Software Requirements Specification

for

Smart Home Security System

Revision 0.2 draft

Prepared by Theyab Alsubaie, Abdullah Altuwayrsh and Muntathir Alsaleh

MX-222-555_SWE-Course_Project

2023-03-08

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
Smart Home Security System's Software Requirements Specification	2023-03-26	First Draft	0.1
Smart Home Security System's Software Requirements Specification	2023-03-27	Second Draft. To include User Story in the feature section. To use line spacing of at least 1.15 to have the document more readable.	0.2

1. Introduction

1.1 Purpose

This document presents a detailed description of an automated home security alarm system to protect the home from intrusion. It will explain the requirements, specification and should provide a security and safety features of the system, the interfaces of the system, what the system will do, the constraints under which it must operate and how the system will react to external stimuli since the system is covered by a multiple sensors, actuators, and Near-field communication card reader.

1.2 Document Conventions

Main Section Title:
Font: Times New Roman. Face: Bold Size: 14

Sub Section Title:
Font: Times New Roman. Face: Bold Size: 12

Other Text Explanation:
Font: Times New Roman. Face: Normal Size: 12

1.3 Intended Audience and Reading Suggestions

This document is intended for general use including the stakeholders, developers, clients, and customers of the system.

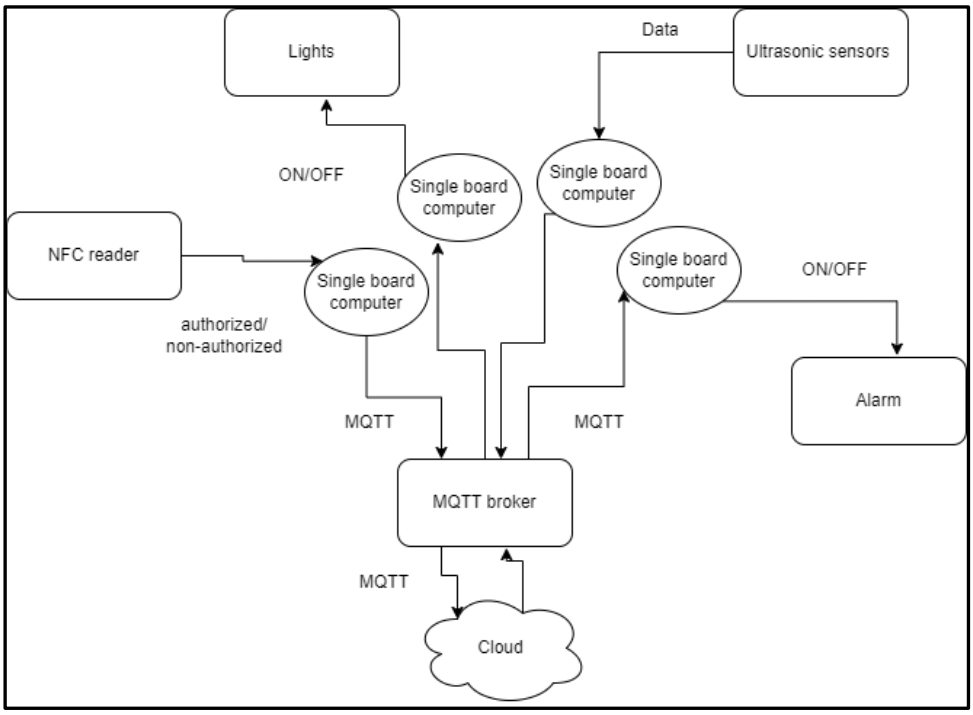
1.4 Product Scope

The scope of this product is to build a small embedded system in case of intrusion so the system will trigger of someone pass by with the help of using multiple sensors, actuator, and an NFC Card reader so basically the security alarm system will ask for a passcode within a period of 15 seconds, otherwise if an attempt was failed the alarm system will immediately notify the homeowner.

1.5 References

2. Overall Description

2.1 Product Perspective



2.2 Product Functions

- Guard homeowner from thieves' intrusions.
- Alarm checking system which differentiates between thieves and owner.
- Smart light to deter thieves by sensors.
- Provide online monitoring for the home security system.
- Receive notifications in case of intrusions or suspicious activity

2.3 User Classes and Characteristics

The general customer who will be using our product is a homeowner. Our system is easy

To use which will make it fine for normal people to understand it. It does not need technical experience or a high educational level. Part of the users will be using this product remotely from their office or outside home. While some customers will be using it locally inside of their homes.

2.4 Operating Environment

The hardware will be using single board computer. Sensors, lights, NFC reader, alarm are all part of the hardware component which will be used. For the software part, it will be emulated using packet tracer software to have the best possible integration.

2.5 Design and Implementation Constraints

There are some limitations such as power consumption. Many sensors will be running continuously which will consume a lot of power. Power optimization can be used but to a certain limit since security is a critical thing. Furthermore, the language is limited to English at this first release. In addition, records of security data must be stored which will need a hard disk for storage.

2.6 User Documentation

2.6.1 User Manual

What is in the box:

- Security device
- Gate entry NFC card reader
- NFC Card x3
- Ultrasonic Sensor x8
- Flood Light x8
- MQTT Broker
- Sound alarm device
- Cloud key device
- User Manual

2.6.1.1 Security Device

This is the main device in the Smart Home Security System that you will use to safeguard your home during your absence. During the first-time use, you will have to set up a secret pin to arm and disarm the system. The system limits pin entry to 3 times with 3 seconds delay in between, failing to enter the correct pin will results in the system going-into lock-down mode for 15 minutes. During lock-down mode, if the alarm was triggered prior to the wrong pin entries. it cannot be turned off.

2.6.1.2 Gate Entry NFC Card Reader

Gate entry NFC card reader will allow the homeowner to enter the home without triggering the alarm as it will disarm the system once the card gets read and it has access to the perimeter.

2.6.1.3 NFC Card

The NFC card is factory programmed and is linked to the Smart Home Security System.

2.6.1.4 Ultrasonic sensor

The Smart Home Security System comes with 8 ultrasonic sensors for placement around the house perimeter. The information generated will be displayed in the cloud dashboard, in addition to triggering the flood lights to turn on.

2.6.1.5 Flood Light

The Smart Home Security System comes with 8 Flood Lights to secure your home perimeter from stalkers or thieves who are trying to sneak into your home. Once an object is detected by the ultrasonic sensors it will trigger the flood light to turn on to deter any intrusion attempt.

2.6.1.6 MQTT Broker

The MQTT Broker is the communication device that relays all the messages between the Smart Home Security System devices.

2.6.1.7 Sound Alarm Device

The Sounds Alarm Device will play a siren sound once an intrusion is detected. The siren is rated at 85 dB at 10 cm (about the length of the long edge of a credit card).

2.6.1.8 Cloud Key Device

The cloud key is a device that relays the status of the Smart Home Security System to the cloud which enables the homeowner to view his/her home statistics such as:

- Whether an intrusion is detected
- Log of intrusions
- Last time object was detected moving along the outside perimeter of the home
- Log of detected object date time
- Last authorized entry to the home
- Log of authorized entries to the home
- Last time the system was armed
- Log of arming and disarming of the system

2.6.2 User Manual format

The user manual shall be in English language, double side printed with a standard size of ISO A4. The manual shall also be available in PDF format in the cloud dashboard.

2.7 Assumptions and Dependencies

2.7.1 Assumptions:

- The home shall be equipped with electricity
- The home shall have a reliable Internet connection
- The homeowner should have mean of accessing the cloud dashboard such as a laptop or a mobile phone
- The Smart Home Security System shall be powered using an Uninterruptable Power Supply (UPS, not included with the system)
- The home shall have a grounding rod installed by a professional electrician.

3. External Interface Requirements

3.1 User Interfaces

The Smart Home Security System will have one GUI in the cloud dashboard. The GUI shall display a simple statistic about the system status as prescribed in this document, section 2.6.1.8 “Cloud Key Device”.

3.2 Hardware Interfaces

The Smart Home Security System will have one hardware interface used by interacting with module “Security Device” as prescribed in section 2.6.1.1 in this document. The hardware shall allow the homeowner to:

- Enter a pin (0-9) in response to the Security Device prompt
- Press a button to arm or disarm (if armed) the system

All communications within the Smart Home Security System ecosystem shall use MQTT protocol.

3.3 Software Interfaces

All single board computer devices shall use any operating system that fully utilizes the memory size and hardware capabilities such as Raspbian. The cloud dashboard shall be based on Ubuntu distribution, version 20.04 LTS equipped with PHP version 7 or later and MySQL database version 8 or later. Below is a summary of messages flowing in the ecosystem and the cloud:

Message ID	Source	Destination	Value	Topic (MQTT ONLY)	Purpose
1	Sensor 1	Flood Light 1	0	sensor1	To turn off the flood light upon object exit of detection area
2	Sensor 2	Flood Light 2	0	sensor2	To turn off the flood light upon object exit of detection area
3	Sensor 3	Flood Light 3	0	sensor3	To turn off the flood light upon object exit of detection area
4	Sensor 4	Flood Light 4	0	sensor4	To turn off the flood light upon object exit of detection area
5	Sensor 5	Flood Light 5	0	sensor5	To turn off the flood light upon object exit of detection area
6	Sensor 6	Flood Light 6	0	sensor6	To turn off the flood light upon object exit of detection area
7	Sensor 7	Flood Light 7	0	sensor7	To turn off the flood light upon object exit of detection area
8	Sensor 8	Flood Light 8	0	sensor8	To turn off the flood light upon object exit of detection area
9	Sensor 1	Flood Light 1	1	sensor1	To turn on the flood light upon object detection
10	Sensor 2	Flood Light 2	1	sensor2	To turn on the flood light upon object detection
11	Sensor 3	Flood Light 3	1	sensor3	To turn on the flood light upon object detection
12	Sensor 4	Flood Light 4	1	sensor4	To turn on the flood light upon object detection
13	Sensor 5	Flood Light 5	1	sensor5	To turn on the flood light upon object detection
14	Sensor 6	Flood Light 6	1	sensor6	To turn on the flood light upon object detection
15	Sensor 7	Flood Light 7	1	sensor7	To turn on the flood light upon object detection

16	Sensor 8	Flood Light 8	1	sensor8	To turn on the flood light upon object detection
17	NFC Reader	Security Device	0	gate	Upon use of card with no access permission
18	NFC Reader	Security Device	1	gate	Upon use of card with access permission
19	Security Device	Cloud Key device	0	guard	Upon disarming the system, to relay information to the cloud
20	Security Device	Cloud Key device	1	guard	Upon arming the system, to relay information to the cloud
21	Security Device	Sound Alarm	0	siren	To deactivate the siren
22	Security Device	Sound Alarm	1	siren	To activate the siren
23	Cloud Key device	Cloud server	s1=0	N/A (over http protocol)	to relay to the cloud that the system is trying to turn off the flood light upon object exit of detection area
24	Cloud Key device	Cloud server	s2=0	N/A (over http protocol)	to relay to the cloud that the system is trying to turn off the flood light upon object exit of detection area
25	Cloud Key device	Cloud server	s3=0	N/A (over http protocol)	to relay to the cloud that the system is trying to turn off the flood light upon object exit of detection area
26	Cloud Key device	Cloud server	s4=0	N/A (over http protocol)	to relay to the cloud that the system is trying to turn off the flood light upon object exit of detection area
27	Cloud Key device	Cloud server	s5=0	N/A (over http protocol)	to relay to the cloud that the system is trying to turn off the flood light upon object exit of detection area
28	Cloud Key device	Cloud server	s6=0	N/A (over http protocol)	to relay to the cloud that the system is trying to turn off the flood light upon object exit of detection area
29	Cloud Key device	Cloud server	s7=0	N/A (over http protocol)	to relay to the cloud that the system is trying to turn off the flood light upon object exit of detection area
30	Cloud Key device	Cloud server	s8=0	N/A (over http protocol)	to relay to the cloud that the system is trying to turn off the flood light upon object exit of detection area

31	Cloud Key device	Cloud server	s1=1	N/A (over http protocol)	to relay to the cloud that the system is trying to turn on the flood light upon object detection
32	Cloud Key device	Cloud server	s2=1	N/A (over http protocol)	to relay to the cloud that the system is trying to turn on the flood light upon object detection
33	Cloud Key device	Cloud server	s3=1	N/A (over http protocol)	to relay to the cloud that the system is trying to turn on the flood light upon object detection
34	Cloud Key device	Cloud server	s4=1	N/A (over http protocol)	to relay to the cloud that the system is trying to turn on the flood light upon object detection
35	Cloud Key device	Cloud server	s5=1	N/A (over http protocol)	to relay to the cloud that the system is trying to turn on the flood light upon object detection
36	Cloud Key device	Cloud server	s6=1	N/A (over http protocol)	to relay to the cloud that the system is trying to turn on the flood light upon object detection
37	Cloud Key device	Cloud server	s7=1	N/A (over http protocol)	to relay to the cloud that the system is trying to turn on the flood light upon object detection
38	Cloud Key device	Cloud server	s8=1	N/A (over http protocol)	to relay to the cloud that the system is trying to turn on the flood light upon object detection
39	Cloud Key device	Cloud server	ge=0	N/A (over http protocol)	to relay to the cloud that the system is sending a message upon use of card with no access permission
40	Cloud Key device	Cloud server	ge=1	N/A (over http protocol)	to relay to the cloud that the system is sending a message upon use of card with access permission
41	Cloud Key device	Cloud server	a=0	N/A (over http protocol)	to relay to the cloud that the system is sending a message upon disarming the system
42	Cloud Key device	Cloud server	a=1	N/A (over http protocol)	to relay to the cloud that the system is sending a message Upon arming the system
43	Cloud Key device	Cloud server	v=0	N/A (over http protocol)	to relay to the cloud that the system is trying to deactivate the siren

44	Cloud Key device	Cloud server	v=1	N/A (over http protocol)	to relay to the cloud that the system is trying to activate the siren
45	Cloud server	homeowner mobile	Alert: Intrusion detected	N/A (over smtp protocol)	To inform homeowner about a security incident

3.4 Communications Interfaces

3.4.1 Communication Standards

The Smart Home Security System shall use the following standards in the ecosystem:

- MQTT (v3.1.1 or later)
- HTTP (v1.1)

3.4.2 Message Formatting

The messages shall not contain any spaces. Messages should be as short as possible to decrease time-on-air, processing, and power.

3.4.3 Communication Security

Messages sent through MQTT should be encrypted through the protocol itself using the same username and password for all devices. The cloud dashboard communication encryption is not needed as the cloud will not be programmed to have the capability to issue any command that may jeopardize home security.

3.4.4 Synchronization Mechanism

The ecosystem shall depend on a reliable internet to relay the status in real-time. Any internet outage will hinder the synchronization between the ecosystem and the cloud. The ecosystem itself shall not be affected by internet outages as it uses MQTT protocol to send and receive messages that does not rely on the internet.

4. System Features

4.1 Checking the security system status remotely

4.1.1 User Story

As a homeowner, I want to check the security system status remotely, so that I can leverage smart home capabilities

4.1.2 Description and Priority

The Smart Home Security System allows users to remotely check the security system status using their mobile device or a computer. This feature enables the user to determine if the security system is armed or disarmed and if any intrusion has taken place, providing real-time statistical information.

4.1.3 Stimulus/Response Sequences

1. The homeowner opens the cloud dashboard's websites and access security system status functionality.
2. The website generates the status of the security system by collecting database information.
3. The server checks the security system status and sends a response to the homeowner's browser.
4. The browser shows the current state of the security system on the homeowner's device.

4.1.4 Functional Requirements

- Request for Security System Status: The user's browser must send a request to the server for the current security system status.
- Retrieve Security System Status: The server must retrieve the current security system status from the security system database.
- Response to Request: The server must send the current security system status to the user's browser.
- Display Security System Status: The user's browser must display the current security system status to the user.

4.2 Receiving Notification in Case of Intrusion

4.2.1 User Story

As a homeowner, I want to receive notification in case of intrusion, so that I can catch the thief before he runs away

4.2.2 Description and Priority

The Smart Home Security System allows the homeowner to receive email notifications in case of an intrusion in their home. This feature provides the homeowner with immediate information of any potential security intrusion to act accordingly.

4.2.3 Stimulus/Response Sequences

1. Upon the security system detection of an intrusion, the cloud module will get notified of such incident by the security ecosystem.
2. The server then generates an email notification and sends it to the homeowner's email address.

4.2.4 Functional Requirements:

- Intrusion Detection: The security system must be able to detect an intrusion and send an alert to the server.
- Send Email Notification: The server must send the email notification to the homeowner's email address.

4.3 Alarm system shall not be triggered by authorized access

4.3.1 User Story

As a homeowner, I want to enter my home without triggering the alarm, so that I can enter my home without getting arrested by police by mistake

4.3.2 Description and Priority

The alarm system is disarmed in case of homeowner entering the house using the NFC tag. While the alarm should still be active in case of unauthorized access where an intruder is trying to get inside of the house. This feature has high priority, since it is extremely crucial for the system not to have false positive intrusion detection.

4.3.3 Stimulus/Response Sequences

1- The homeowner uses his NFC tag to enter the house.
2- The Security Device checks the tag and confirms the identity and authorization of the person.
3- After successfully identifying the homeowner, the alarm system will not be triggered upon entry.
4- Record of entry will be stored and may be displayed in the cloud dashboard.

Alternate scenario:

1. An intruder breaks into the homeowner's home.
2. The Smart Home Security System detected the opening of the door without a valid NFC card.
3. The Security Device sends a command to the Sound Alarm.
4. The Sound Alarm activates the siren.
5. Record of intrusion will be stored and may be displayed in the cloud dashboard.

4.3.4 Functional Requirements:

- The alarm must turn on during unauthorized access.
- The system should recognize the homeowner and disarm the system.

4.4 Deterring thieves by triggering lights upon sensor's object movement detection

4.4.1 User Story

As a homeowner, I want to have my home's perimeter to have sensors, so that I can have my outdoor lights turn-on automatically to deter thieves.

4.4.2 Description and Priority

This feature combines the light with ultrasonic sensors to detect suspicious movements and to turn on the flood light to deter thieves in case of the sensor detecting a moving object and record these data in the cloud to be displayed in the dashboard.

4.4.3 Stimulus/Response Sequences

1- An object moving along the house outside perimeter.
2- The Sensor will detect this movement.
3- The Flood Light will be turned on.
4- The location of the activated sensor/flood light will be recorded in the cloud.

4.4.4 Functional Requirements:

- The lights should turn on in case a sensor detects any movements.

4.5 Guarding the home from thieves' intrusion

4.5.1 User Story

As a homeowner, I want to guard the home from thieves' intrusion, so that I can feel safe

4.5.2 Description and Priority

Guarding the home from the intrusion feature is a crucial component of the smart home security system and its main objective to detect any unauthorized intrusion into the homeowner's premises and to provide a rapid response to prevent the intruder and notify the owner. The function must be reliable, user-friendly and offer homeowner a sense of security

4.5.3 Response Sequence

When system is armed, guarding home from intrusion function is activated, the following response sequence should occur:

1. Detection: This Feature must be used with sensors like door and window sensors, motion detectors to detect unauthorized entry into the home.
2. Alert: The system must notify the owner via email immediately that an invasion has been detected.
3. Deterrence: The system must have a siren alarm that sounds immediately when detection of intrusion to prevent the intrusion.
4. Action: The system must be able to take appropriate action to stop intrusions, such as lighting activation.

4.5.4 Functional Requirements

The feature guard the home from the intrusion should include the following functional requirements:

- Multiple Sensors: The system must use sensors to detect any illegal entry, including door and window sensors, motion detectors and other smart home sensors.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

The safety against home intrusion function must also meet the following non-functional requirements:

- Reliability: The system must be exceptionally reliable and capable of detecting intruders accurately and consistently.
- Performance: The system must respond quickly to requests for the security system status within 2 seconds.
- Compatibility: The cloud dashboard minimal and simplistic look should be compatible with a range of mobile and desktop browsers that are considered mainstream such as Chrome and Firefox.
- The ultrasonic sensor must work continuously to sense movements.

5.2 Safety Requirements

The ecosystem devices shall use electrical plugs with a grounding pin connected to the home's grounding rod to avoid electrical shocks.

5.3 Security Requirements

5.3.1 Privacy

The logs shall not be accessible by any unauthorized entity. However, in case of legal order by a court within Saudi Arabia relating to national security incident, the logs shall be released to the government. In case of unauthorized access to the logs, the homeowner shall be notified within 60 business days from when the incident was recognized by the cloud custodian; the Saudi Computer Emergency Response Team (CERT) shall be notified within 48 hours (2 days) from when the incident was recognized by the cloud custodian.

5.3.2 Authentication And Encryption Requirements

- The system shall rely on MQTT authentication and encryption and shall not implement encryption module by itself.
- The ecosystem relies on MQTT authentication mechanism using a unified username and password.
- The NFC Card Reader must detect the correct NFC Card Tag without delay.
- The system will have 3 seconds delay between trails in the keypad.
- The system will allow 3 trials of password before it alerts and locks for 15 minutes.

5.4 Software Quality Attributes

The programmers shall write a code that is readable to ensure maintainability. Also, the programmers shall have the cloud dashboard as simple as possible to maintain compatibility with a range of mainstream browsers. The ecosystem must have certain features enabled or used so that it ensures high availability and reliability whenever possible.

5.5 Business Rules

The ecosystem has only a single role which is the “homeowner”. However, there are two functionalities associated with the homeowner’s state such as whether the homeowner is interacting with the ecosystem physically or viewing statistics remotely.

6. Other Requirements

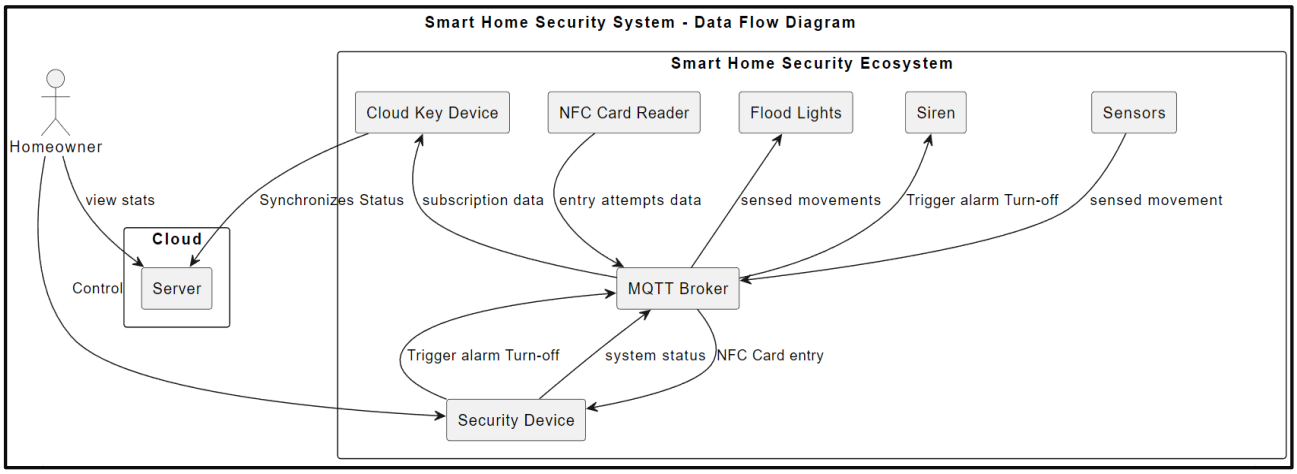
- User-friendly: System must be easy to use and configure with clear instructions and user-friendly interfaces.
- User Interface: The cloud dashboard shall have a simple interface without any complex UI or sophisticated graphics.
- Email Content: The email notification must contain clear information about the intrusion, such as the time of the breach.

Appendix A: Glossary

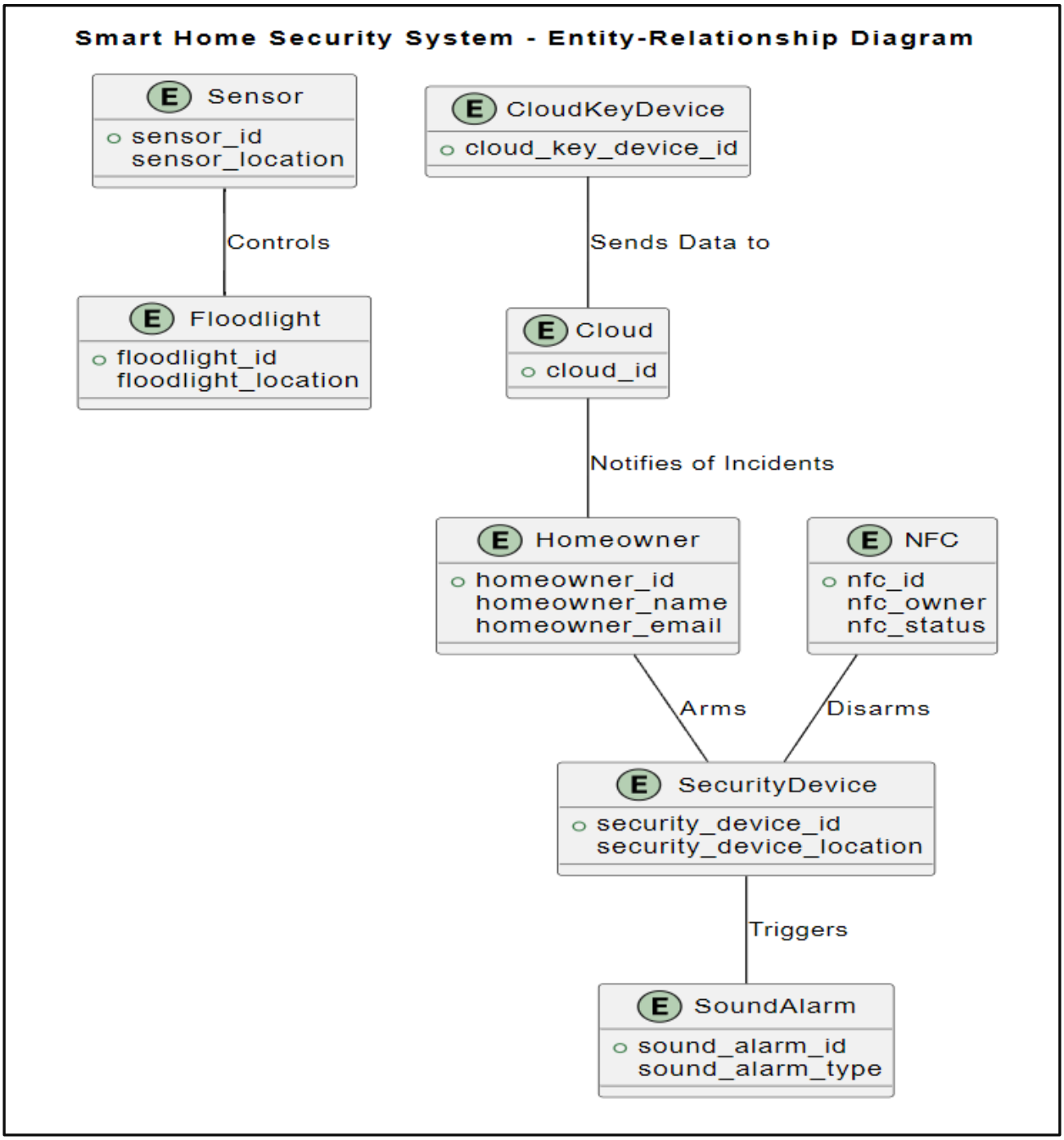
SRS: Software Requirements Specification
UI: User interface
CERT: Computer Emergency Response Team
Email: Electronic mail
MQTT: Message Queue Telemetry Transport
NFC: Near-Field communications
HTTP: Hypertext Transfer Protocol
SMTP: Simple Mail Transfer protocol
LTS: Long term support version
SQL: Structured Query language
MySQL: Relational Database Management System
GUI: Graphical User Interface
UPS: Uninterrupted Power Supply
PDF: Portable Document Format
PHP: Personal Home Page Tools, PHP: Hypertext Preprocessor

Appendix B: Analysis Models

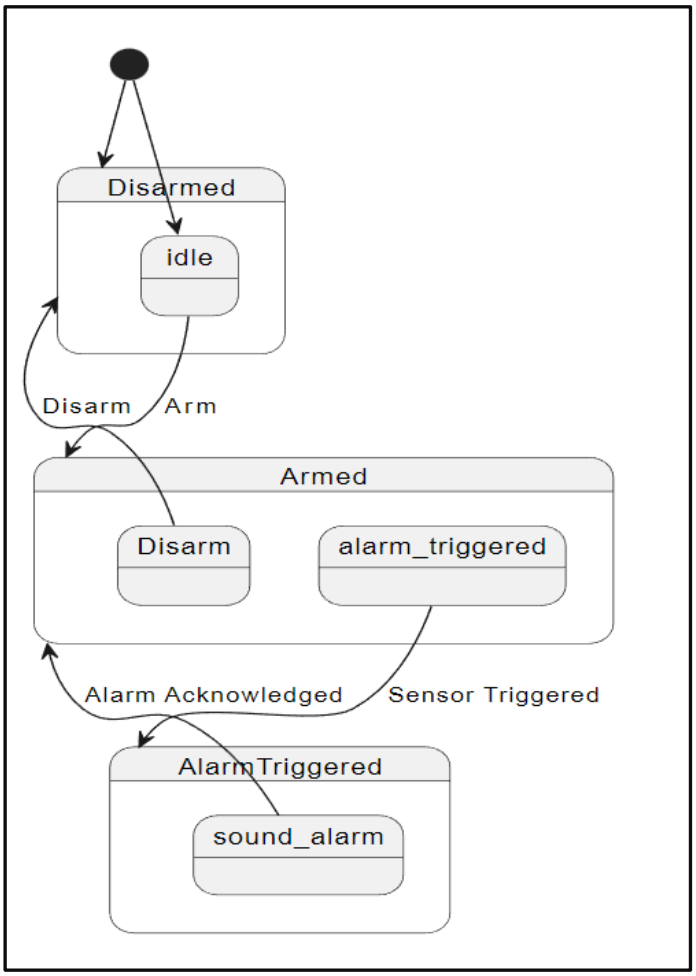
Data Flow Diagram:



Entity Relationship Diagram:



State-Transition Diagram:



Appendix C: To Be Determined List

To be determined.