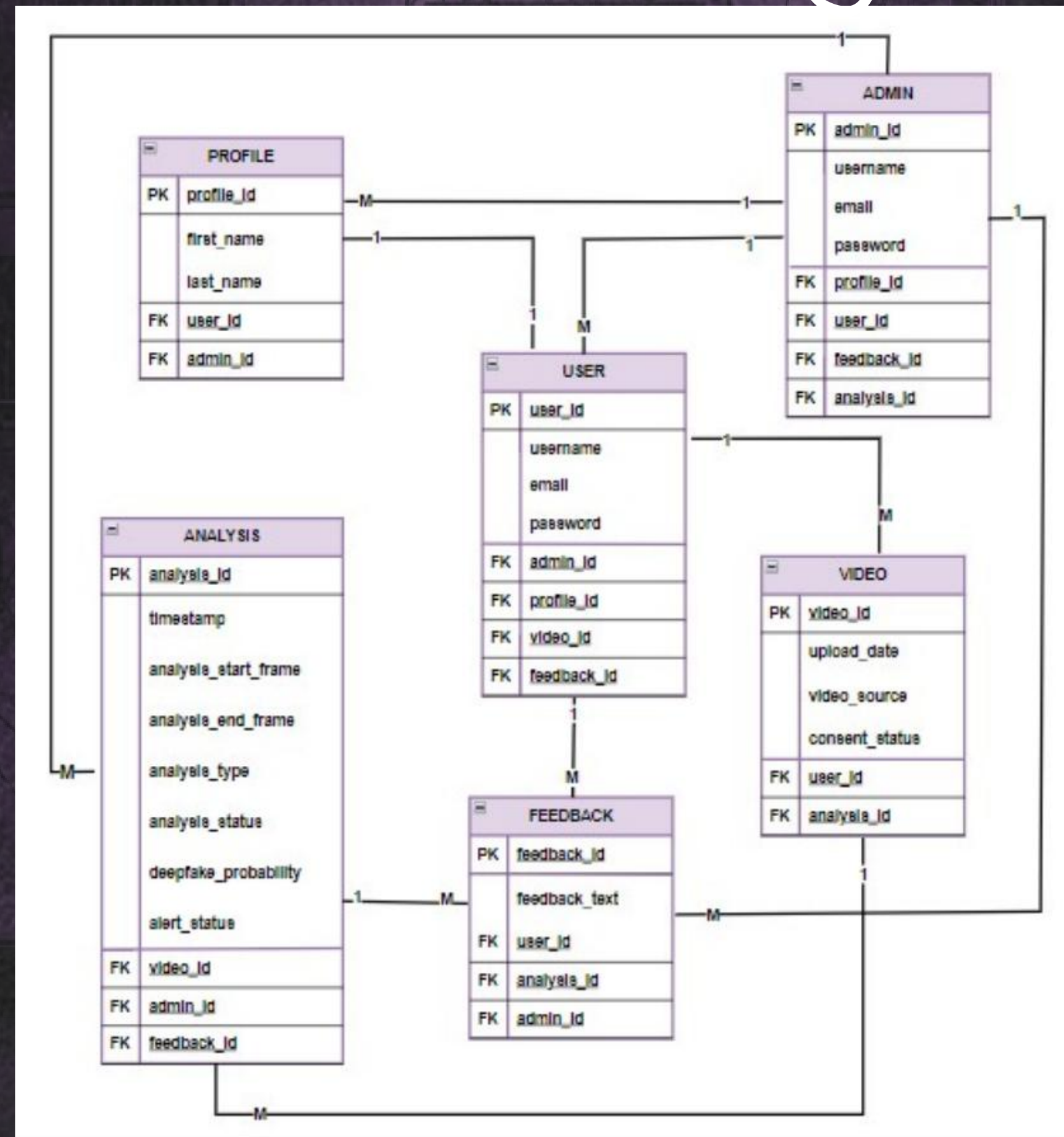
Class Diagram



Entity Relationship Diagram



Database Diagram



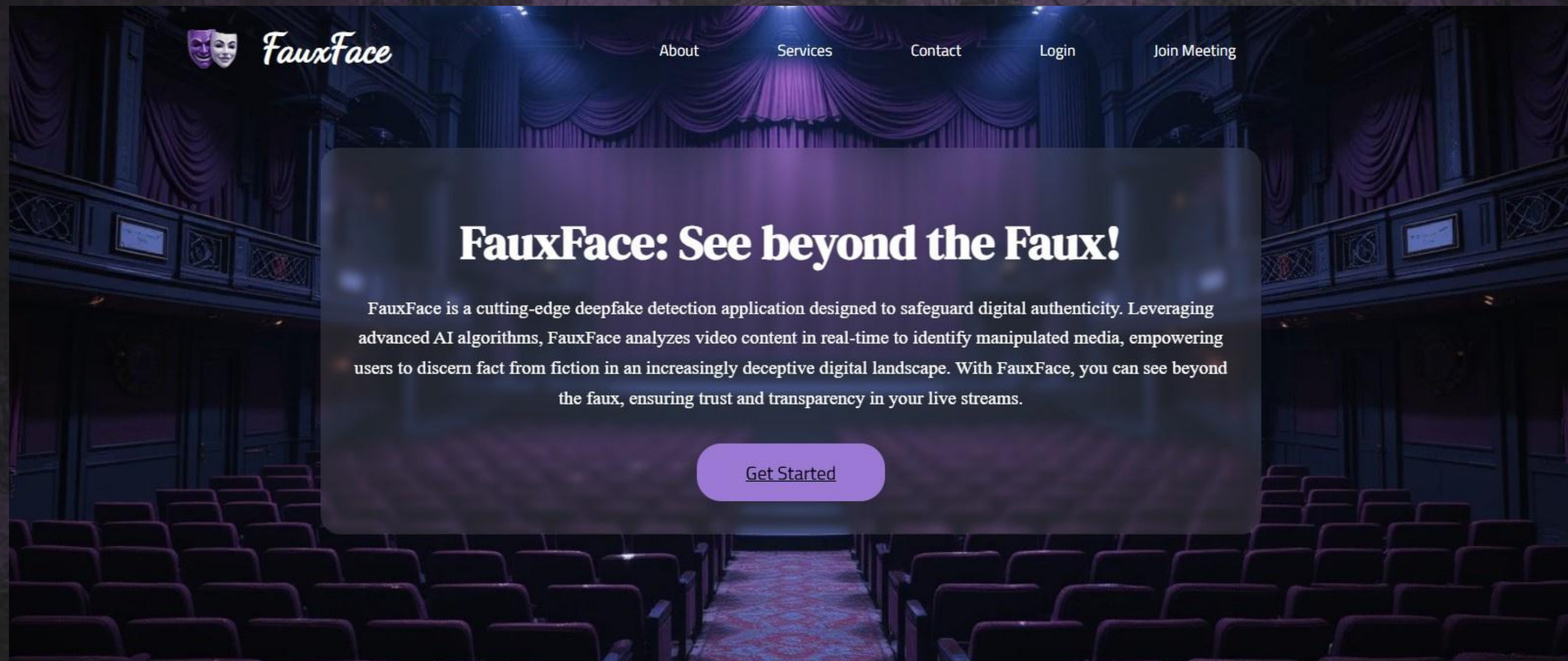
User Interface:

WebApp Logo:



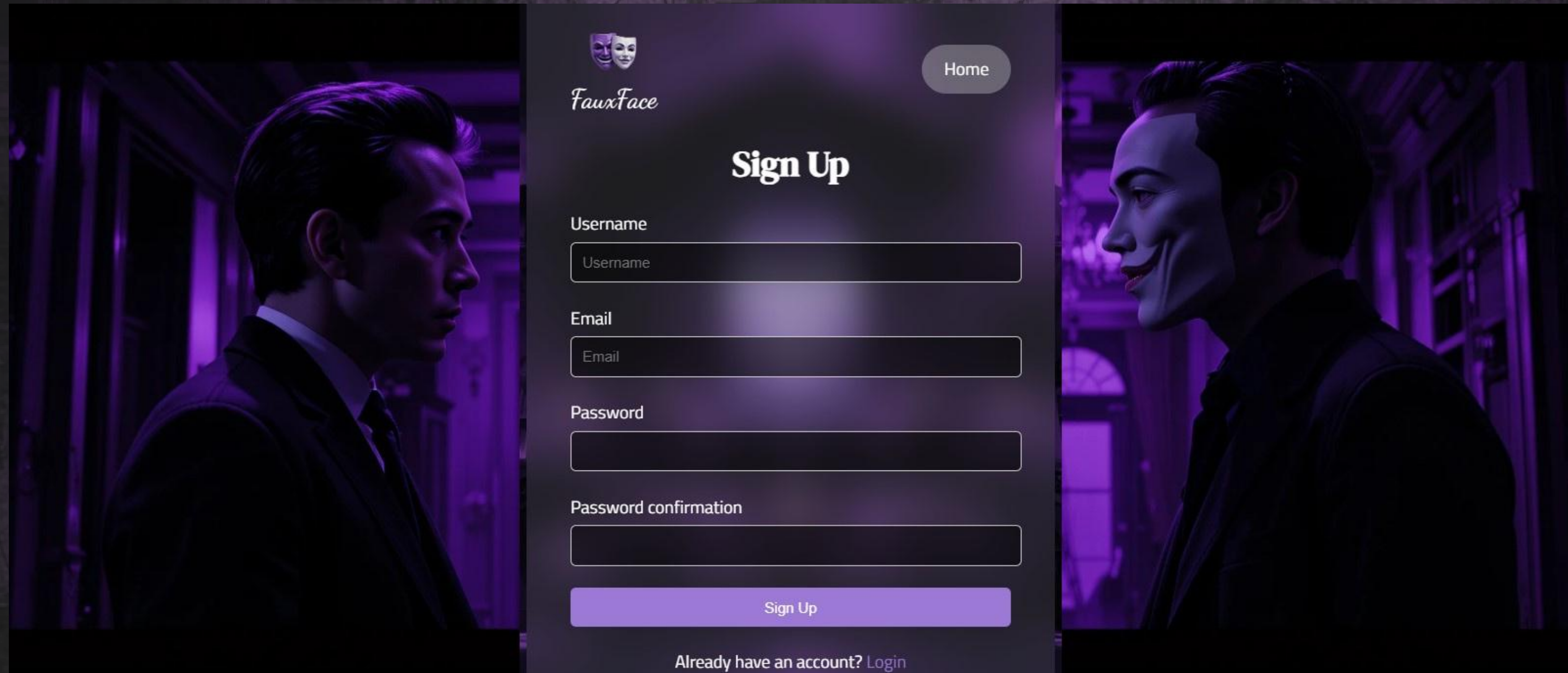
User Interface:

Homepage:




User Interface:

Signup:



The image shows a user interface mockup for a website called "FauxFace". The background is a dark, moody image of a man in a suit, with a white mask covering his face. The interface is centered and features a "Sign Up" form. At the top left is the "FauxFace" logo, which consists of two stylized masks. At the top right is a "Home" button. The form has four input fields: "Username", "Email", "Password", and "Password confirmation". Below the form is a "Sign Up" button. At the bottom, there is a link that says "Already have an account? Login".

 Home

Sign Up

Username

Email

Password

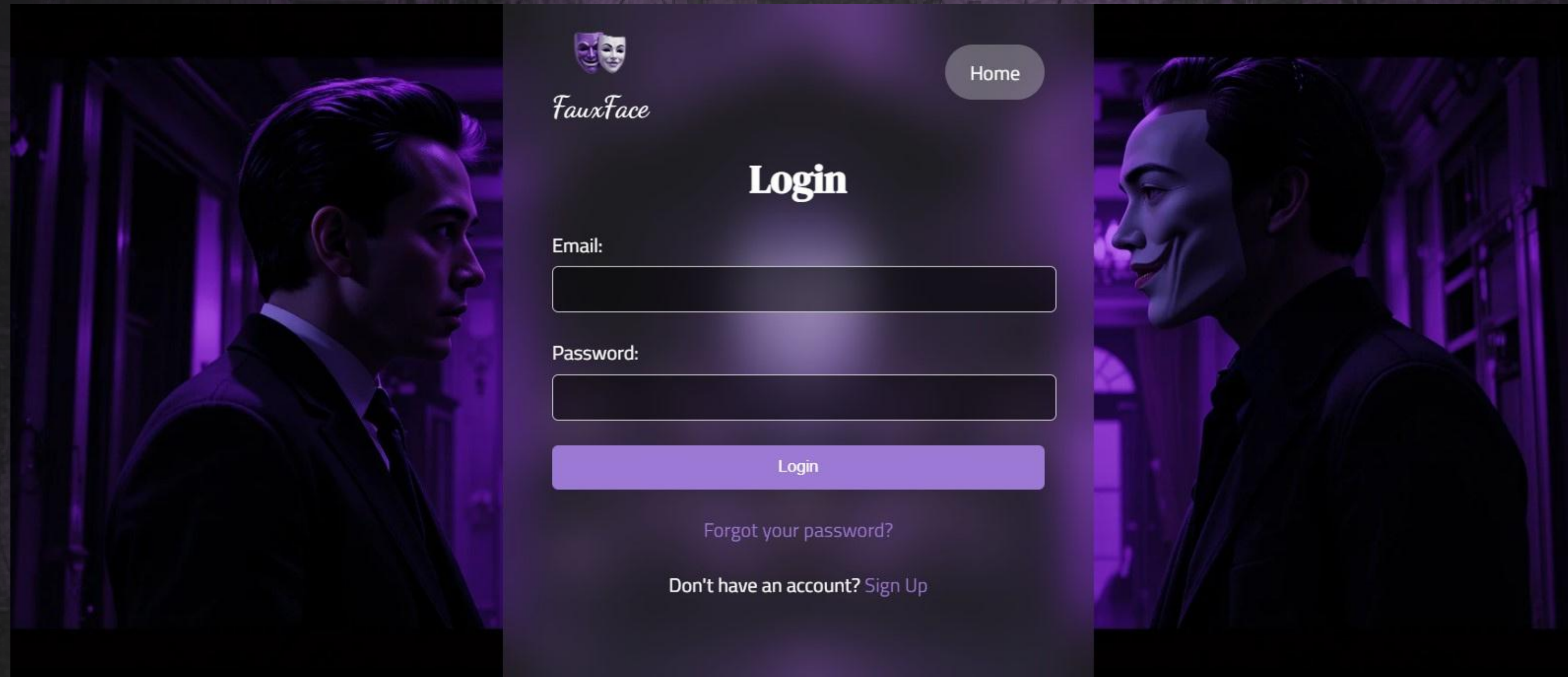
Password confirmation

[Sign Up](#)


Already have an account? [Login](#)

User Interface:

Login:



The image shows a user interface mockup for a login page. The background is a dark, moody image of a man in a suit, split into two panels. The central panel is a dark gray rectangle containing the login form. At the top left of this panel is a logo consisting of two masks and the text 'FauxFace'. At the top right is a 'Home' button. The main heading 'Login' is centered. Below it are two input fields: 'Email:' and 'Password:'. A 'Login' button is centered below the password field. At the bottom, there are two links: 'Forgot your password?' and 'Don't have an account? Sign Up'.

[Home](#)

Login

Email:

Password:



Login

[Forgot your password?](#)

Don't have an account? [Sign Up](#)

User Interface:

Dashboard:

Welcome back, **bisma_azeem!**

Dashboard

Profile

Settings

Contact

Logout

Start Live Stream

Real-Time Deepfake Detection

Our advanced detection system analyzes WebRTC video streams in real-time, providing instant feedback on potential deepfake content during your video calls.

- Browser-based WebRTC implementation
- Real-time frame-by-frame analysis
- Instant visual indicators for suspicious content
- Continuous monitoring throughout your call
- Secure peer-to-peer connections
- No plugins or downloads required

Upload Video

Video Analysis

Upload pre-recorded videos for comprehensive deepfake analysis. Our system examines each frame using advanced AI models to detect manipulation with high accuracy.

- Supports MP4 format
- Detailed frame-by-frame analysis
- Comprehensive authenticity report
- Visual indicators of manipulated areas
- Downloadable video results

User Interface:

Profile:



bisma_azeem

lofikofi13@gmail.com

Member Since: May 2025

Last Login: May 07, 2025 20:31


Account Status: Active

[Edit Profile](#)

[Back to Dashboard](#)

User Interface:

Account Settings:



Account Settings

Username

Email

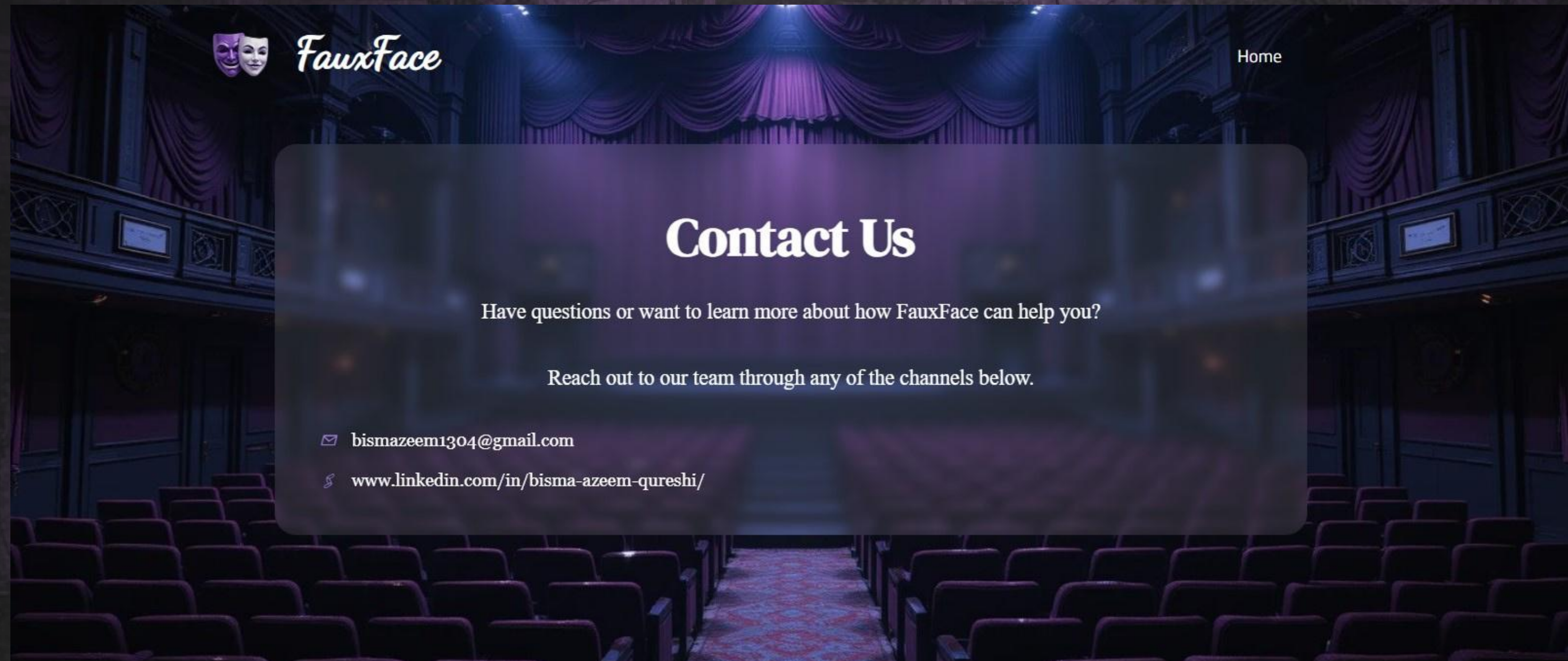
New Password (leave blank to keep current)

Profile Picture
 No file chosen

☒ I consent to store my video input data for improvement purposes

User Interface:

Contact Us:



User Interface:

Logout:



Logout Confirmation

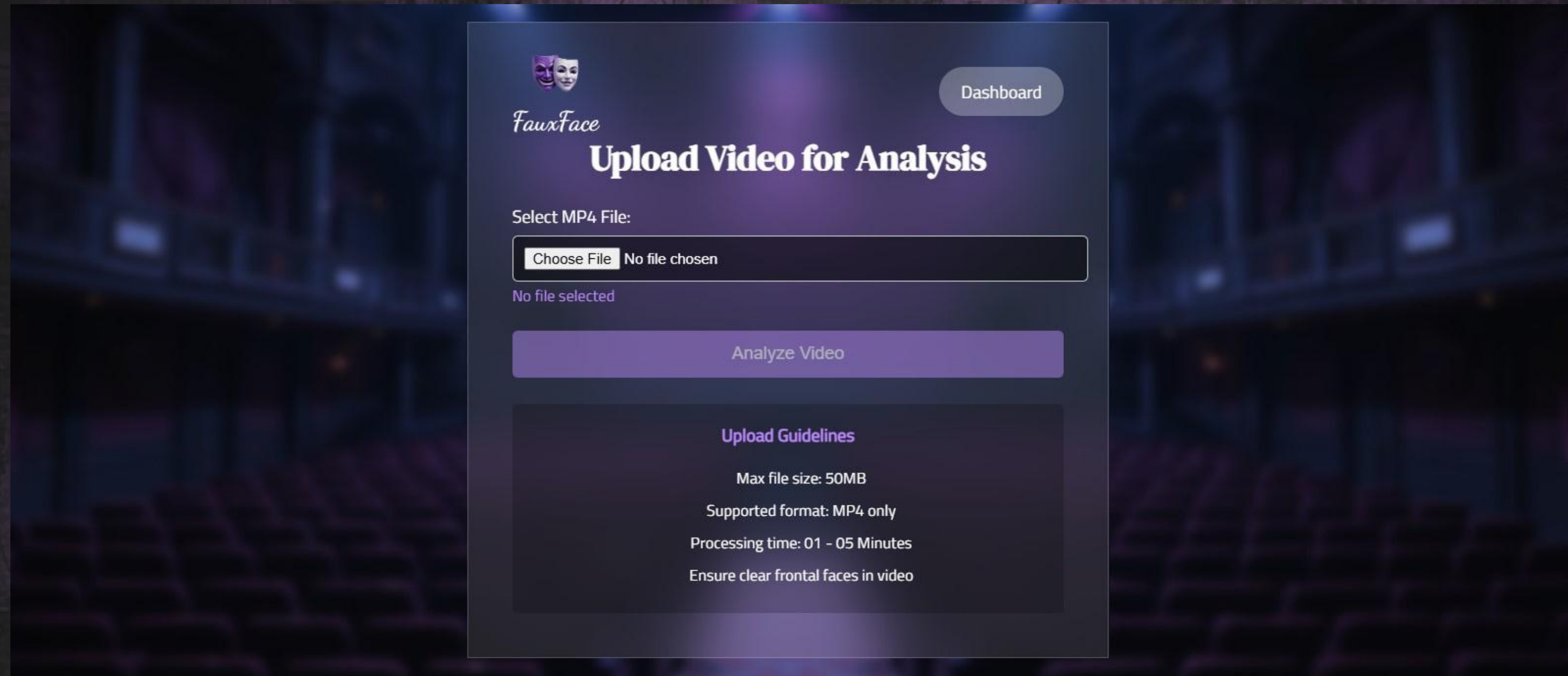
Are you sure you want to logout from your FauxFace account?

Yes, Logout


Cancel

User Interface:

Upload Video:



The screenshot displays the 'FauxFace' web application interface for video upload. At the top left is the 'FauxFace' logo, featuring two stylized masks. To the right is a 'Dashboard' button. The main heading is 'Upload Video for Analysis'. Below this, a section titled 'Select MP4 File:' contains a file selection button labeled 'Choose File' and the text 'No file chosen'. Below the button is the text 'No file selected'. A large blue button labeled 'Analyze Video' is positioned below the file selection area. At the bottom, a section titled 'Upload Guidelines' lists the following rules: 'Max file size: 50MB', 'Supported format: MP4 only', 'Processing time: 01 - 05 Minutes', and 'Ensure clear frontal faces in video'.

 [Dashboard](#)

Upload Video for Analysis

Select MP4 File:

[Choose File](#) No file chosen

No file selected

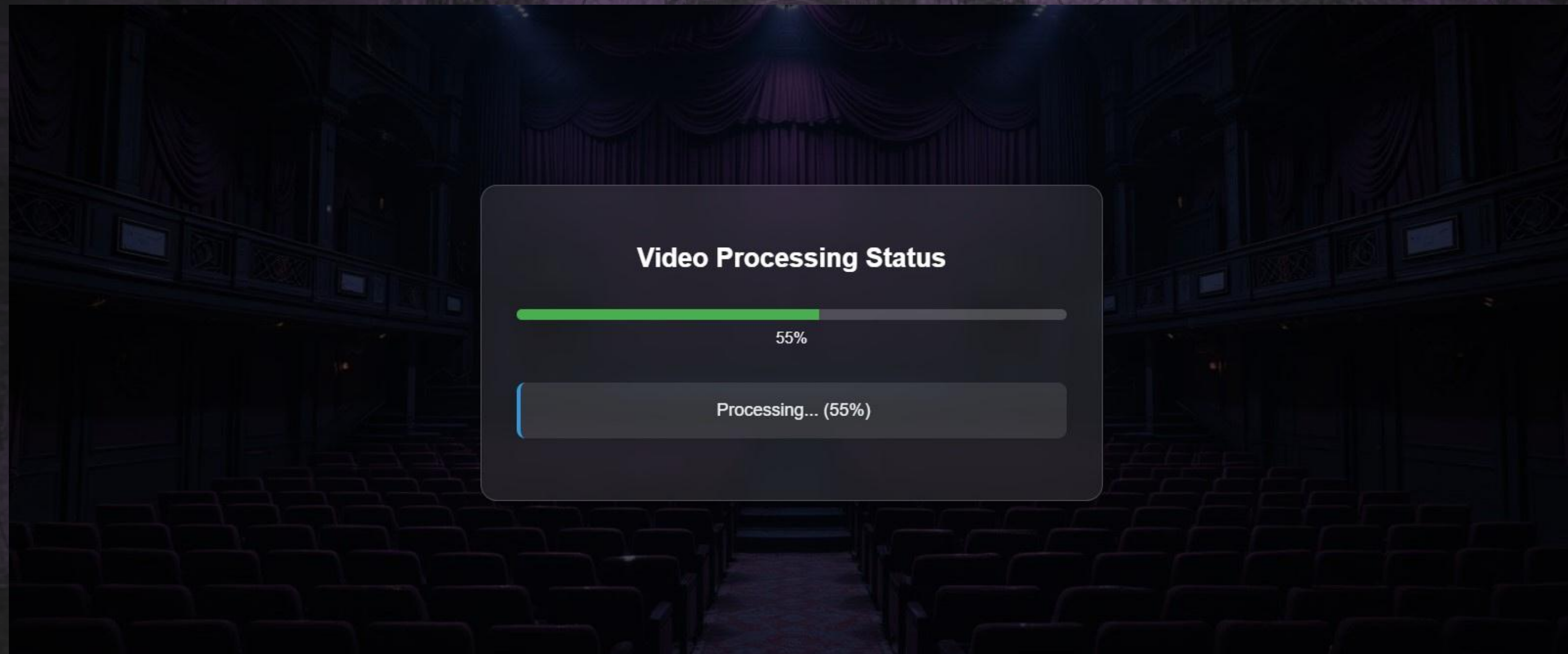
[Analyze Video](#)

Upload Guidelines

- Max file size: 50MB
- Supported format: MP4 only
- Processing time: 01 - 05 Minutes
- Ensure clear frontal faces in video

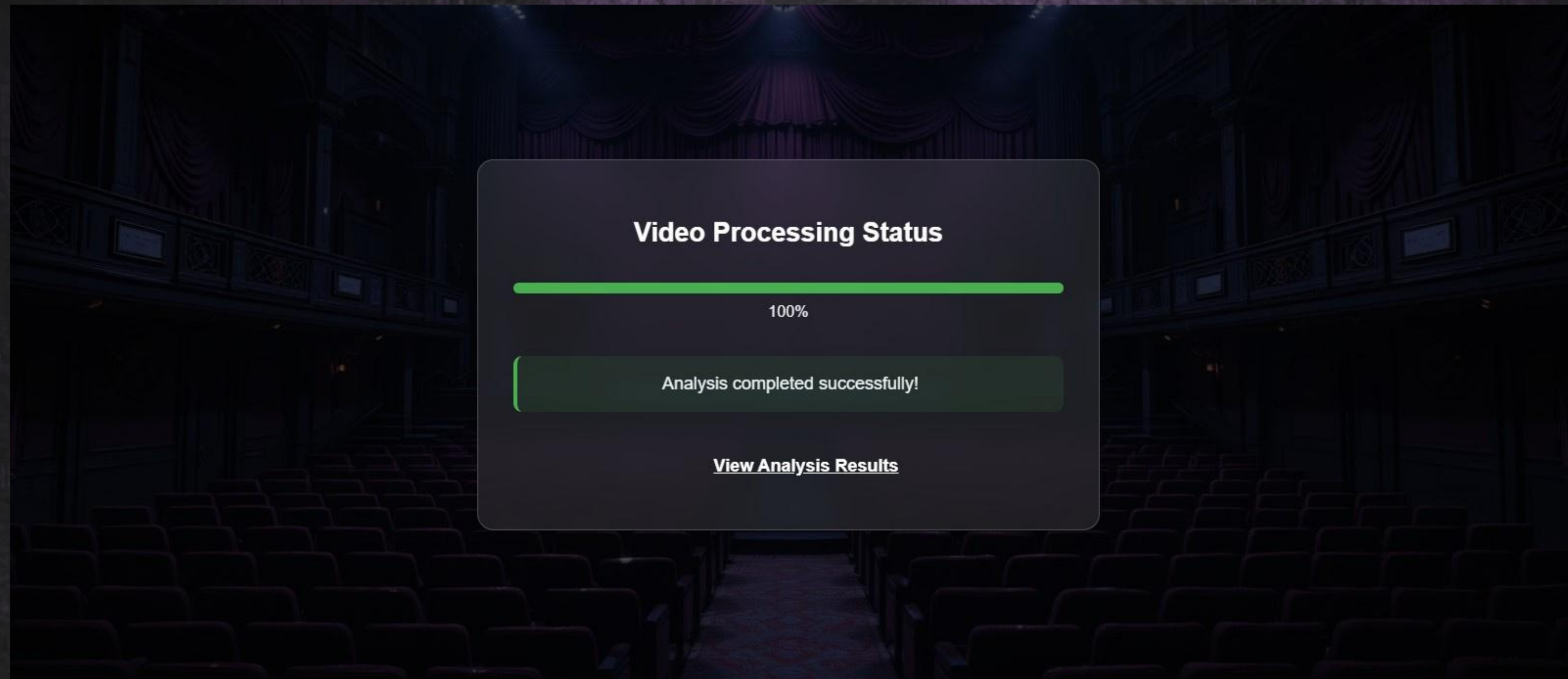
User Interface:

Video Processing Status:



User Interface:

Video Processing Complete:



User Interface:

Video Analysis Report:

Video Analysis Report

Completed

FAKE

Confidence Score of Fakeness: 0.79%

Download Video

Back to Dashboard

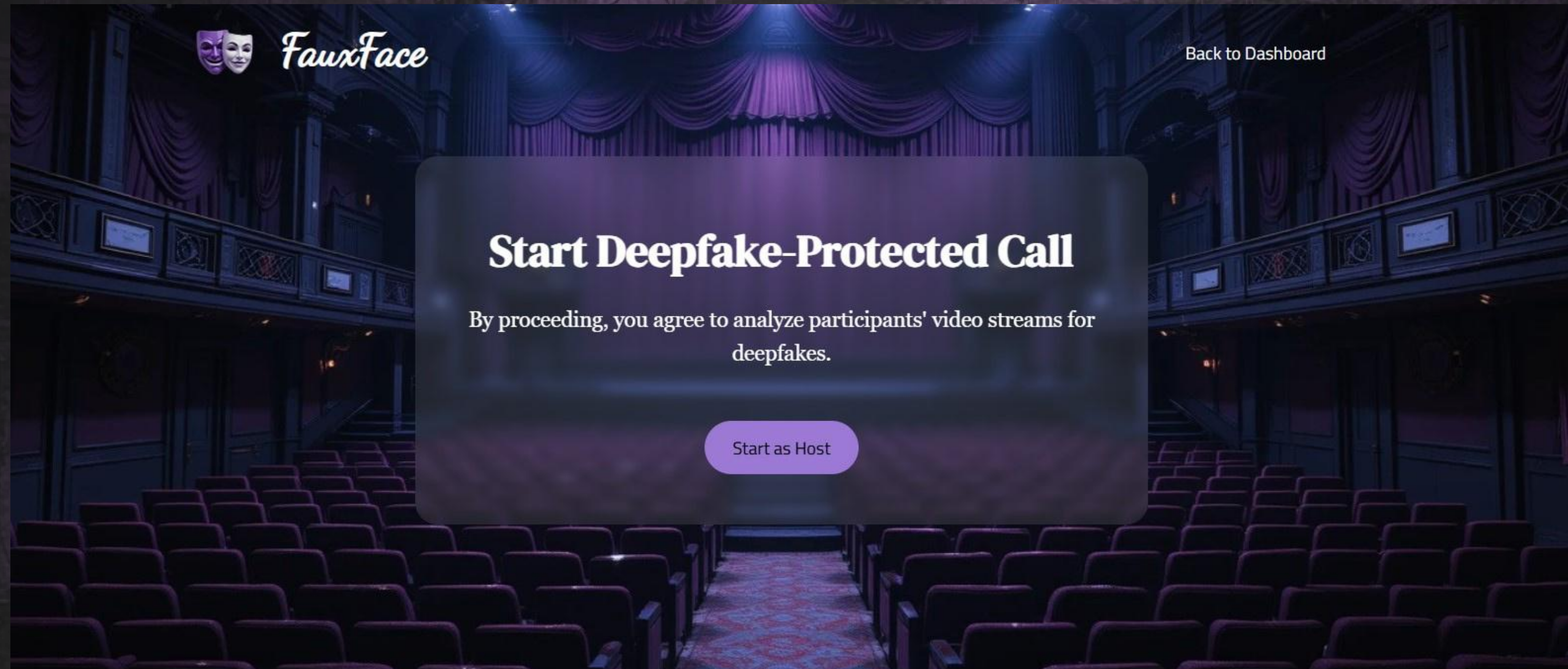
User Interface:

A Frame from Processed Video:



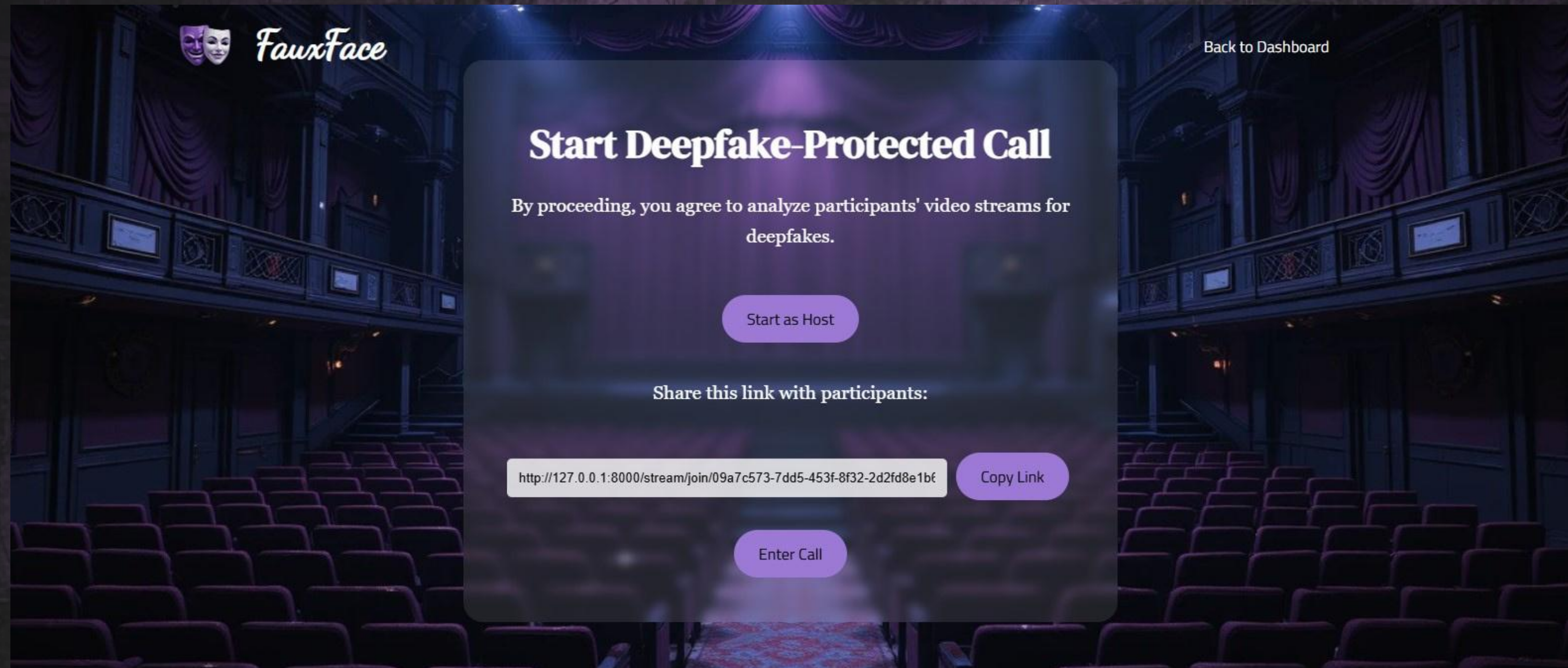
User Interface:

Host Consent Page:



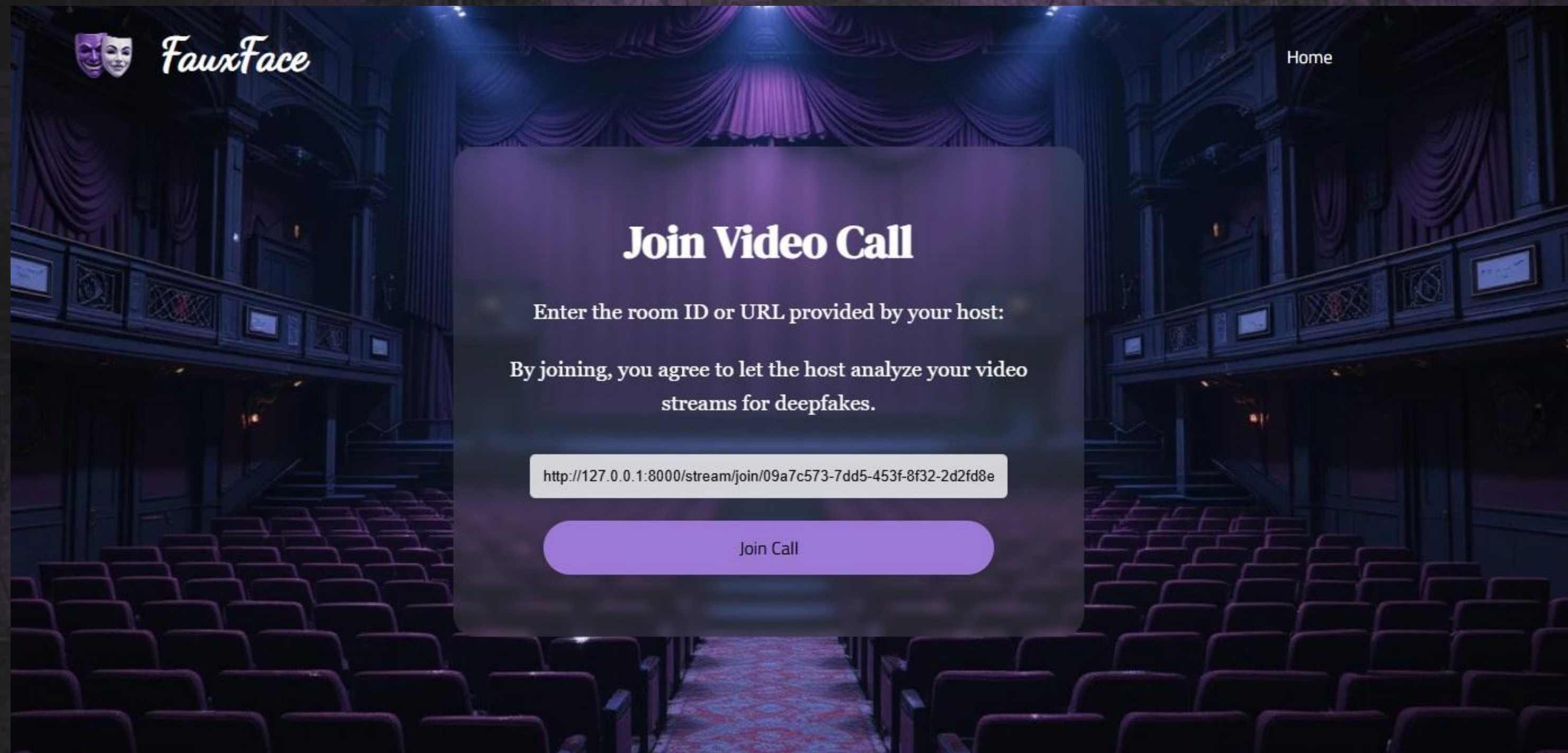
User Interface:

Host link for the Participant:



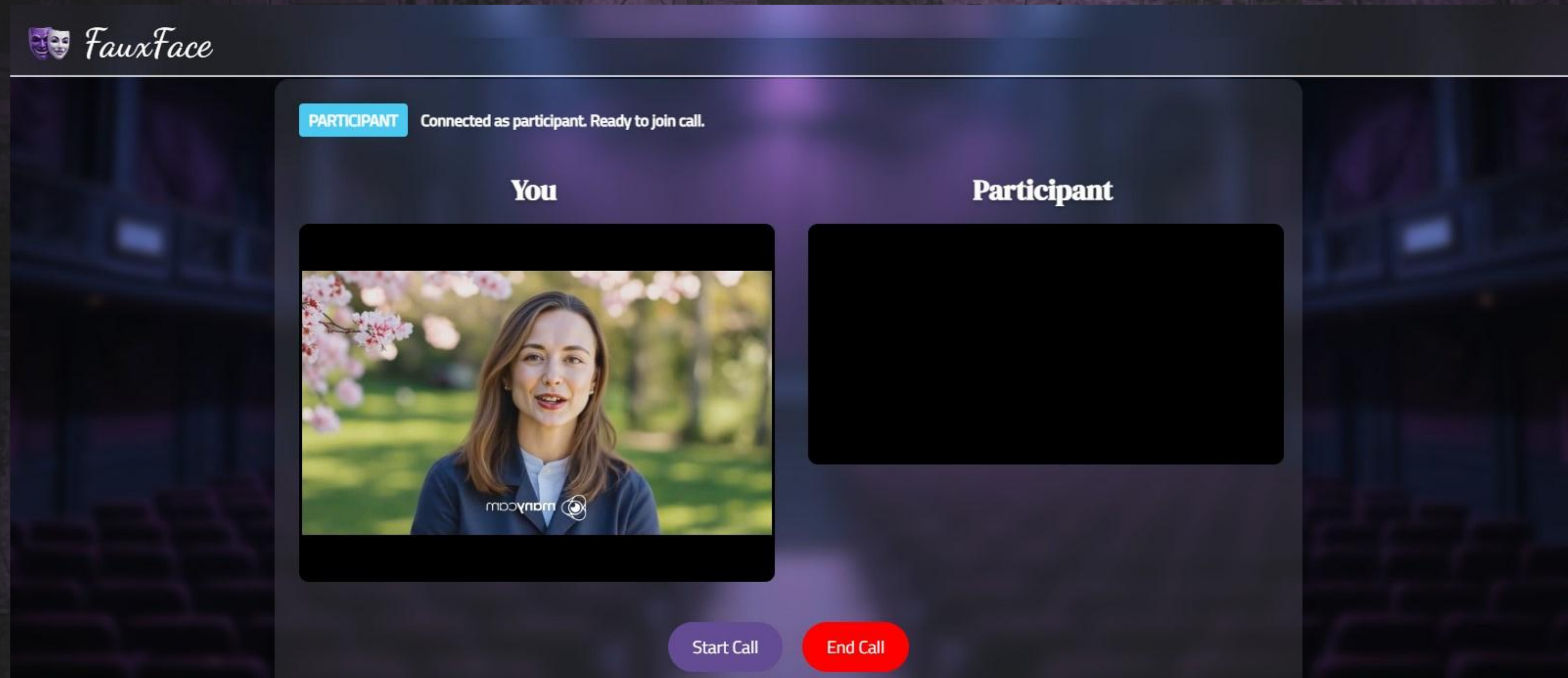
User Interface:

Participant Consent and Join Call:



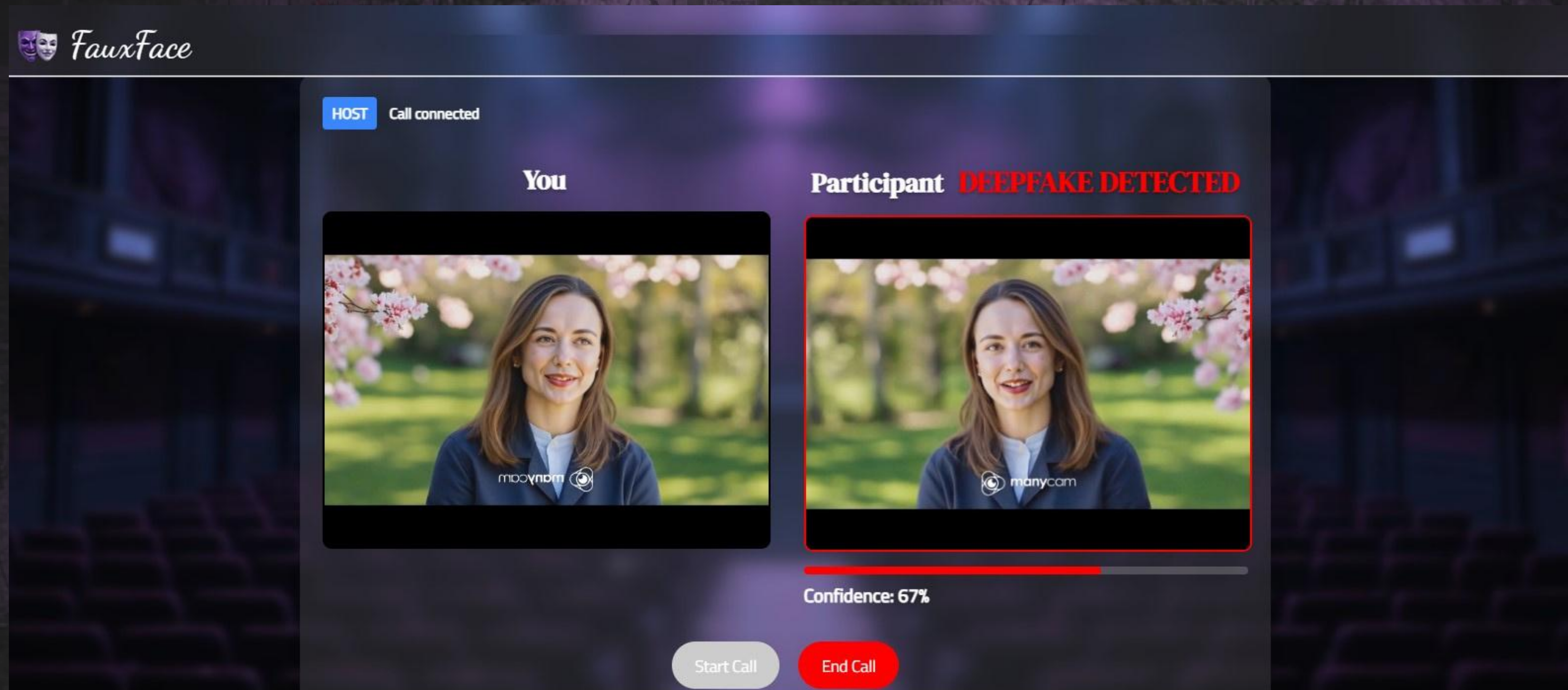
User Interface:

Participant Side Establishing Connection:



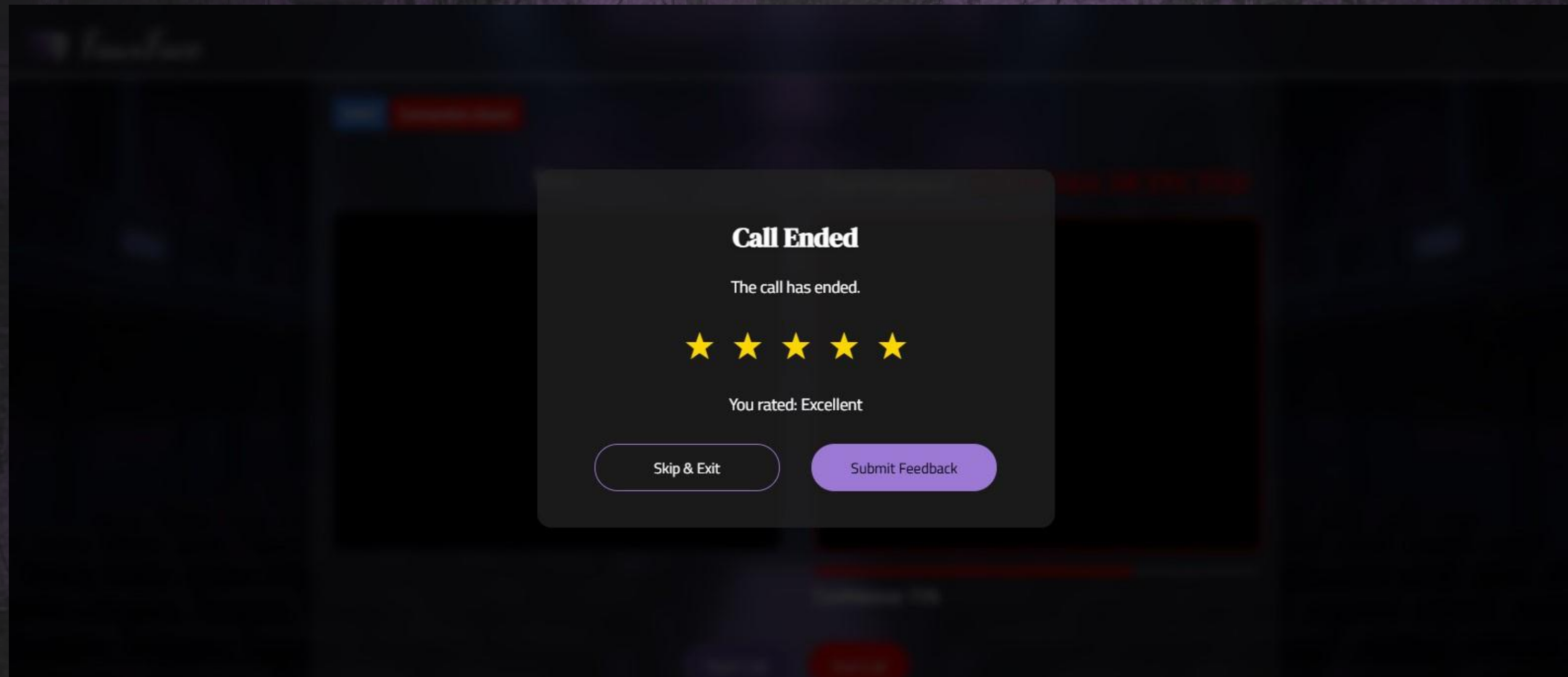
User Interface:

Call Started and Detection Started Immediately:



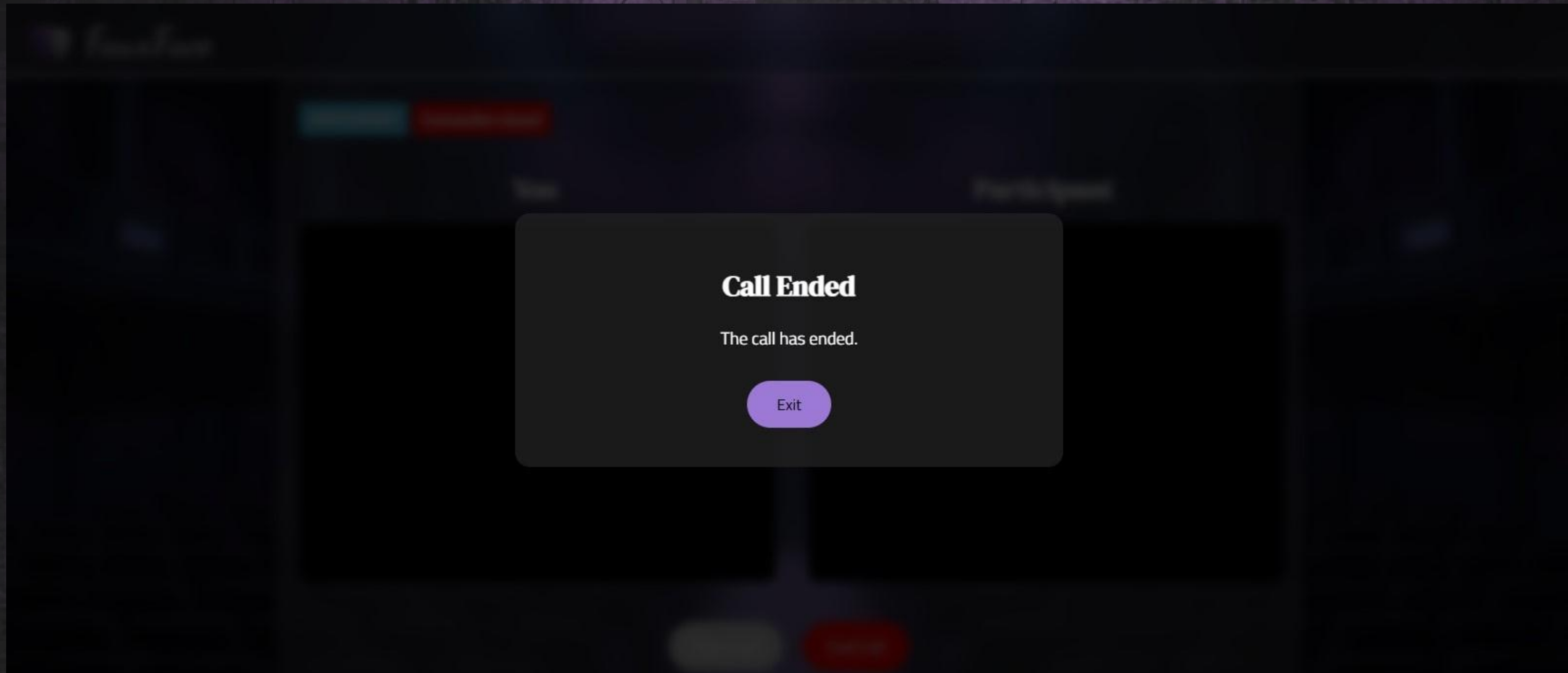
User Interface:

Call End and Feedback (Host Side):



User Interface:

Call End Pop-up (Participant Side):



Tools Used:

Frontend	Backend	Others
<ul style="list-style-type: none">• HTML• CSS• JavaScript	<ul style="list-style-type: none">• Python• Django• Django Channels• WebRTC• SQLite3	<ul style="list-style-type: none">• Tensorflow & Keras• OpenCV• Pandas• Google Colab Pro +• VS Code

Thank You