Software Requirements Specification

for

Anomalous Behavior Detection System (ABDS)

Prepared by

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Reg #** | **Sections Done** | **Marks (50)** |
| Umair Aslam | L1F20BSSE0385 | Section 2, UML diagram, ER diagram, DFDs, Goal Modelling. |  |
| Maryam Maqsood | L1F20BSSE0383 | Section 1, Section 5, Section 4 |  |
| Ahmed Khawar | L1F20BSSE0558 | Section 3, state diagram, sequence diagram, use case diagram, UI design |  |
| Rehan Ali | L1F20BSSE0575 |  |  |

Table of Contents

Table of Contents ii

Revision History ii

1. Introduction 1

1.1 Purpose 1

1.2 Document Conventions 1

1.3 Intended Audience and Reading Suggestions 1

1.4 Product Scope 1

1.5 References 1

2. Overall Description 2

2.1 Product Perspective 2

2.2 Product Functions 2

2.3 User Classes and Characteristics 2

2.4 Operating Environment 2

2.5 Design and Implementation Constraints 2

2.6 User Documentation 2

2.7 Assumptions and Dependencies 3

3. External Interface Requirements 3

3.1 User Interfaces 3

3.2 Hardware Interfaces 3

3.3 Software Interfaces 3

3.4 Communications Interfaces 3

4. System Features 4

4.1 System Feature 1 4

4.2 System Feature 2 (and so on) 4

5. Other Nonfunctional Requirements 4

5.1 Performance Requirements 4

5.2 Safety Requirements 5

5.3 Security Requirements 5

5.4 Software Quality Attributes 5

5.5 Business Rules 5

6. Other Requirements 5

Appendix A: Glossary 5

Appendix B: Analysis Models 5

Appendix C: To Be Determined List 6

# Introduction

## Purpose

Anomalous Behavior Detection System (ABDS) is a security system that detects suspicious activity. There are many security systems in the market but our system brings a different approach. Existing security systems in the market have rely heavily on human involvement that is why they are full of errors but our system is an automated approach, a system that removes human errors and detects the suspicious activity automatically. Our purpose is to provide a reliable surveillance system to the user and to be able to detect suspicious or anomalous behavior automatically with the use of artificial intelligence and machine learning algorithms and inform the user before any potential hazardous incident.

## Document Conventions

We documented our SRS in Times new Roman, any important requirement was bold so that the reader can easily understand the emphasis on it. The heading were done in bold and the requirements were written in bullets. The requirements are listed in preference order the most important as first and least important as last. Every statement in this document is relevant to our product. In section 4 every requirement is given a ranking and relevant numbered importance.

## Intended Audience and Reading Suggestions

Our SRS is intended for developers who will be able to develop our product according to our requirement specification, for marketing staff who will promote our product in the market and guide us throughout in our developing of product according to the market needs, it will be intended for users and testers. The users will be able to understand our product and will get familiar with its benefits and working. The testers will be able to test the test cases according to our debugging section specified in document.

There is no specific reading order, however, it is desirable that a user reads the document from the very start to thoroughly understand our product. The developers should read the functionalities of our product first so that they can understand the working of product for designing. The testers should read the debugging section for the test cases.

## Product Scope (Take/Refer from PD 1)

Our product ABDS is an automated surveillance system that involves the use of artificial intelligence and machine learning. It detects the anomalous behavior through the use of sensors and actuators. We have used extensive data sets and algorithms to teach our system through artificial intelligence. For detections, we have used motion sensors, pressure sensors, and the feature of facial recognition. Our system is operated by remote control and it can be accessed through mobile phones and tablets. It is compatible with both Android and iOS. Furthermore we have used multiple cameras for our system which have a methodical placements so they become hard to detect by the intruders and cannot be vandalized. Our product will be an advancement of all security products existing in market

## References

Vision and Scope document in Appendix C

Priority Ranking Document in Appendix C

Use Case diagrams in Appendix B

# Overall Description

## Product Perspective

The Anomalous Behavior Detection System (ABDS) in itself is a complete surveillance system that will be able to handle all the necessary and normal working and requirements of a surveillance system. However all these systems only provide surveillance and not much else, going one step further than this we want to give the user preemptive warning about a threat by examining the footage and detecting suspicious behavior in individuals and informing the user so that they can take the necessary actions. It’ll also have the functionality to call the Police or Fire department quickly in case of an emergency with the press of a button and in a particular mode it’ll be able to call the authorities automatically when it detects a break-in or a fire.

## Product Functions

* The shifting of power source from main to backup and vice versa should not be more than 1 second.
* The System should have two modes, active and passive, and user can control which mode to turn on or they can set a timer.
* The system should have local and cloud storage options for storing footage.
* The system should be configurable with a smartphone.
* The system should have enough modularity that new cameras and features can be added easily.
* The live feed from the cameras should be displayed remotely to a phone.
* The system should automatically detect suspicious behavior.
* There should be backup power in case of power outage.
* If a camera goes offline or the system is tampered with or is being turned off manually, the user should be notified on the configured device.
* The user data such as CCTV footages, daily activity reports and personal information should be protected.

## User Classes and Characteristics

Our product will have two major use classes which are

Home Owners

Business Owners

Other supporting classes will be

Admin

Home Owners:

Home owners will be the users that will use the lower end of our product which will include less cameras and less sensors to make its price more competitive with existing camera systems.

Some of the attributes of this user are as follows

* Education: Education among them will be high and most of them will be graduated.
* Jobs: Many of them will have corporate jobs would be out of their houses most of time.
* Technical Expertise: This will be quite low in home owners so we’ll need to automate as many thing as possible and make the system very user friendly and easy to use.
* Age: the age will vary from 30 to 50.

Business Owners:

This user class is going to be our major focus and more important to us in terms of satisfaction because they will buy our bigger ranged product which will include more cameras and more hardware for the coverage of a wider area. Business owners will include corporations such as factories and plazas who want to ram up their security

Some of their attributes are as follows:

* Education: Education will vary a lot so it’s hard to pinpoint it.
* Employees: These corporations may have from 50 to upwards of a thousand employees that would all be covered under our system.
* Technical Expertise: While the owners themselves wouldn’t have much expertise but they would already have a dedicated person for surveillance whose technical expertise would be high.
* Security: As these major corporations would have very expensive assets that our system would protect, so, we need to make sure our system never fails.

Admin:

This will be class that will be responsible for maintaining and updating our system and providing customer support to our users. Some of its attributes can be

* Education: Graduated with preferably some experience in the field.
* Age: 25 to 40
* Technical Expertise: They would be very informed in technicalities and would have good experience in technical matters.

## Operating Environment

In our operating environment we will be dealing with both software and hardware. Our hardware would include 8mp High Definition cameras which would be connected to the central Hub with optical fiber wires.

The hub would be the place where all of the processing, storing and execution would be done. It houses storage for storing upto three weeks of continuous footage and a small processing unit for our system to detect the anomalous behavior as well as capability to connect to the internet for remotely accessing the system.

The system would also include various sensors on doors, windows, and other entry points to detect break-ins and smoke detectors within the house to detect a fire hazard.

## Design and Implementation Constraints

There are a few design constrains that may hinder our development

Privacy policy of protecting our user’s personal footages will force us to make our system really secure which will take more time to develop and increase our cost.

As we depend on third party sources for our cameras it’d be hard for us to provide them separately or as a replacement in a competitive price comparing with other camera companies.

The hesitation of users in using a product that stores and analyzes their personal footage maybe high and we may need to win their trust before implementing this system.

Using machine learning and AI to detect suspicious behavior is not going to be easy to developing and implementing that feature is also cumbersome.

## User Documentation

We will provide following documents to the user;

* A detailed user manual explaining all functions and all tasks.
* Online help through our website and chat forms.
* Short videos detailing everyday tasks that a user may need to perform.
* Customer support through call.

## Assumptions and Dependencies

Assumptions:

With this product we are assuming that people would accept a system that uses AI and analyze all the data that is being given to it. There may be some hesitation in acceptance of this product.

The government may not consider this threatening to the user privacy.

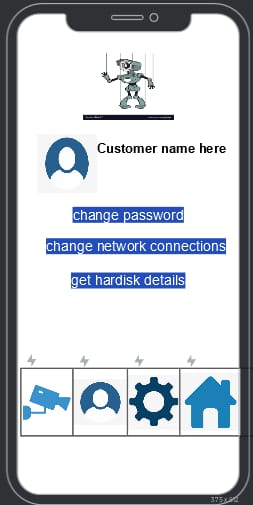
Dependencies:

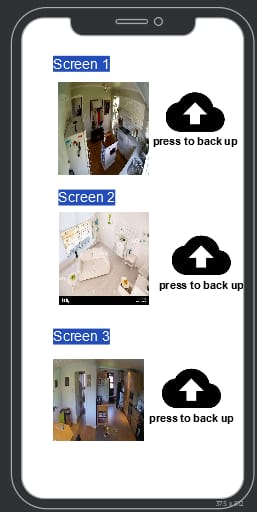
We are dependent on third party companies for supplying us with cameras and sensors, so if they fail or prove to be of worse quality than our product will fail.

We are dependent on the AI for our detection and if it has a bug or it fails then our entire system may become redundant.

# External Interface Requirements

## User Interfaces

Some of the UIs are given below



## Hardware Interfaces

A camera which will be connected to the raspberry pi 3 that rasberry pi3, will have its own network adapter which will be used by the system to access internet to establish the connection with our server and to connect to our app on our smartphone as we will use the basic IOT convention to work with our system by our smart phone. Also, a backup power will be used for our system incase of power outage our system will be powered by it also a servers and spouting hardware will be used to support the deployment of our system on customer end our panel will also have a hard disk where it will store the data – training data gathered from the system. Which will be later transmitted to our servers.

## Software Interfaces

## We will be implementing the SQL for our database to keep our customer data in a structed manner along with that whatever data we will receive from our customer system we will implement the python coded ML models on it (which processing will be done on our servers) we will make sure to use Linux OS on your servers as it’s faster than the traditional windows OS and we can also customize to go minimal on our overhead. We will have an entire app dedicated for setting of our system through smartphone, we will also have FTP server configured on our server and client on our panel.

## Communications Interfaces

We will use the TLP (transport layer protocol) for our FTP communication between our system and server we will use FTP for transmission of training data obtained from the system itself and we will figure out the appropriate port for our application to server communication

# System Features

1. **Power backup**

### Description and Priority

Our system has a power backup feature which allows our system to run in case of a power failure. The batteries save the power is the background so when the power is shut down the passive mode of system is turned on and the system is shifted. This way our system does not turn off in case of direct power failures. It is rated 7 as it has both high benefit and high penalty.

### Stimulus/Response Sequences

The feature will only be enabled in case of power outage.

### Functional Requirements

REQ-3: The System should have two modes, active and passive, and user can control which mode to turn on or they can set a timer.

REQ 5. There should be backup power in case of power outage.

REQ-7: The shifting of power source from main to backup and vice versa should not be more than 1 second.

1. **User Verification**

### 4.1.1 Description and Priority

Our system only allows authorized user to access the system. The user is asked to enter the authorized login ID and password to identify themselves. The login ID should be valid and the user will be given 5 tries after which the system will be locked. In case the ID entered is invalid the user will get a message on the configured device. It will be rated 8 as it has high benefit and rated 10 for extremely high penalty.

### 4.1.2 Stimulus/Response Sequences

To access the system, to make changes and to view the CCTV footages the user will be asked to enter a user login. The user will be given 5 tries, on every wrong try the user will get a message of his/her configured device so that the user can be alerted in case someone is trying to tamper with the system. After the valid login ID and password is entered the user will logged in to the system.

### Functional Requirements

REQ-10: If a camera goes offline or the system is tampered with or is being turned off manually, the user should be notified on the configured device.

# Accessible by Configured Device

### Description and Priority

Our system can be accessed by any configured device such as smartphone, tablet, laptop etc. The user has to authenticate the configured device to the system and then the user can access the CCTV footages and daily activity reports or live feed on his/her device. It is rated 5 as high risk and 8 as high penalty.

### Stimulus/Response Sequences

The user will first identify the device such as smartphone or tablet to the system, entering the device name and scanning a QR code. An application of the security system will be installed on the phone where the user will log in from the same authorization ID. The user would have to enter the ID whenever he opens the feed on the phone to identify themselves as an authorized user.

### Functional Requirements

REQ-4: The live feed from the cameras should be displayed remotely to a phone.

REQ-6: The live feed from the cameras should be displayed remotely to a phone.

# Data Backup and Protection

### Description and Priority

The safety of our user’s data is highly important for us so that is why we have a backup option in our system where all the user’s data such as CCTV footages and daily activity reports are backed up on cloud storage. That can be accessed by user any time and incase of accidental deletion and loss of data the data can be accessed from cloud storage. That data can be accessed through configured device as well but only if user identifies themselves as authorized user by entering a valid login ID and password.

### Stimulus/Response Sequences

The daily live feed of camera would be stored in a local and back up storage such as cloud storage. The data backed up is daily. During back up if an error occurs the user is notified and the backup is started once again. Once the backup is complete the user is notified on the configured device.

### Functional Requirements

REQ-3: The system should have local and cloud storage options for storing footage

# Other Nonfunctional Requirements

## Performance Requirements

* Our system shall detect any suspicious activity in 0.5 seconds.
* In case of power failure, our system shall immediately shift to backup power in 1 second.
* In case of manual shut down of power, the user will be notified on configured device and would only be shut if the authorized user permits.
* The system should have the type interface that can be easily learned by novice users in a 2 hours of training and expert users in 20 minutes.
* The system will only allow the authorized users with a valid ID and password to view the CCTV footages and daily reports on the configured device.

## Safety Requirements

* In case of a suspicious activity detected by the system the user will be notified as well as the system will contact the nearest police station.
* To save ourselves from accidental deletion of data or loss of data due to power failure the data will be saved as backup on cloud storage.
* Sensors should inform the user if a camera is tampered with.
* Any foreign attempt of login will be notified to the user.
* Three factor authentication for system critical aspects.

## Security Requirements

* Only authorized users should be able to operate the system.
* Every time a user operates the system he or she should enter a valid ID and password and it should be a two factor authentication.
* The data of user can only be accessed by the authorized user and the privacy of user should be protected at all cost.
* The user should be identified by facial recognition using the retina sensors.
* If a user wants to change the authorization or add any other user, the user must contact customer support and verify that he or she is an authorized user.

## Software Quality Attributes

* The system should have modularity so that it can maximize adaptability and allows the user to add and modify data sets according to changing requirements for different scenarios.
* The system should be operational 24 hours and during the update it should not shut off and should run in background.
* The response time for the screening should not be more than 0.5 seconds.
* The system should be portable enough so that it can be easily shifted without vandalizing anything in it.
* All the data sets provided during testing should be operational.

## Business Rules

* It shall not take more than 1 second to detect suspicious activity by the system.
* The system should be compatible on android and iOS so it can be configured with a smartphone or a smart device easily.
* To shift from active to passive mode the timer should be set for not more than 5 seconds and should be shifted in between 10 seconds.
* The live feed of cameras should be only viewed on a phone when a valid logic ID and password is entered.
* In 1 second the power should be shifted to back up in case of power outage.
* The user should be notified in not more than 0.2 seconds in case the system is tampered with.
* The daily reports and the CCTV footages should only be view on the configured authorized device.
* If someone tries to login through another device the system shall not proceed the request and notify the user on configured device.
* The system should be able to accommodate, if a user requests more cameras to be installed in future

# Other Requirements

Some requirements that remained unmentioned in the rest of the document are listed here.

* The system should have a total of 100 Gbs of storage.
* The server should not have a downtime of more than 1 hour in 1000 hours of runtime.
* At least 40 minutes of power backup should be provided with the system.
* Multiple firewalls to prevent ddos attacks should be implemented.
* Three factor authentication when accessing could storage.
* System should be as generalized as possible to enable reusability.

# Appendix A: Glossary

Some important acronyms are;

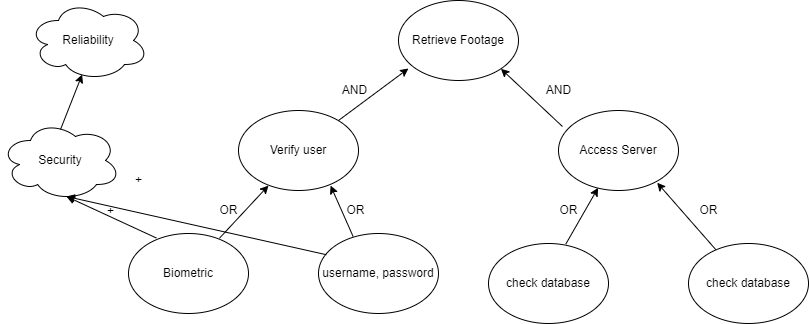
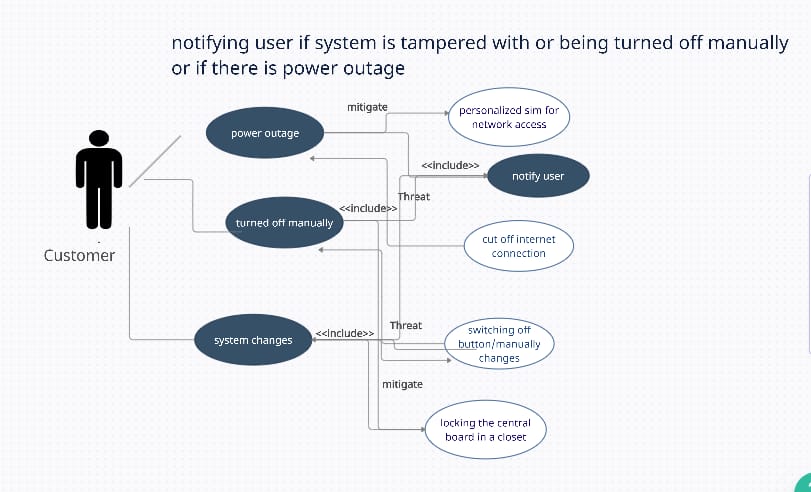
ABDS (Anomalous Behavior Detection System)

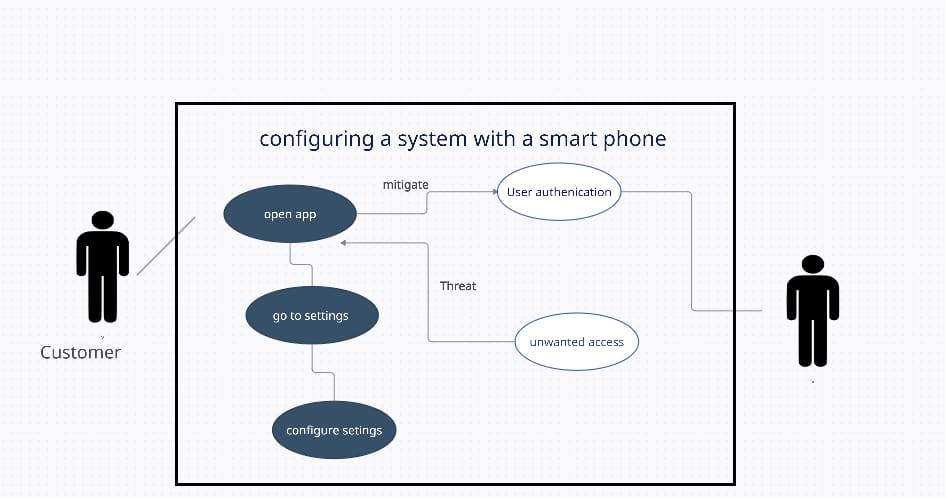
ER (Entity Relation)

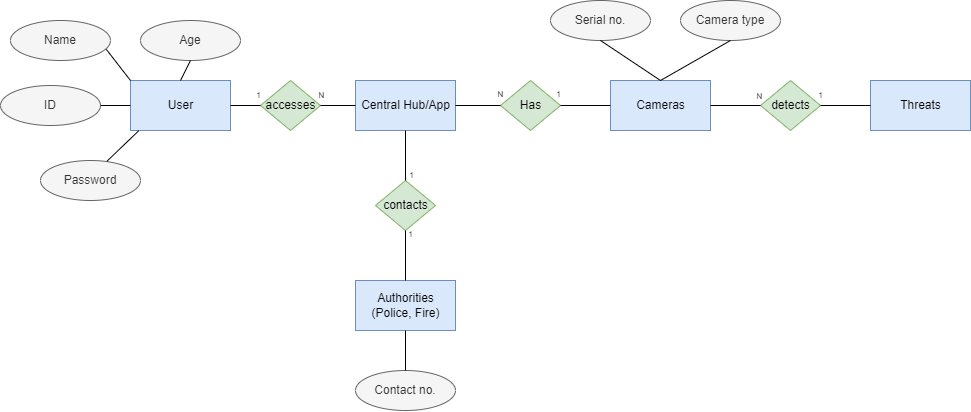
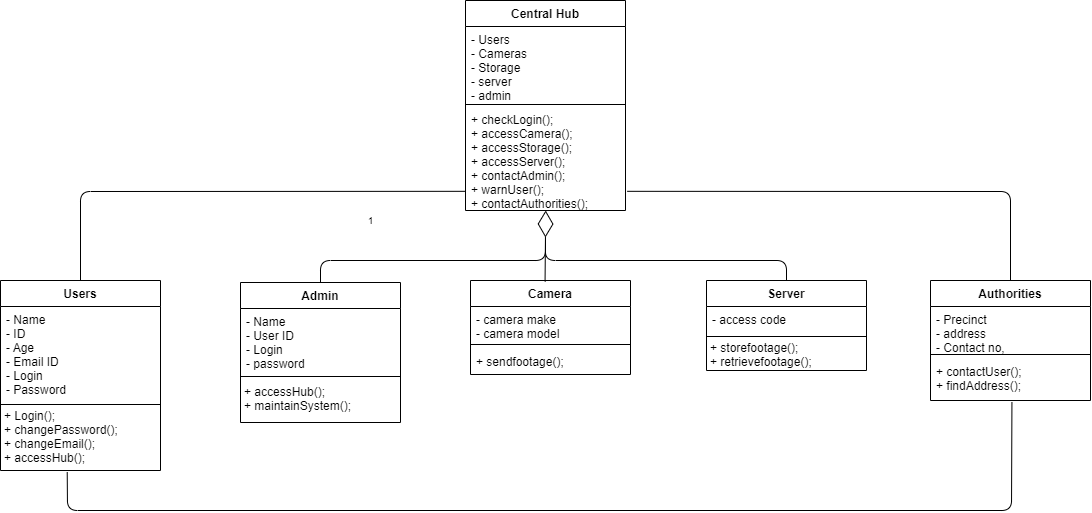
GRL (Goal-oriented Requirement Language)

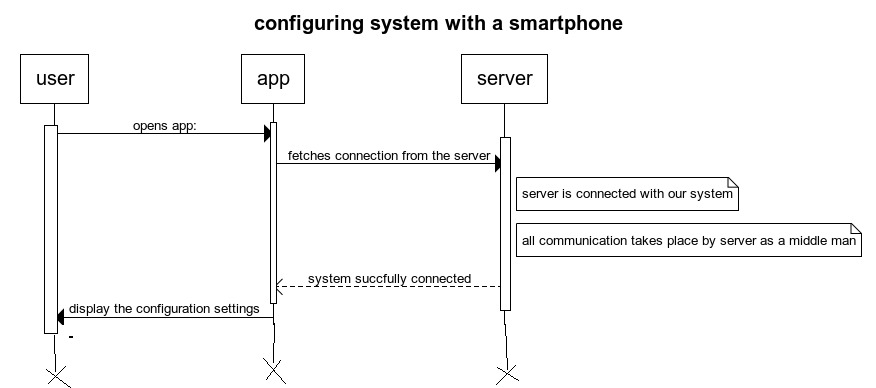
REQ (Requirement)

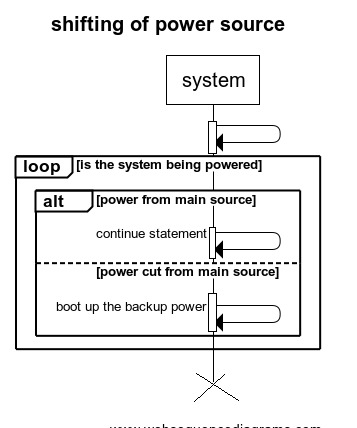
Appendix B: Analysis Models

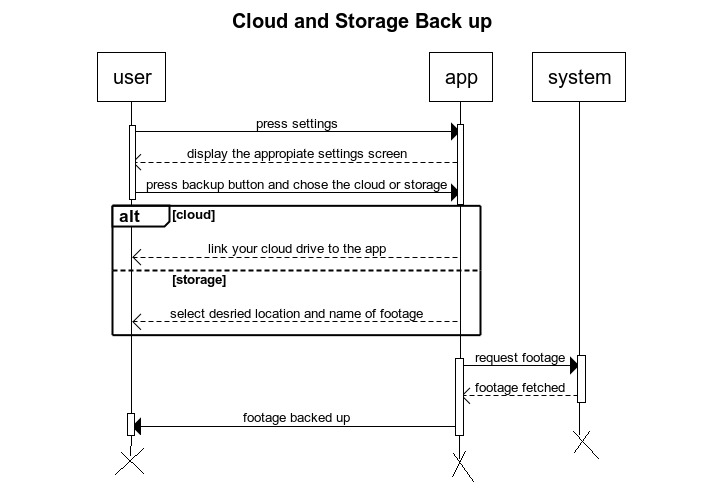
* **Goal Modelling using GRL**
* **Use Case Diagram**

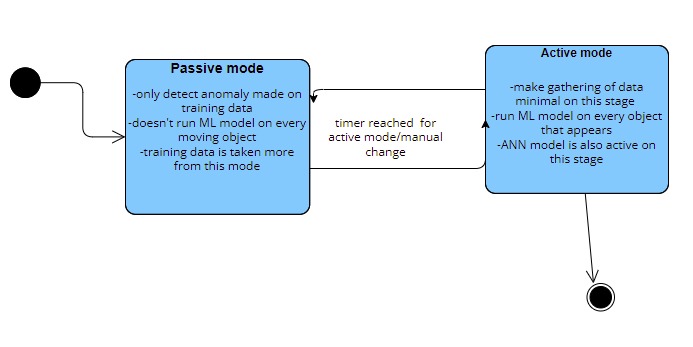


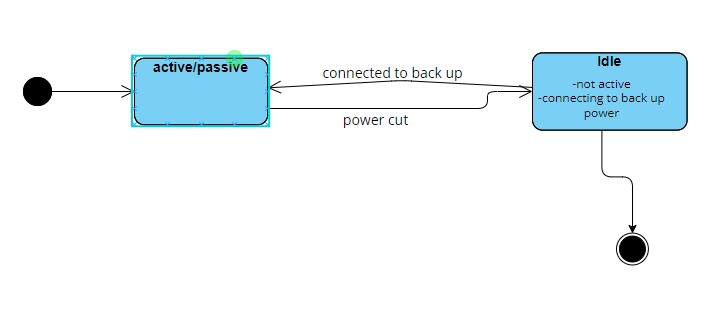
* **Complete ER Diagram**
* **Class Diagram**
* **Sequence diagram of 3 important scenarios**



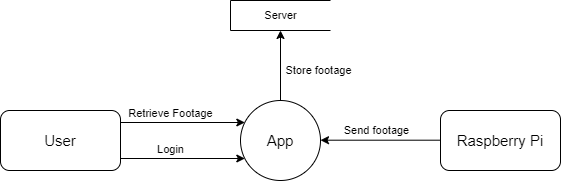


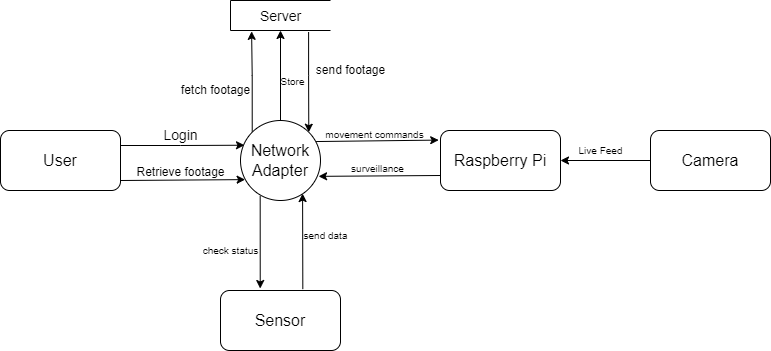
****

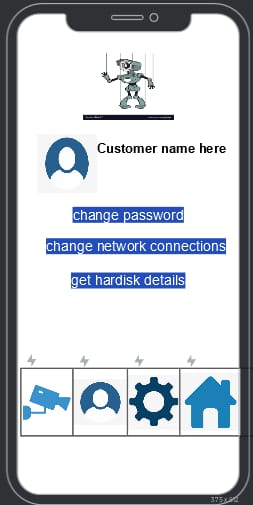
* **State Diagram at least 2**

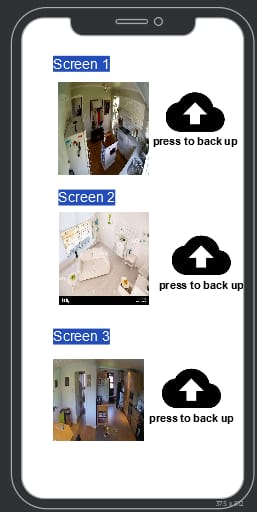


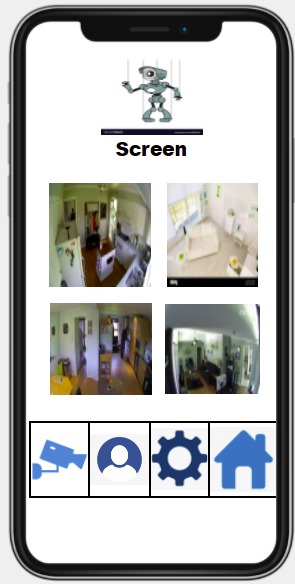
* **DFD Zero level + Level 1**

DFD Zero Level:

DFD Level 1:

* **3 Important UIs**

****



Appendix C: To Be Determined List

* Vision and Scope Document
* Priority Ranking Document
* Legal Requirements
* Licensing and Contracts