University of Waterloo

ECE 355 - Software Engineering

**Software Requirements Specification**

Group 3 Security System

Group 3

Ayush Gupta, 20292953

Ankit Srivastava, 20298545

Usman Khan, 20266360

# Executive Summary

This document contains the requirement specification for the Group 3 Security System. This document details the requirements that were set forth by the customer. The authors of this document have been tasked with creating a proof-of-concept of a next-generation security system. The authors have the responsibility of gathering all necessary and relevant requirements. These requirements will be used in the next phase to create a design document. Finally, this document and the future design document will be used to implement that proof-of-concept requested by the customer.

This document takes the information acquired through the requirement elicitation process and presents them in a form that both the developers and customers can use in the subsequent stages of the software development process. The bulk of this document pertains to the functional requirements of the security system. These functional requirements are broken down into scenarios, use case model, object model, dynamic model and interfaces. These sections together fully describe the functional aspects of the software gathered through requirements elicitation. The following section concerns the non-functional requirements such as performance, scalability and usability. The last section of this document discusses the user interfaces of the security system. Together, all these sections represent the information gathered through the requirements elicitation process and fully describe the system to be designed in the next pahse.

# Purpose

The purpose of this Software Requirements Specification (SRS) is to address various issues from, functionality, to external interfaces, to design constraints and more of the Group 3 Security System. This SRS will serve as the complete description of the Group 3 Security System. This document is broken into four distinct sections. This first section serves as the introduction and provides the basic background knowledge and details necessary for the subsequent sections. The second section discusses the functional requirements of this software. The third section in-turn discusses the non-functional requirements. Finally, the last section is dedicated to a discussion of the user interfaces. Certain sections such as the functional requirements are broken down further into subsection to better aide in the presentation of the materials.

The audience of this SRS are all the stakeholders of this project. Thus, the audience includes the customers who have requested this system and provided the bulk of the requirements, the team responsible for analyzing, designing and implementing the system, and the consulting firm which employs the team working on this project. All of the above stakeholders benefit for a SRS that thoroughly details all the necessary software requirements. Specifically, the SRS gives the customer confidence that their requirements have been properly understood. For the team working on the Group 3 Security System, it is as an important exercise in collecting all the relevant requirements and also serves as the basis for the design and implementation phases later on in the project life cycle. For the consulting firm, this SRS serves as documentation of the work performed by the team and creates a written record of the requirements communicated by the customer.

# Objectives

This group has been tasked with designing, implementing and demonstrating proof-of-concept of a next-generation home security system. The system will contain several features that are not present in current-day implementations of home security systems. The goal of the system is to use the latest technology, such as wireless communication and GPS, for home monitoring and management. The customer has provided three areas of focus for the system: physical security, green energy management and family safety. In addition to the control panel present in most conventional home security systems today, the system will also need to interface with smartphones to give users greater freedom and accessibility in managing their security system.

The customer has laid out several objectives that need to be satisfied regarding the home security system. The physical security subsystem should be able to reliably detect and act on safety threats, such as intruders, when the system is armed. The physical system needs to be able to notify the relevant parties if warranted. For instance, if a flood is detected, a home owner needs to be alerted via an emergency notification through both the central console and the owner's smartphone. The user of the home security system should also be able to easily access data streams generated by cameras. They should be able to view these streams either locally or through a web server. The criterion for evaluation of this requirement is a working security system that is able to successfully detect unsafe conditions while at the same time, minimizing the number of false-positive alarms.

The green energy management subsystem is to monitor and manage a wide range of household appliances and systems that affect the local environment. The system should be able to manage HVAC systems, interior and exterior lighting and other appliances with the goal of maintaining a comfortable and safe environment for the residents of the home. The criterion for evaluation for this requirement would be to be whether the system is able to influence environment and follow a set of pre-defined set of parameters.

The family safety subsystem should be able to monitor and ensure the well-being of individual family members. This subsystem should be able to adapt to the living patterns of a wide range of individuals and react accordingly. For instance, the family safety subsystem could be used to detect whether an elderly member of the household has fallen and call for help if required. At the same time, the system could be used to track the whereabouts of a younger member of the family via a GPS bracelet. The criterion for evaluation for this requirement would be whether the system is able to successfully detect falls, track users via GPS and successfully monitor their day-to-day habits.

The customer has also requested that the system continuously log all activity and make these logs available for review by the user. The logs will be responsible for tracking everything from intrusion detection events to battery low status on monitoring equipment. The criterion for evaluating this requirement is whether the system generates a detailed log of all events that is accessible to the user. The log needs to capture all the activity and actions managed by the system.

Redundancy and fail-safes need to be built into the system, especially for the physical security subsystem. These redundancies need to ensure that a single fault does not bring the entire system down. The system should be able to gracefully handle a wide variety of unexpected events. For instance, if a malicious entity has disabled the land lines to the home, the system should be able to fall back on a built-in GSM module to still alert the home owner and the proper authorities. The system should be able to handle a power outage by falling back on battery power if necessary. The system should be able to deal with a fault in a sensor. This fault could be anything from low battery, to problem with the hardware, to intentional interference by an intruder. The criterion for evaluation for this requirement would be whether the system is able to smoothly transition from the power grid to a backup battery, and how well the system deals with interference caused by faulty hardware or malicious entities.

# Scope

Due to time and resource constraints, the first iteration of this next-generation home security system will focus on one of the three subsystems. Specifically, the team will focus on the physical security aspect of the system. This limitation in scope of the project is due to the fact that it is not possible to dedicate resources to all the subsystems. Each subsystem requires a significant resource investment that just is not available to this team at the moment. As such the team will focus its efforts on the physical security subsystem. However, even with the focus on physical security, the system will be designed that additional subsystems should be easy to add and not require a great deal of work. The system will emphasize extensibility and modularity to adding additional subsystems in the future easy.

The focus on physical security obviously means that there will be problems in the other two subsystems that will not get resolved. Even within the physical security subsystem, there will be aspects which have a greater emphasis put on them compared to others. For example, the team will work towards integrating smartphones into the system, and thus may not have time to implement as wide a variety of sensor types as possible. The extendible nature of the system should help in alleviating some of these issues by making it easy to add additional sensor types in the future.

# Terminology and Definitions

**QT**: Cross-platform application framework developed by Nokia for developing application software and graphical user interfaces.

**GUI**: Graphical user interface

**GSM**: Global System for Mobile Communications

# Functional Requirements

## High-level Functionality

The following home security system provides the client with a complete security solution. It not only monitors the activities inside the house once it’s turned on but also monitors all vulnerable entry points to the house, thus preventing any break ins.  
The system itself is comprised of Magnetic door/window sensor, and an IR sensor for motion detection. These combined together detect whether there is a forced break-in through a window or a door. It further detects the movement inside the house to verify that the theive has actually entered the house. The Camera sensors on the other hand automatically move towards the point where a movement has been detected. At this point in time, a call is made by the Central Control Unit to the house owner allowing him to see a live view of the house using the security cameras installed. Also, in case of a false alarm he has the full authority to de-activate the system.  
Apart from the following sensors the security system also consists of natural disaster, fire and gas leak sensors. These sensors detect whether a fire or a gas leak has taken place. In case of such a situation, the appropriate quick response body is contacted while also contacting the house owner.

## Scenarios

A home alarm system is in place in order to detect unwanted intrusion into a house. It plays an important role in protecting the house and all your valuables in it. The system should be active all times and should monitor break-ins and thefts even when you are sleeping.

Some major scenarios have been discussed in this section of the report, allowing us to analyze how the system would work in different environments.

### During a Day/Night Theft

Overview- During this scenario we have assumed that the home residents are either out of the house for a vacation or work or in the house and sleeping. We also assume that all doors and windows have been closed for the system to trigger.

In the following scenario we assume that a burglary takes place and the burglar tries to enter the house by using forced methods of entry like breaking a window or by breaking a lock on the door.

Actors participating- The client/home owner, the intruder, emergency response team(police) and the central control server.

System Response- The magnetic proximity door or window sensors will be installed in order to measure such forced entries into the house. In case a burglar tries to break a window and get into the house the alarm will get triggered. This event in turn triggers a chain of events. Firstly and foremost it will inform the user that an intrusion has occurred and send a live feed to the user. It will wait for 5 minutes for the user to respond back saying its false alarm, otherwise a message to the police would be sent giving them details of the burglary and the location of the house. Moreover the siren will also start.

### During a Pet Movement/Intrusion

Overview – During this scenario we make certain assumptions, which include, the owner of house leaving his pet alone in the house while activating the home alarm system. This causes a situation where the alarm system needs to detect the pet and distinguish it from a burglar.

Assumption: All the cameras are working in conjunction with the motion sensors.

Actors participating- The pet & the central control server

System Response- During such a scenario the motion sensors and the cameras will pick up movement of the pet and transmit it to the central server. The server should be intelligent enough to carry out image detection and manipulation, allowing it to differentiate between burglars and pets causing movement. Also if the owner equips the system with an image of its pet then the central server should be able to distinguish the pet from any stray animal which may have had entered the premises causing the alarm to trigger. Thus, the server won’t trigger an alarm.

### During a Fire or Flood

Overview- This scenario can be caused by natural events like flood or earthquake. We assume the owner of the house has activated the house alarm when a fire or a natural disaster takes place. In case of a fire the system an immediate message should be sent to the fire department, asking for assistance.

Actors participating- The client/home owner, emergency response or medical aid team and the central control unit

System Response- During this scenario the system gets an input from the flood response sensors or the fire alarm. On receiving the input, it does the following things. It firstly informs the appropriate emergency response team and asks for assistance. Then it calls the owner allowing him to remotely see the condition of the house and determine if the alarm is valid. If the alarm is not valid then the user can disalarm the system as well.

### False Alarms Due to Non-Predictable or Natural Events

Overview- For the following scenario we assume that a false alarm is activated due to any of the following events like, breaking of a window by high speed winds or an unwanted pet entering the house. Such scenarios will trigger the alarm system, but they don’t act as actual threats to the house.

Actors participating- The client/home owner and the central control unit

System response – In case of such events, the sensors should perform exactly as they would in case of a burglary. But the central control unit should be able to analyse the situation and state whether there is an actual theft or not. Also the video of the incident should be relayed to the house owner, telling him about the accident which took place and making sure that it is not really a theft which is taking place.

### Low Battery Indication in the Sensors

Overview- During this scenario we assume that the owner has activated the alarm but one of the sensors is running out of battery. Such a scenario would not allow the system to be very efficient therefore it’s important to inform the home owner about the following situation.

Actors participating- The client/home owner and the central control unit

System response- In such an event, the sensor should tell the central control unit that it is running out of battery. The central control unit should in turn message the client on his cellphone that the system is not performing efficiently due to a low battery on one of the sensors and in order for it to continue to perform efficiently the battery must be replaced.

## Use Case Model

The following diagram illustrates the use case model for when the home owner is about to alarm and disalarm the system.

Figure 1 Use Case Model for Authenticating Login

Alarm System: Initially to start the system the user needs to alarm the system. This sequence could be done when the user is leaving the house or in night.

DisAlarm System: This is the use case when the user returns back and disalarms the system or disalarms it remotely. After activation of a sensor due to user’s entry he will have 1 minute to disalarm it.

Thus, in the above both the use cases the primary actor is the home owner. The goal here is to activate or deactivate the alarm. This could be done via the GUI panel on the central server or using the phone. If the phone is used, the phone establishes an encrypted communication system and in turn sends commands to the central server.

Both of these use cases include the Login Authentication use case and would lead to that. This is entered whenever the home owner needs to make a change to the security system state. It is assumed that the user set a password during the installation and the user needs to enter this password which will let him access the security system. Once the system is authenticated, the user can then perform the above 2 use cases of alaraming/disalarming the system.

The following diagram shows the use case model of activation of sensors which could trigger the alarm.

Figure 2 Use Case Model of Sensor Activation

Pet Moves: The primary actor here is the pet. Motion of the pet when the system is alarmed could trigger the motion sensor of that room.

Burglar Breaks In: The primary actor here is the burglar or the intruder. The existence of the burglar is identified if the system if alarmed. The burglar can trigger either the motion sensor alarm or the magnetic proximity alarm.

Activates Motion Sensor: Activation of the motion sensor could be due to motion in a specific room. This situation is entered when the pet or burglar moves in a room. The assumption made is that the motion sensor is activated and working properly. This would in turn activate the imaging and video recording of that room via the cameras. These camera images are then sent to the central server.

Central Server Analyses Images: This use case is triggered when the motion sensor of a room is activated. In this use case the central server analyses the images and checks them with pre-stored images and algorithms to distinguish between the pet or the burglar. Thus, two things can happen here

Pet Detected – If this happens then the system ignores the camera warnings and doesn’t trigger any alarm.

Other Movement Detected: If any other kind of movement is detected then the alarm is triggered

Activates Magnetic Sensor: The primary actor here is the burglar. Activation of the magnetic would happen if:

Burglar tries to force his way through an alarmed window or door

External wind tries to open the door.

In either case, the alarm needs to be triggered as one of the doors and windows are now open.

Central Server Trigger Alarms: This use case is entered if the motion analysis of the camera images shows intruder or magnetic sensor goes off. This would in turn start many actions. This will activate the siren, encrypt a warning and images and videos of house to be sent to the home owner. This would also trigger the mechanism of reporting the emergency services.

Siren Activated: The siren activation will happen once the alarm is triggered. The goal here is to tell the neighbours that a breach has occurred. This will help them coming to the house for help. Another assumption is that listening to the sound; the intruders will actually leave the house.

Emergency Team Reported: After the triggering of the alarm the central server will inform the emergency teams about the breach. The main actors are the emergency response personnel which include fire department and the cops. This will end with a phone to these teams and the assumption is they will arrive on scene in time to stop the intrusion.

Encrypt Message and Informing Home Owner: The message from central server including a warning and video feed of the house will be encrypted using the RSA key setup during initial installation. This message will relayed via GSM and 3G signal to the home owner. Thus, the home is primary actor for these systems. The assumption is that the home owner can take immedictae action like returning to home or informing someone nearby of the intrusion and will also have a copy of the video feed as proof against the burglars.

## Object Model



Figure 3 Overall system class diagram

Figure 3 above shows the overall structure of the security system. The diagram shows how the different components are related to each other. The diagram is representative of the way in which the system would be installed in a user’s home. A wide variety of sensors would be installed throughout a user’s home. All these sensors would communicate wirelessly to a central control unit. The central control unit would be responsible for converting the objected oriented model of the security system into physical control signals via control unit bridge. This central control unit would ideally be installed in a secure location in the house. In order to increase redundancy, several central control units could be used, with each unit responsible for a set of sensors. This would make it more difficult for an intruder to interfere or disable the control unit. The security system would be where all the logic of the system would be implemented. It would also be the part of the system that the user would interact with through a control panel. The user would also be able to interact with the system through a mobile app available on their smartphone.



Figure 4 Detailed SecuritySystem class diagram

Figure 4 above shows a more detailed view of the security system and its composition. The security system would consist of 1 or more zones. These zones represent the abstraction of a physical region in space. A zone could be anything from a single room to and entire house. Each zone would be composed of 1 or more sensors. The collection of sensors would be responsible for monitoring and managing the zone to which they belonged.



Figure 5 Sensor class diagram

Figure 5 above shows the hierarchy of the sensors with the security system. Each subclass contains the sensor type-specific implementation. The proposed hierarchy would enable users to easily add additional sensors. For the developers the above hierarchy means they would be able to quickly support new sensors as they became available. This new sensor type implementation could be pushed out to customers via an update allowing them to be able to add the new sensor type to their existing system. This setup increases the system’s extensibility and allows it to adapt to changes in technology and security.



Figure 6 Objects associated with arming the system

Figure 6 shows the objects that would be used when the user interacts with the security system. The control panel would be responsible for all the user facing features such as getting user input, displaying status information and error messages. The control panel would be the unit that the user would use to arm and disarm the system. When arming, the user would have to ensure that the system is in a valid state (i.e. windows and doors are closed) before the system arm countdown would begin. An error message will be displayed if the security system is not in a valid state. Once the correct security code is entered, the zone(s) to be armed are selected and the system is in a valid state, the user will have 30 seconds to exit the zone before the system becomes armed.



Figure 7 Objects associated with intruder detection

Figure 6 above shows the objects involved in the detection of an intruder. Specifically in the above diagram, a magnetic sensor is being triggered by the opening of a window when the system is in the armed state. The sensor sends a signal to the central control unit which processes the event. Event processing involves parsing the data being sent and identifying the sensor that is sending the event. This data is then passed on to the security system via the control unit bridge, which has been excluded from the above diagram. The event is interpreted be the security system to check whether the event is valid and what actions if any need to be taken. The set of actions to be executed in the case of a valid intruder event are defined by the user. Pre-defined actions can include, activating a siren to scare the intruder away, enabling cameras to track the situation and communicating with external stakeholders, such as the home owner and the security company.



Figure 8 Objects associated with communicating with external stakeholder

Figure 8 shows how the security system communicates with external stakeholders. These external stakeholders can be the user’s smartphone with the mobile security app or the security company responsible for monitoring the home.



Figure 9 Objects associated with arming the system through the mobile app

Figure 9 shows the objects in the use case where the user is arming the system through the mobile app. Similar to the security system installed at the user’s home the mobile control panel is responsible for managing all user interaction with the system through the mobile app. The mobile control panel receives user input telling the system to arm itself. The mobile security system constructs a message containing the instruction to arm the system. The data is encrypted to ensure that no third party is able to interfere. The security system receives the message containing the instructions to arm the system and proceeds as if the instruction was received from the local control panel.



Figure 10 Objects associated with installing a new sensor

Figure 10 shows the objects involved when installing a new sensor into an existing security system. The process of installing additional sensors to the security system could be carried out by either a security company technician or the user. Once the sensor is installed, it is configured in the central control unit so that the control unit is able to identify the sensor when the sensor transmits data to it. The user or technician also needs to make the security system aware of the new sensor. To do this that user or technician uses the control panel to add the new sensor, specifying the sensor type and to which location it belongs.

## Dynamic Model

Figure 11 Sequence diagram showing dynamic behavior when arming the system

Figure 11 above is a sequence diagram depicting the dynamic behaviour of the objects involved in arming the system. The actor in this case is the home owner who wishes to arm the system before they leave their home. The home owner uses the control panel to enter the security code and the specify zones they wish to arm. The control panel verifies the security code and then asks the user for which zones they wish to arm. This user’s instructions are sent to the security system were the system state is checked before the necessary zones are armed.

Figure 12 Sequence diagram showing dynamic behavior when an intruder is detected

The diagram illustrates how control moves from the sensor, to the central control unit, to security system via the bridge, finally resulting in the activation of the siren. While only the activation of the siren is shown as the result of an intruder detection event, the system is able to take other actions as well, such as contacting the home owner or the security company. The sequence diagram is limited to activating the siren in order to make the diagram easier to follow.

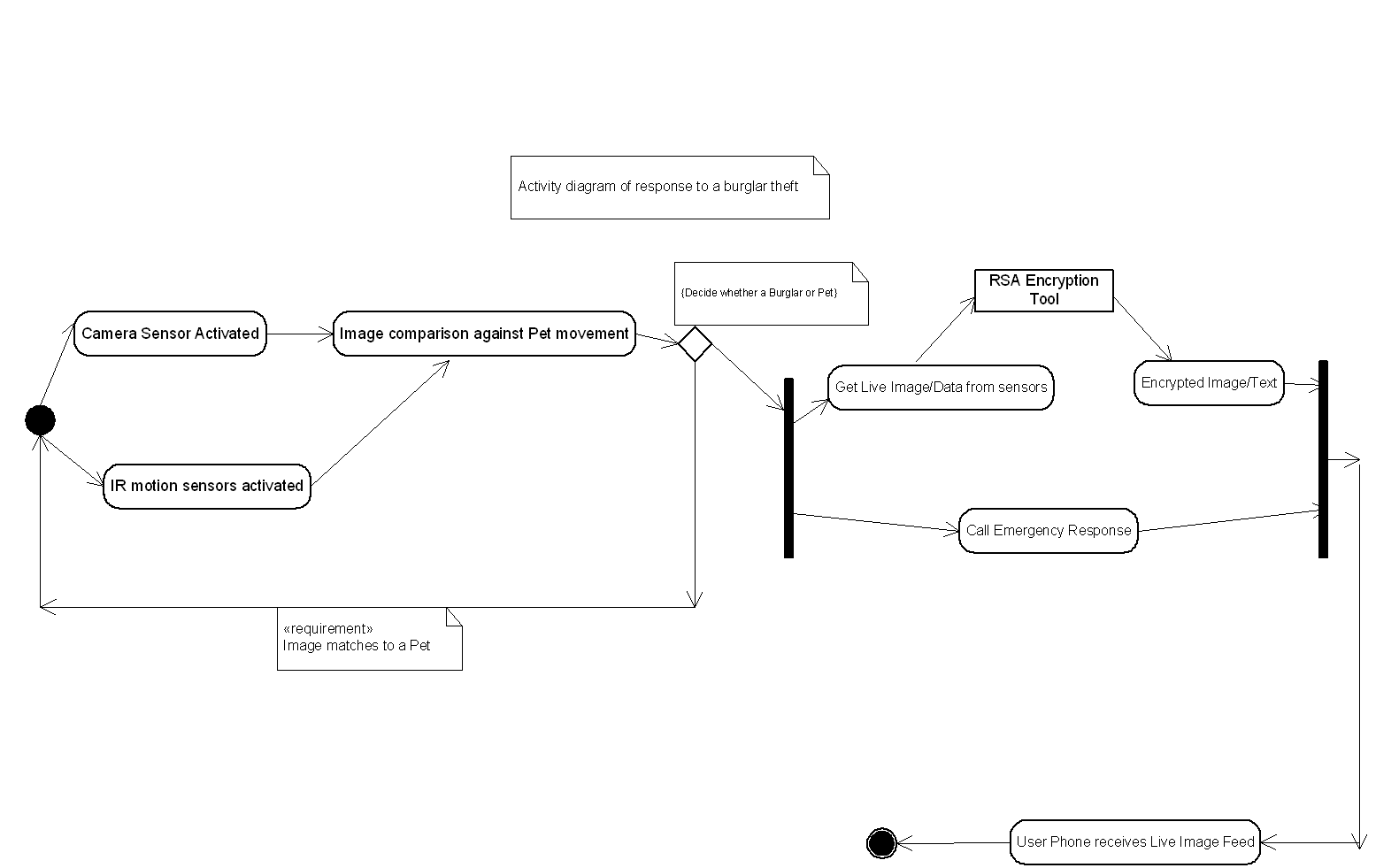


Figure 13 Activity diagram of response to a burglar

Figure 13 shows an activity diagram also depicting the detection of an intruder. The diagram shows the activities and actions of the system in response to the detection of an intruder.

## Interfaces

The system has a centralized server known as the Central Control unit. This Central Control Unit not only analyses images using complex imaging algorithm but also communicates with the client’s phone. But before establishing this communication with an external device like the clients phone, it RSA encrypts the data and then establishes a secure communication channel in order to transmit this data over to the phone.

For the prototype we aim to make an android app with its user interface developed in QT. The QT lib. Is a cross platform library which would allow us to have a common user interface between the centralized control unit and the android mobile app. The communication between the centralized control unit and the mobile app will in turn take place using GSM and 3G data transmission thus allowing the user to receive a live feed from the security cameras. The client on the other hand would have full authority to de-activate certain sensors or the complete home security system. The clients input to the Central Control unit would be send back in the form an encrypted query which would then be deciphered and interpreted by the centralized server. The Central Control Unit in-turn would communicate with the actual sensors using normal data packets. This would be the normal TCP/IP data packets with five flags, telling the system whether the sensor has acknowledged its response or not.   
Also, In case of an actual theft the Central Control unit will also inform the appropriate emergency response team about the situation. For this the system will either use a phone connection or if it fails to find a connection, then it will place a phone call using the GSM connection. On a successful connection it will play a pre-recorded message stating the address of the house and the scenario which is causing it to place a call to the emergency response team.

# Non-functional Requirements

Non-functional requirements lets us judge the operation of the home security system, while providing us with detailed system architecture. The requirements give us a detailed outlook of the qualities of the system. In this report certain execution and evolution qualities of the home security system have been specified.

**Accessibility:** The system should have restricted access, only allowing the home owner/client to disable or enable him, while any threat to the house should not be able to access the system in any way. The RSA encrypted interaction, which takes place between the Central Control Unit and the clients cell phone ensures secure and restricted access to the system.

**Availability:** The home security system needs to be available all the time while it’s active. The effectiveness of the system can only be measured with the amount of spontaneity the system shows to threats. Thus, tasks such as database upload to the system and re-booting the system for firmware updates should be kept to a minimum, while the system is active.

**Backup**: The system should be able to back–up all video and audio footage to a secure location in case of theft, since this can be crucial data, which can be used for prosecuting the criminals. Also regular back-ups to the central control unit can be made and the amount of data, which is stored on the server, can be determined according the clients wishes. The amount of data should not affect the speed or efficiency of the system itself.

**Efficiency**: The efficiency and response time of the home security system largely depends on the Central Control Unit. Since the control unit not only receives all inputs from sensors but also carries out complex imaging algorithmic analysis to detect whether the alarm was a false alarm caused by a pet or not. In case of theft situation it also gives a live feed of the cameras to the client, thus in order to carry out such work, highly efficient processors would be required. Although the system would only carry out database uploads and firmware updates when the system has not been enabled, giving it access to larger CPU cycles and memory, making it more efficient.

**Portability:** The system in general is not highly portable after all sensors have been installed, since in order to move the system from one house to another, the previously installed sensors would have to be taken off and re-installed. Although the Central Control Unit allows certain amount of portability at the client end but the physical sensor system is certainly not that portable. The client end can be configured to work with any smart phone, allowing it to remotely receive video feed from the cameras installed in the house. Also the client has full authority to disable and enable the system remotely. This certainly shows the high portability available at the client side of the system.

**Scalability:** The system in itself is highly scalable and more sensors and motion detectors can easily be added to the system. The system easily allows the client to add more rooms to the system as well, which in turn increases the scale of the system. The Central Unit uses a central database from which manipulation of data is done from, thus adding and deleting sensors is an easy task for the system too.

**Robustness:** Systems robustness can be measured by its ability to perform and respond in adverse conditions. For the following home security system, its ability to perform in conditions like no electricity and no phone coverage make it far more robust and effective than other security systems available. During scenarios when no power is available or power is cut-off in order to bring down the house alarm systems by the burglars, the system uses re-chargeable battery power to effectively run itself. Also in scenarios of loss of phone network, the system uses GSM in order to push notifications to the client. Thus we can certainly conclude that the system is highly robust in its actions.

**Usability**: The system is easy to install and not at all complex to use, thus allowing a common person to easily install and use it. Although while installation certain key concepts should be kept in mind for the system to function efficiently. The user must make sure that he/she uses a cell phone, which is accessible at all times to ensure that he or she is contacted immediately in case of an emergency. Also, for optimum performance, cameras need to be installed at locations, which allow view of prime locations such as front door, lockers or safes, etc.

**Legal Issues**: A legal disclaimer would be stated on each system and its packaging, not holding the developers liable for a theft if it somehow manages to occur. The system can only provide an assurance of a high security system but cannot guarantee a theft to not occur.

Thus the following parameters effectively describe the system architecture of the home security system, which we intend to build. This system in-turn would provide the client with a high end, very effective and usable home security system for their house.

# User Interfaces

As mentioned above the security system consists of individual security components and sensors mounted in different rooms and a central server which will be the master unit and has the capability of controlling and interacting with all the other individual components. The user can thus interact with the individual units or the central processing unit to control individual sensors.

In addition to this, the user could control each of the functionality of the central processing unit with his/her smartphone via GSM relay signals. Our app once downloaded on the smartphone can be integrated with the security system in presence of our security personnel. This will establish a secure connection between that particular smartphone by downloading the RSA keys from the system to the smartphone.

**Kinds of Interfaces:**

1. Individual Sensors:
   1. Motion Sensor

This sensor will have a disable button where the central processing unit will ignore the signals send from that particular motion sensor. This will enable the user to activate it again using the central processing unit or by his phone remotely.

* 1. Cameras

As with the motion sensor, the cameras will have an enable/disable button.

Each of the security cameras will also have internal memory to store image frames and video. The camera by default would start filming if the motion sensor in the room goes off. The film will be stored in the cameras hard drive and individual frames would be sent to the central unit to analyze what motion has occurred. In addition to this the camera will have a small numeric keypad attached to it which will enable the user to enter the frequency the camera should take a photograph of the room and send to central processing unit to analyze any motion in the room. This would help in case the motion sensor fails or has not been powered up. The time entered should be in minutes. There will be an option to toggle between just clicking images or storing a video feed for the user to look at later and specify how long the video should be stored for.

* 1. Magnetic Proximity - Door/Window Sensor:

The magnetic proximity sensor will be remotely controlled by the central processing unit. Thus this sensor will have no individual control attached to it.

* 1. Siren, Smoke Detector and Fire Alarm

These sensors will also have no user interface and will activate sound when detect smoke or fire, in case of smoke detector and fire alarm or the central processing  unit sends an alarm signal in case of siren.

1. Graphical Interface:

Both the Central Server and the Smartphone Application will have a Graphical Interface attached to them. This interface will let the user control monitoring of the entire house, monitoring of specific rooms or monitoring of specific sensors in the specific room.

The GUI will be divided in three basic configurations, toggling alarm, basic and advanced:

Workflow:

1. Initially the user will be approached with a welcome screen when he touches the touch pad panel on the central processing unit or opens up the application on the smartphone.

This will have a QWERTY keypad where a password would be required to access the main menu. The following figure shows this:

Figure 14 Welcome Screen

Main Menu:

Enter Password:

1. This would lead the user to the main menu screen which would tell the current status of the system to the user. Then the user would do one of the 3 following things:
   1. Toggle the Alarm/Disalarm configuration. If the system is alarmed, toggling this configuration will disalarm the system and vice versa. The red color indicates the system is alarmed, whereas the green color indicates the system is disalarmed.
   2. Access the basic configuration
   3. Access the advanced configuration

This could be done by touching the buttons on the screen. The following figure illustrates this:

Basic Configuration

Advanced Configuration

Disalarm – 100 %

System is currently Alarmed:

Figure 15 Main Menu

1. Disalarm/Alarm Configuration:

These are the following effects that will happen when the user presses the Disalarm/Alarm button on the main menu screen.

1. If the system is alarmed, then pressing this would disalarm the whole system and the color will change to green and the text would show Alarm.
2. If the system is disalarmed, then pressing this would alarm the whole system and the color will change to red and the text would show Disalarm.

This will let the user alarm/disalarm the whole system and thus would override the changes made in basic and advanced configurations. This option should be most widely used by the user to control the alarm, like in cases of night or when there is no one at home. To alarm/disalarm a specific room, the user needs to go the basic/advanced configuration.

This will also show the percentage of house that is alarmed. If all the rooms all alarmed in the house, which is toggled in basic configuration, the percentage will show as 100%. Toggling the room status to disalarm in basic configuration will reduce the % number. If the number falls below 50%, then the box will appear green and say as disalarmed. Touching it will again alarm the whole system. The following figure shows the case where 4/7 rooms have been disalarmed:

Basic Configuration

Advanced Configuration

Alarm – 43 %

Figure 16 Main Menu with Less than 50% System Alarmed

System is currently DisAlarmed:

1. Basic Configuration:

The basic configuration will have the ability to alarm/disalarm each individual room. The user will need to select a room to toggle its alarm/disalarm status. The rooms which are alarmed will show up as red and others will show up as green.

If the user has pressed the alarm/disalarm button in the previous menu and then entered this configuration then all rooms will show up as the color depending on the choice made in previous menu. The user then presses the specific room to change its alarm status.

As mentioned above, the number next to room indicates the percentage of sensors in the room that have been activated which can be toggled in advanced menu. If the percentage is more than 50%, the room color will change to red. This is explained in the following figures, assuming initially the system is disalarmed:

Shed 0%

Garage 0%

Living Room 0%

Kitchen 0%

Room 3 0%

Room 2 0%

Room 1 0%

Figure 17 Basic Configuration

Basic Configuration:

Touching the Room1, will alarm room1 and turn the icon to Red. Next figure shows the case when the user has alarmed room1 and garage and shed.

Room 2 0%

Room 1 100%

Room 3 0%

Kitchen 0%

Garage 100%

Living Room 0%

Shed 100%

Figure 18 Basic Configuration with Room1, Garage and Shed Alarmed

Basic Configuration:

1. Advanced Configuration:

In the advanced configuration the user can individually control the sensors in each room. This would result in changing the percentage of how much the room is alarmed. To enter the specific sensor list of a room, the person would need to present the room button as shown in the following figure.

Room 2 0%

Room 1 100%

Room 3 0%

Kitchen 0%

Living Room 0%

Garage 100%

Shed 100%

Figure 19 Advanced Configuration

Advanced Configuration:

If the user wants to access and activate/deactivate the sensor in room1, he/she can press room1. As with the rooms, an activated sensor will appear as red and inactivated sensor as green. If the central server cannot reach a sensor, for ex. power issues, then that would appear as black and thus, can’t be toggled. This would bring them to the following screen which will show the following list of sensors assuming room1 is currently alarmed but the Camera#1 is not working.

Camera#2

Window#2

Door

Camera#1

Motion Sensor

Window#1

Figure 20 List of Sensors in Room1

Room#1:

The motion sensor toggles the motion sensor in the room. The Window/Door button will help toggle magnetic proximity sensor. The Camera buttons toggle the streaming of the camera and sending images to the central server or not. Touching the camera would also pop up an option block which would allow the user to control the camera parameters mentioned above remotely which are, frequency at which to take images/videos, length of video and apply same setting to other cameras in the house. The following figure shows the drop down menu where every 120 minutes a video of 2 minutes is recorded:

Done

Select Cameras to Apply

Apply to All Cameras

minutes

120

minutes

2

Video

Length:

Image

Figure 21 Camera Settings Menu

Room#1🡪Camera#1 Settings

Frequency:

Clicking on “Apply to All Cameras” will open the following dialogue box and on confirmation will set these settings for all the cameras present in the system.

Yes

No

Figure 22 Apply to All Cameras Confirmation Dialogue Box

Do you want to apply current settings to all Cameras:

Clicking on “Select Cameras to Apply” will open a list of all the cameras in the house and the user can then select the cameras he/she wants to apply the same settings to. The following figure shows the menu and assumes the user is applying the settings to room1 and room3 both cameras.

Figure 23 List of Cameras in Each Room

Done

Select Cameras:

Room1🡪Camera1

Room1🡪Camera2

Room2🡪Camera1

Room2🡪Camera2

Room3🡪Camera1

Room3🡪Camera2

LivingRoom🡪Camera1

LivingRoom 🡪Camera2

Garage🡪Camera1

Shed🡪Camera1

Kitchen🡪Camera1