

Demo #1 Documentation: Home Security Automation

Group 2

14:332:452:01:00614 Software Engineering

Harmit Badyal

Nikunj Jhaveri

Abhishek Kondila

Kaavya Krishna-Kumar

Kaushal Parikh

Miraj Patel

Nirav Patel

Andrew Russomagno

Sagar Shah

Ashwin Suresh

March 27, 2019

Website: <https://sites.google.com/view/ruhome2019/home>

GitHub: <https://github.com/nikunjghaveri123/HomeSecurityAutomationApp>

## User Documentation

### I. System Hardware

#### A. Arduino Base Unit & Components

1. The Arduino Base Unit is what connects all the physical components and tools and is directly connected to the integral hardware components of our Automated Home Security System. The Arduino Base Unit is connected to the arducam, the LED lights, the motion sensor, gyroscope, and the alarm. These components are designed to simulate our design of the home security automation on a smaller scale. The Arduino Base Unit, once given a signal, can send a signal to the components (specifically LED lights, alarm, and arducam) to turn on/off lights, turn on/off alarm, and to take picture.
2. The Arduino Base Unit can receive signals in several different ways. On a very basic level, we can directly connect the arduino base unit to a computer, which itself can send signals to the arduino base unit, which would then transmit corresponding signals to the various components of the system. In our demo, we used this to show that we have the components of the system connected, however in future and in our final implementation, we plan to not rely on this method of signal transmission at all. We plan to have manual signals triggered by the user be triggered via the mobile app. We will go deeper into that when discussing the state and design of the mobile app, however with the hardware specifically, we have connected the arduino board to a wifi shield, allowing for the arduino to establish a local IP address for use on a local wifi network which then would allow for wireless connection to be established between a mobile device and the arduino base unit on the same network. Using HTTP request, the device should be able to wirelessly send signals to the arduino base unit which would then send the corresponding signals to the output components of the system. Perhaps, the most important aspect of our hardware, is the automation aspect. So, in terms of signals being sent to the arduino base unit, we intend for the listening devices such as the motion sensor and the gyroscope to send a signal to the arduino base unit to either take a picture, turn on/off lights, or turn on/off the alarm.
3. In terms of hardware placement, the front door will have the embedded arducam, the motion sensor will be placed outside in an optimal location for detecting people movement in front of the door, the gyroscope will be placed on the hinge of the door in order to detect the opening of the door, the base of the unit, along with the alarm and LED lights will be placed on

the inside of the door. Users will have the ability to manually activate/deactivate the features of the system components and also be able to take a picture of the outside via the mobile app. When the motion sensor in front of the door is triggered, the arducam should simultaneously be activated, taking a picture of the outside of the door. Once the gyroscope is triggered, signaling that the door is opened, the alarms and lights should be activated if the system hasn't already been deactivated by the user or the facial recognition software.

## II. Mobile App

### A. User Settings

1. With the mobile app, the admin user should be able to create new users as well as delete and modify other users for the mobile app itself. Each user on the mobile app should have a clearly defined list of privileges. For example, not all users should have the ability to turn on/off features for the different modes. Not all users should be able to disable the motion sensor and gyroscope indefinitely, and leave the home vulnerable when a user sets the mode into home mode or away mode. Not all users should be able to modify other user settings. There will be a table of sorts that would identify the privileges of each user within the app. The admin user will be able to have complete control of every feature and modify each setting and also edit other users' privileges. The main priority is to make sure nobody is accidentally changing settings and alternating standard settings that really only the admin should have access to.
2. We demonstrated a UI in which the admin user would have the ability to toggle settings for each user that has a registered account in the app. We also show how the user is capable of making a new account as opposed to registering with an existing account.

### B. System Settings

1. With the mobile app, as we discussed in the system hardware section, the user should be able to directly control settings related to the system hardware components. For example, the user should be able to turn on/off the lights, turn on/off the alarm, and take a picture with the click of a button.
2. In our demo we showed this with a UI that allowed for the toggling of the lights, alarms as well as a button that would be able to take a picture of the outside of the door.

### C. Accessing Firebase

1. With the mobile app, the user should be able to access the firebase and be able to access the database of images captured by the arducam of

unidentified visitors to the front door and should also be able to modify the database of user images that would be relevant in the facial recognition.

2. In theory, the user should be able to upload pictures of themselves to the firebase and be able to add users to the system so that the facial recognition system would recognize them and automatically disarm the system upon determining that they were the visitors to the door. The user upon learning that an identified that someone unrecognized approached the door or even attempted to enter, should be able to extract images of the intruder/potential threat, and use judgement to make a phone call to emergency services.
3. In our demo, we showed how we have a firebase connected and have it connected to the android app, as well as the facial recognition software, however we still have yet to insert the ability to modify and extract images from the database. This will be implemented in future and in the final implementation of the mobile app.

### III. Facial Recognition

#### A. User Detection

1. The user should be able to trust the facial recognition software to determine if the person approaching the door is a recognized user. The user should become aware who is entering.
2. We showed this in the demo by taking a picture of one of the three members of the group that had an established profile and demonstrated how upon the analysis of the photo it took of one of these three individuals, the system was able to match the picture to one of the three people's profiles and hence be able to determine how much of a match the users were and what the accuracy would be. Otherwise it would show a lesser value of the match.
3. We still have yet to automate this and have it run once the arducam is triggered. This would allow the user to know who exactly is entering the house once the motion sensor triggers the arducam. This would also on the other hand allow us to know if someone who should not be in the vicinity is approaching the door and attempting to enter.
4. In order to allow for the system to be more accurate in detecting users, we created profiles which would contain pictures from multiple angles and viewpoints allowing for the system to run through all the pictures in the profile in matching the user with the person detected by the arducam.