Purpose of Application

An Android app to validate whether a video file has been tampered to provide additional safety individuals that store home security video files in the cloud.

Functional Requirement

This table will list the functional requirements which describes what the application should do.

#	Requirements
1	The user must interact with the application through a Graphical User Interface (GUI)
2	The application initial loading page shall support the option to login and sign up/register
3	The application shall provide a forgot password feature to recover a forgotten password based on a username
5	The application will integrate with live streaming security cameras which will display the live stream through the app
6	The application shall support the for ability for a user to record a live stream by clicking a button
7	The application shall support adding a digital signature or adding a digital video fingerprint to a video during recording/save
9	The application shall support validating the integrity of a video file to see if it has been altered or manipulated by determining whether the signature/digital fingerprint is still present on the video file.
11	The application must allow the end user to view the stored videos
13	The application must check the validity of the video
14	The application shall support displaying the validation progress on the screen
15	The application shall display 'Valid' or 'Invalid' on the screen after validation has completed for a file.
16	The application shall support removal of video signature/digital fingerprint from a video file if it has been edited
17	The application shall provide a logout button to log the user out of the application

Table 3.1 Functional Requirement

Structuring System Requirement

Use Case Model

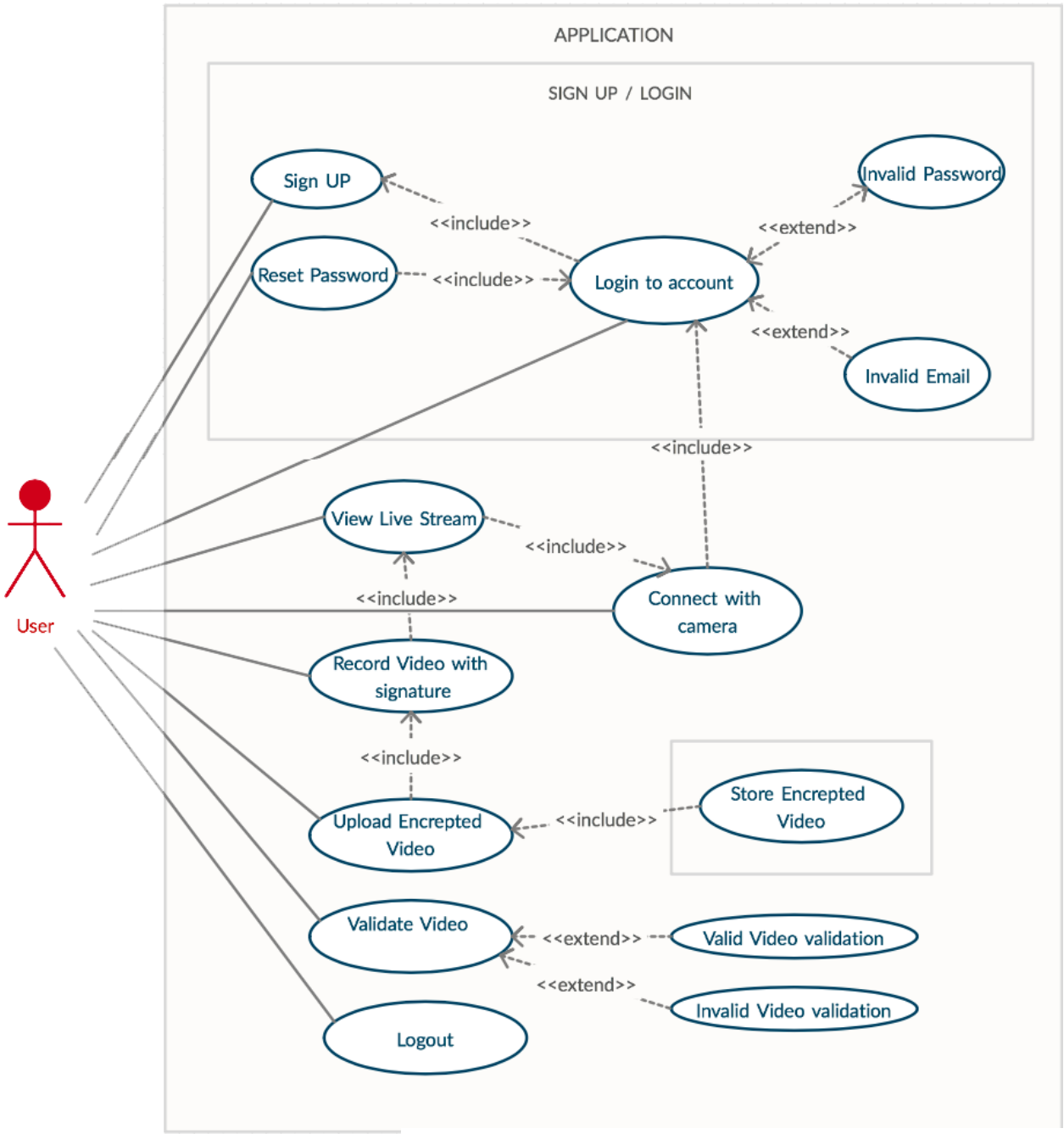


Figure 3.14 Use Case Model

Use Case Descriptions and Scenarios

Use Case	**Sign Up**
Description	The application will display a screen featuring the ability to perform Sign up
Steps	1. Open registration screen. 2. Enter user details 3. create a new user
Actors	User and System
Priority	Core

Table 3.2 Use Case Description

Use Case	**Login**
Description	The application will display a screen featuring the ability to perform login
Steps	1. Open login screen. 2. Insert user details 3. Authenticate user
Actors	User and System
Priority	core

Table 3.3 Use Case Description

Use Case	**Reset Password**
Description	The application will provide a reset password feature to recover a forgotten password based on a username and emailing
Steps	1. Open login screen. 2. Press forget password button 3. Enter username and email 4. Update password
Actors	User and system
Priority	Core

Table 3.4 Use Case Description

Use Case	Connect with camera
Description	The application shall support setup screen to integration with live stream security camera.
Steps	1. Enter camera details 2. Authorize connectivity
Actors	User and System
Priority	Core

Table 3.5 Use Case Description

Use Case	View live stream
Description	The application shall support the ability for a user to view incoming live stream footage from a security system which will display on the phone back to the user
Steps	view incoming live stream
Actors	User and system
Priority	Core

Table 3.6 Use Case Description

Use Case	Record Video with signature
Description	The application shall support the ability for a user to record a live stream by clicking a button then adding a digital signature or adding a digital video fingerprint to a video during recording.
Steps	1. Record video stream 2. Adding a digital signature or adding a digital video fingerprint 3. Encrypt video 4. Store video
Actors	User and System
Priority	Core

Table 3.7 Use Case Description

Use Case	Store Video
Description	The application shall support the ability to integrate to a cloud-based database to upload and store an encrypted video file to the logged in user's cloud storage
Steps	1. Save video 2. Store video to cloud-based database
Actors	User and system
Priority	Core

Table 3.8 Use Case Description

Use Case	Validate Video
Description	The application shall support validating the integrity of a video file from the user's cloud storage to see if it has been altered or manipulated by determining whether the signature or digital fingerprint is still present on the video file.
Steps	1. Retrieve videos 2. Validate video
Actors	User and system
Priority	Core

Table 3.9 Use Case Description

Data Flow Diagram

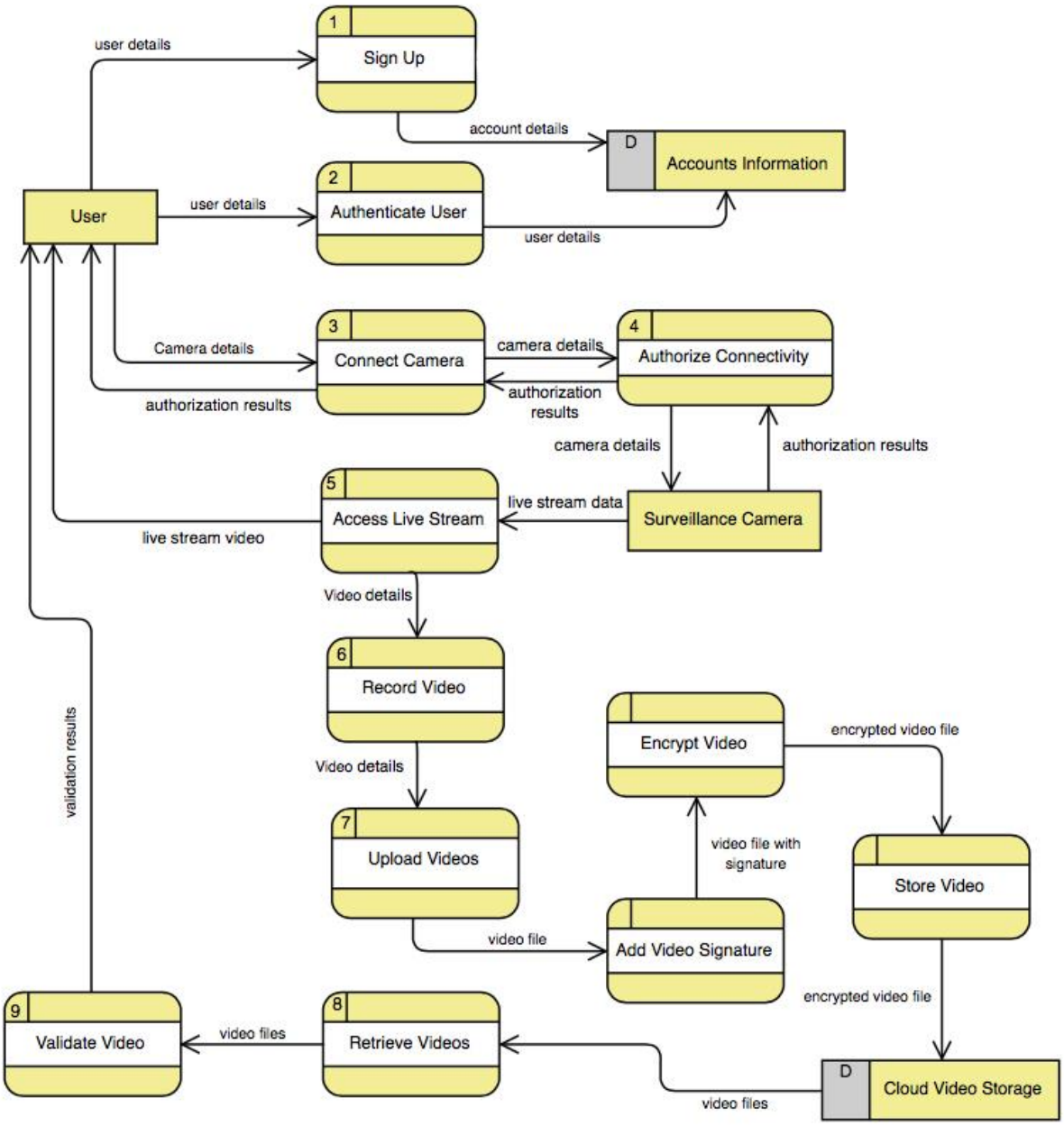


Figure 3.15 Data Flow Diagram

In this section, we will explain the Steps of data the flow diagram:

1. A user enters user details during the **Sign-up** process and account details are sent to the **account information database**.
2. A user entered user details during the **authenticate user** process
3. A user provides camera details during the **connect camera** process and the camera details are used in the **authorize connectivity** process which connect with the **Surveillance camera**. The **Surveillance camera** returns authorization results during the **authorization process** which were performed during the **connect camera** process and the authorization results are sent back to the user.
4. **Surveillance camera** provides live stream data during the **access live stream** process which delivers live stream video to the user.
5. The **Surveillance camera** provides live stream data during the **access live stream** process which provides video data during the **record video** process which also uses the video data during the **upload video** process delivers live stream video to the user which sends the video file to the **video storage database**.
6. The **video storage database** provides video files during the **access video** process which are used during the **validate video** process which returns video validation results to the user.

Interface Design

The design phase should include a prototyping stage. Prototype is “a preliminary visual mock-up that looks like a real app, and that demonstrates an app’s fundamental design and function, but does not contain working code” (Sara, 2018).

This section shows prototype of user interface design for the proposed application depend on the functions and requirements described in chapter3.

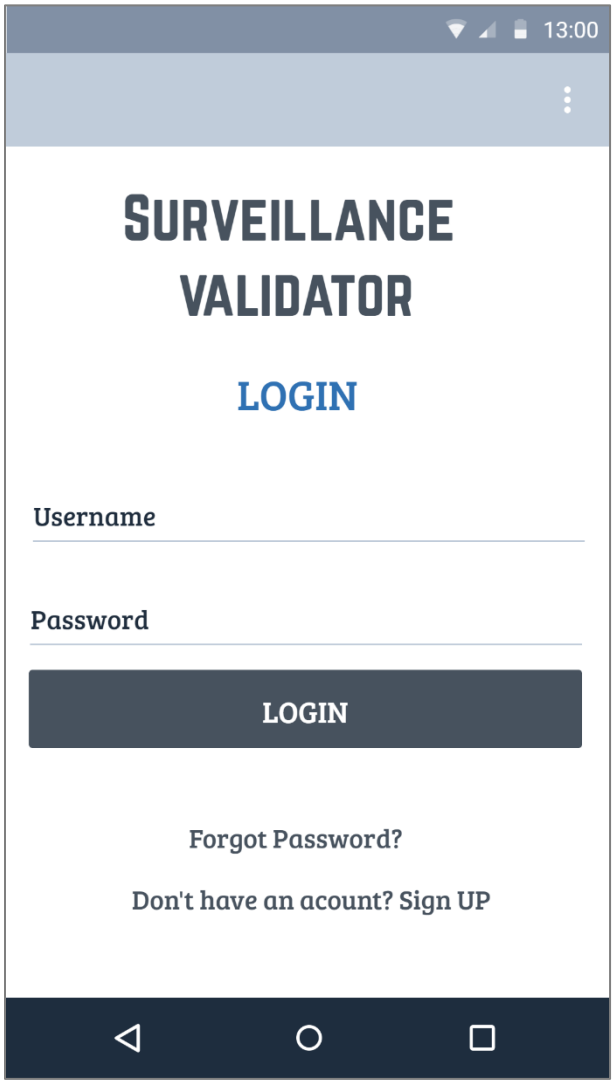


Figure 4.1 Login Interface

Figure 4.2 Main menu Interface

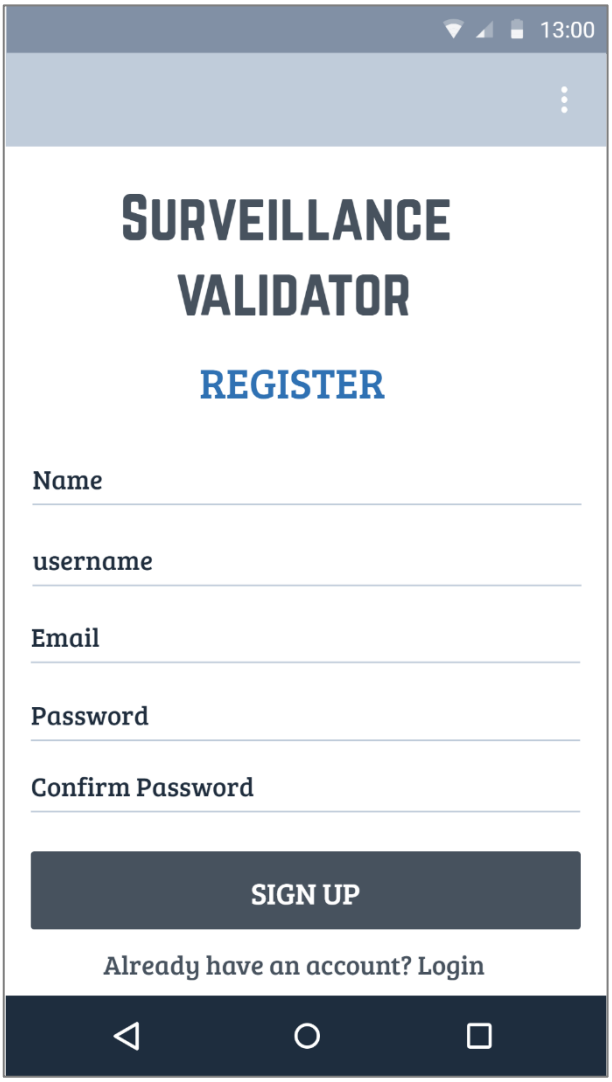


Figure 4.3 Registration Interface

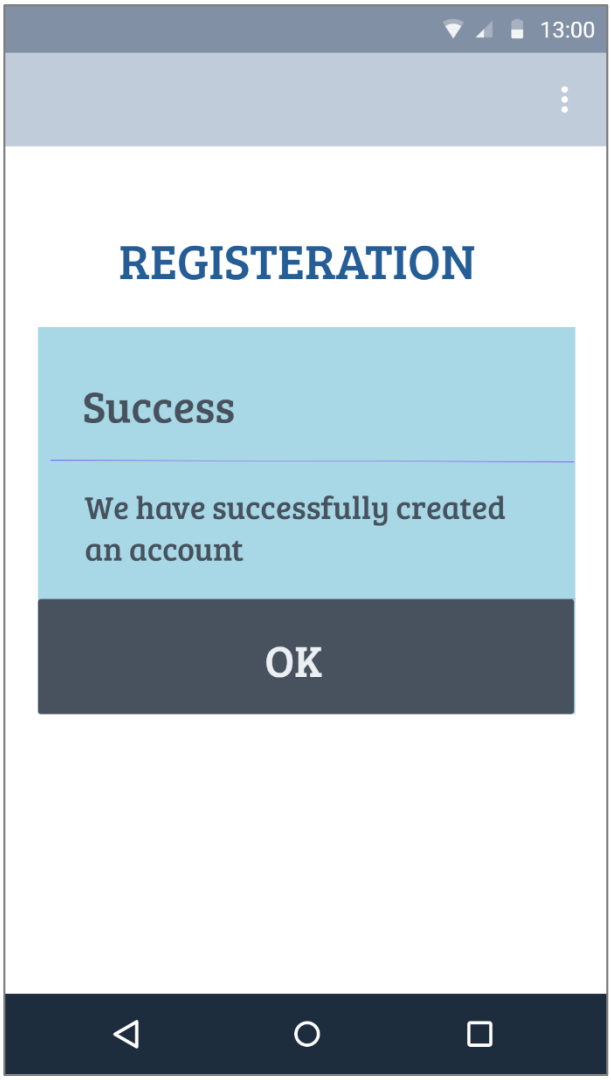


Figure 4.4 Successful Registration Interface

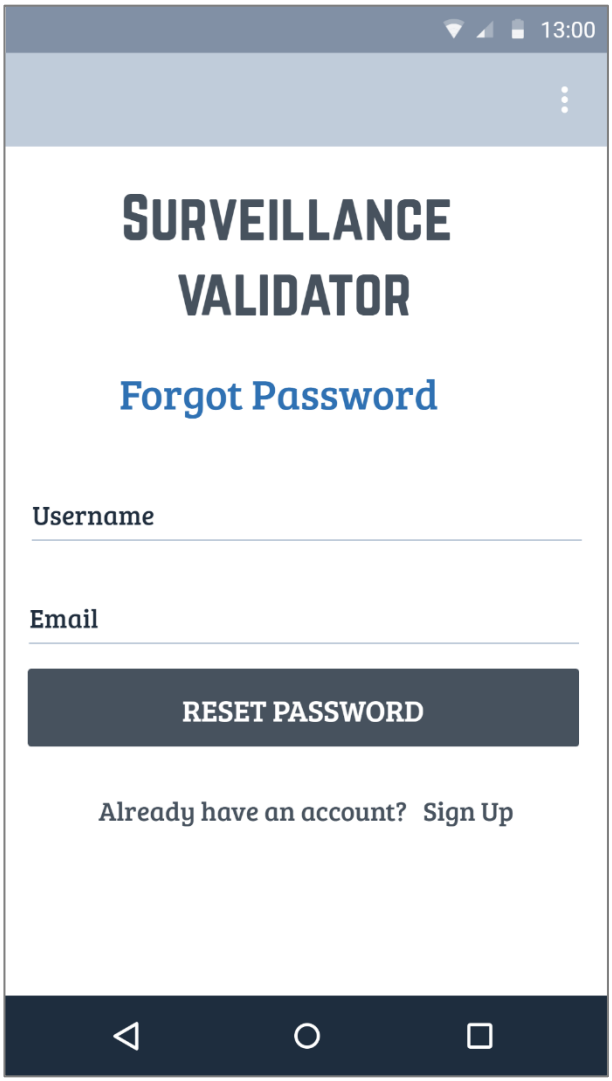


Figure 4.5 Forgot password Interface

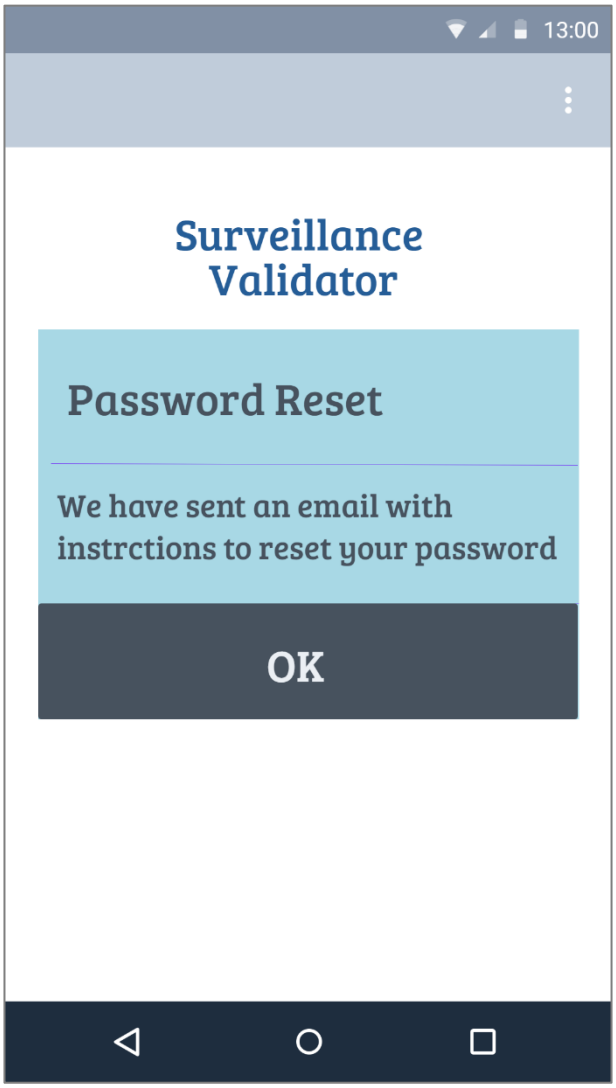


Figure 4.6 Reset password Interface

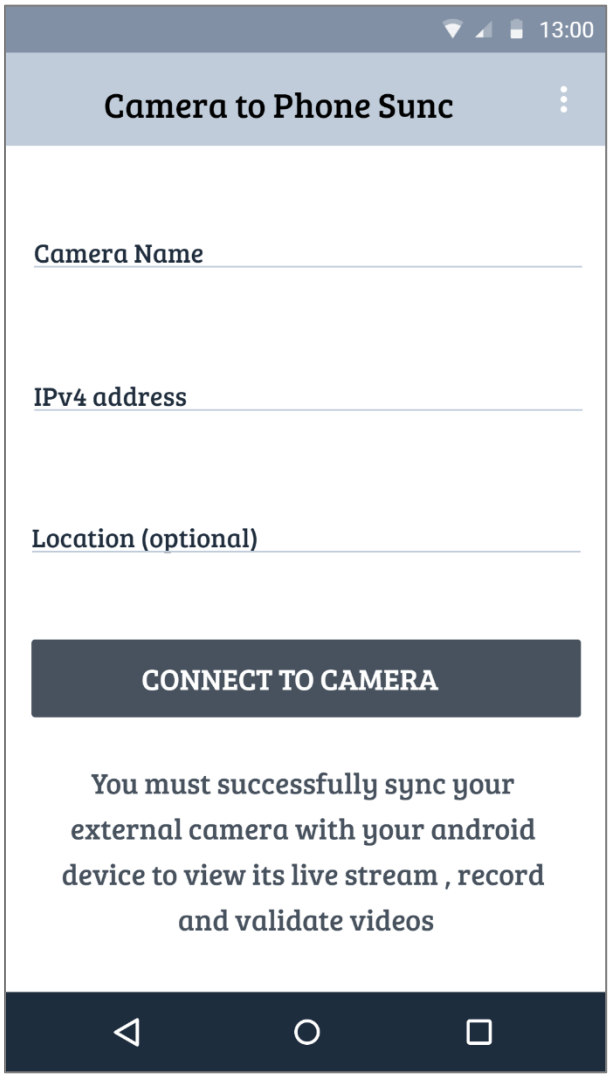


Figure 4.7 Camera Sync Interface

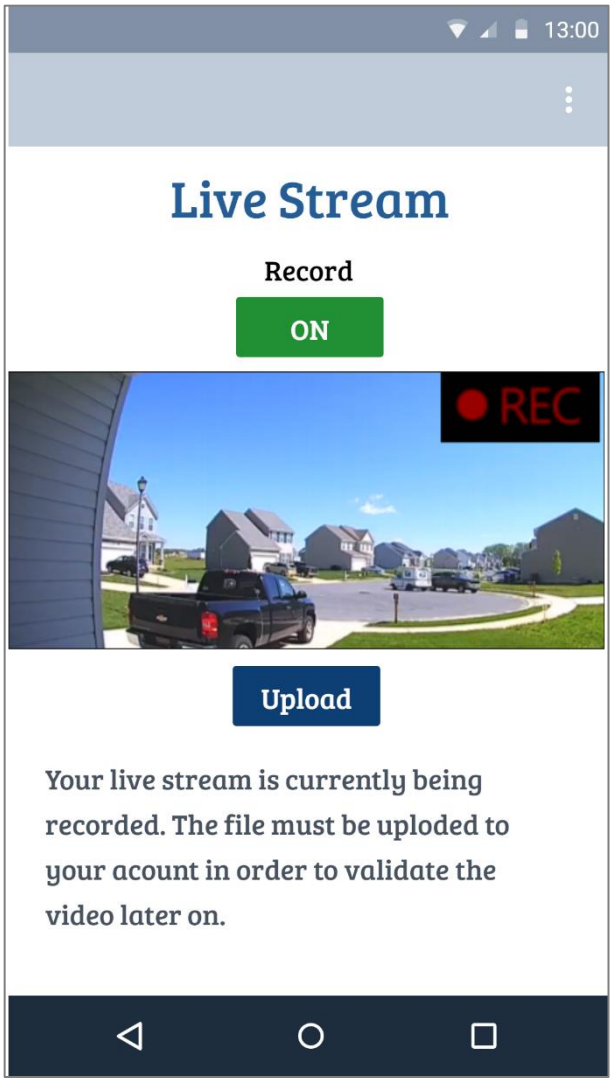


Figure 4.8 Recording Interface

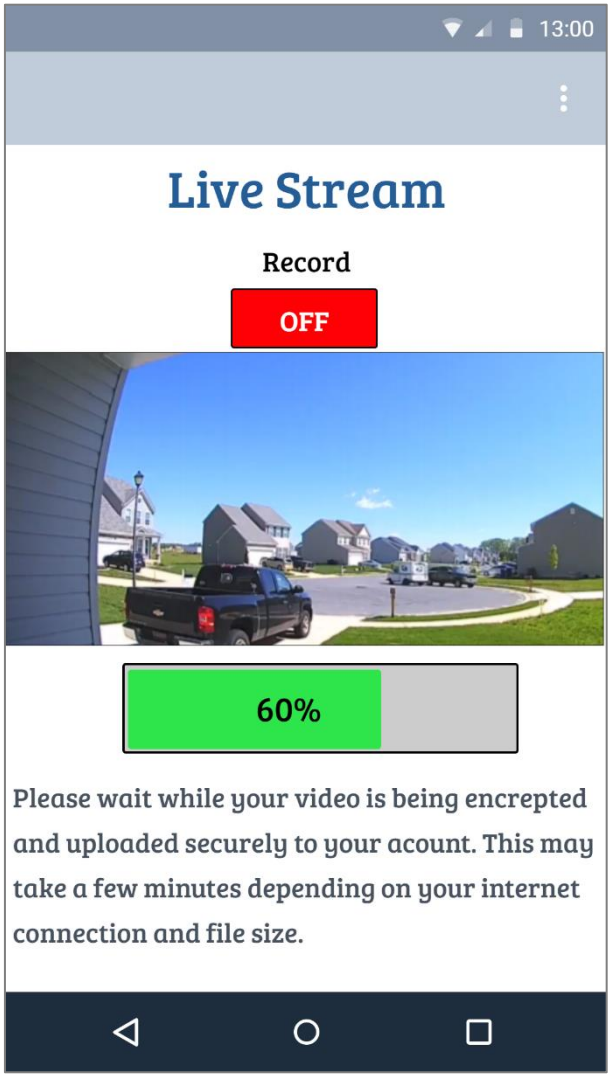


Figure 4.9 Video Encrypted Interface

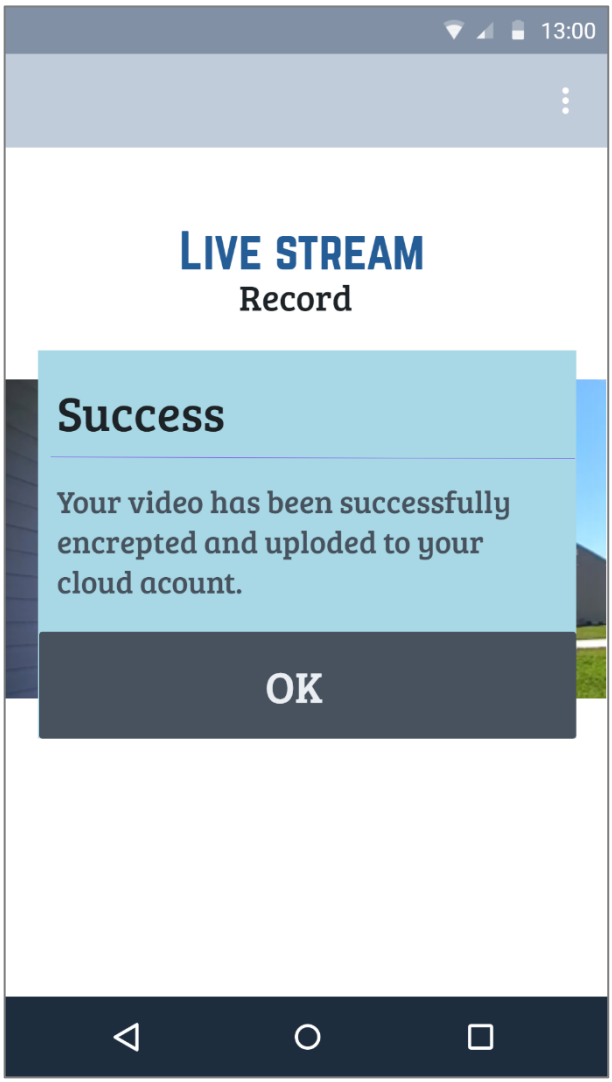


Figure 4.10 Successful Video Encrypted Interface

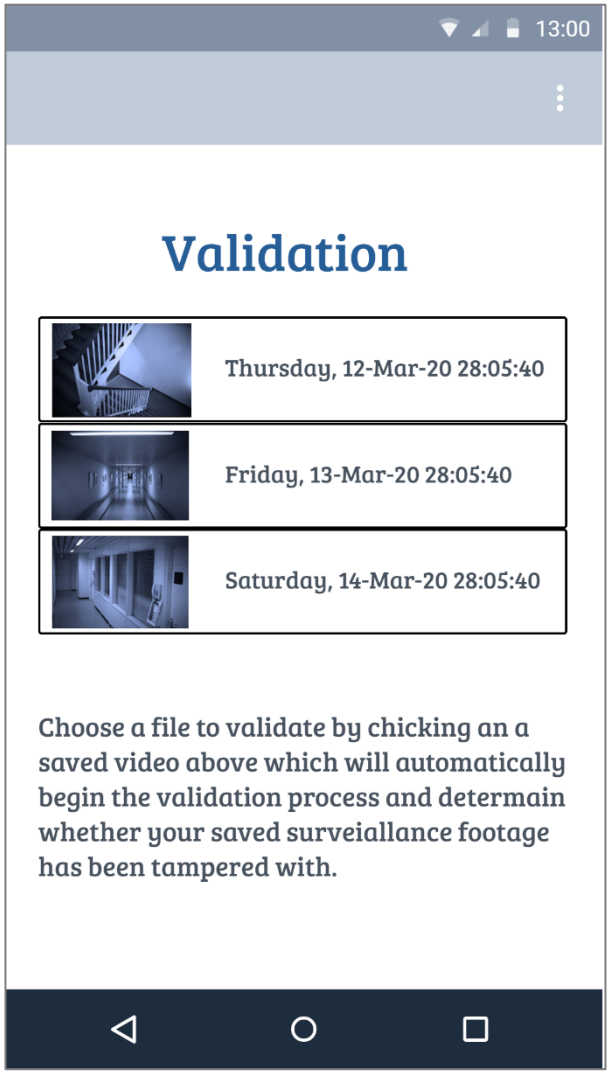


Figure 4.11 Validation Interface

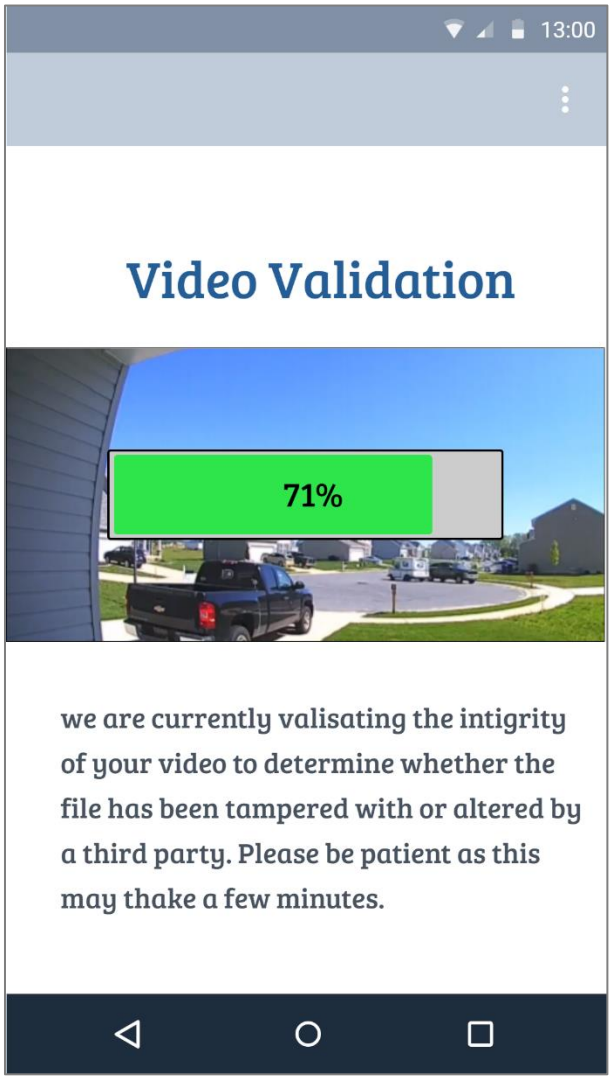


Figure 4.12 Validation process Interface

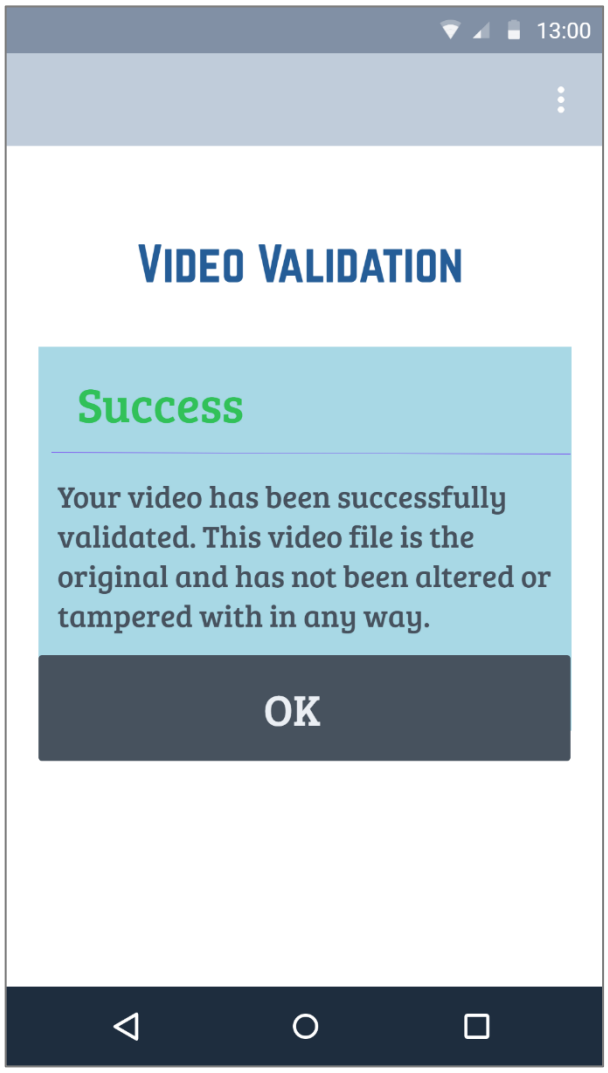


Figure 4.11 Valid Video Interface

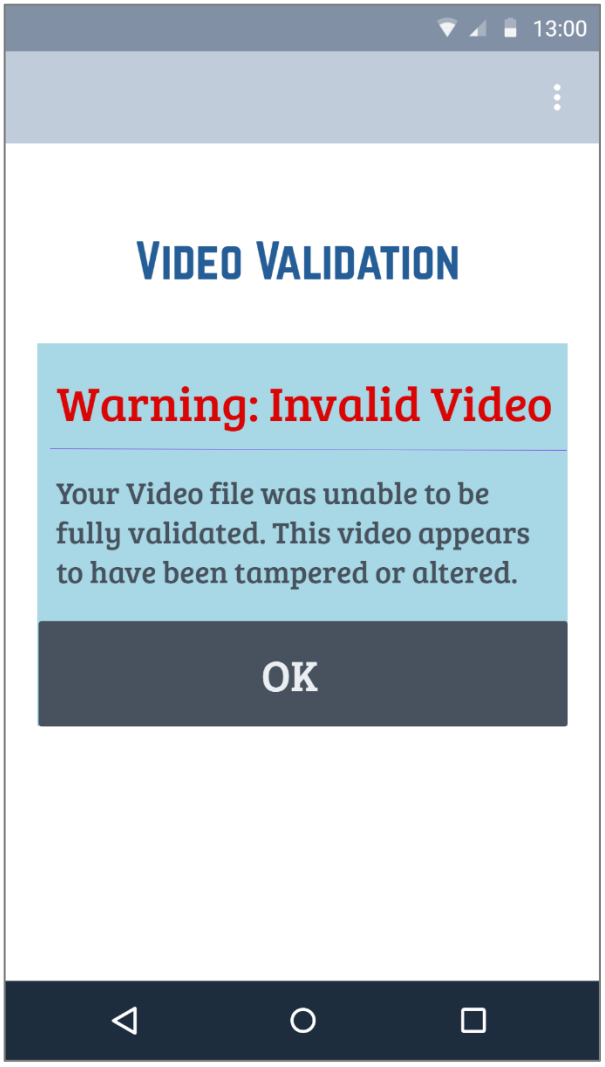
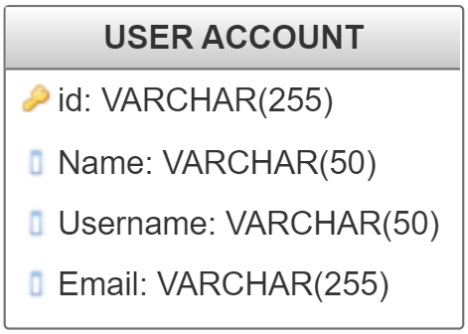


Figure 4.11 Invalid Video Interface

Database Design

Database design involves a model developed to guide how the data can be stored and organized. The Surveillance Video Validator application has a simple database to store the user account information. The Account table will hold the details for each customer's account. The fields include a unique Account Id (primary key), Name, Email and Username.