Smart Home Security User Manual

By : Shahid Ali

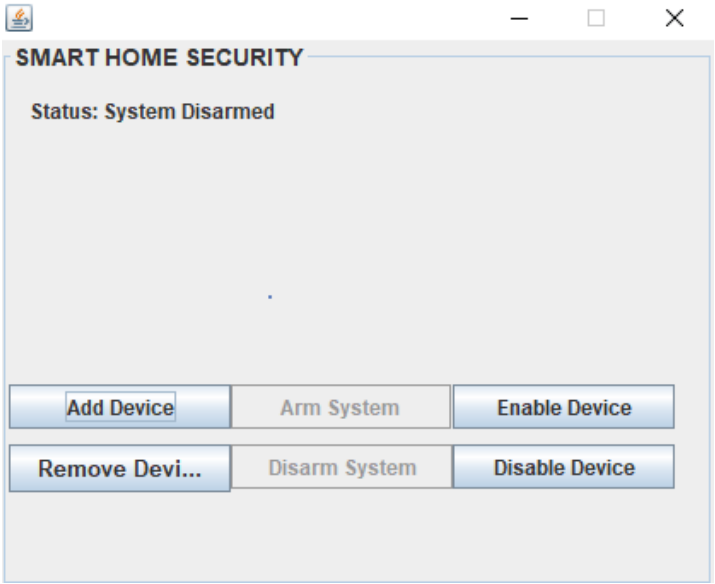
TABLE OF CONTENTS

SYSTEM OVERVIEW

Smart Home Security Feature Description

A Smart Home Security System controls and monitors the security devices that are mounted on the doors and windows in the the house. Smart home security prototype is designed in a manner that allows a user to mount the device on the door and control the prototype through a central hub. This system will require less maintenance as the owner of the system can make modifications for example, replacing a microcontroller and sensors when required. Smart home security is a DIY (Do It Yourself) that will be cost effective. The system will allow user to monitor the events generated by the sensors on door and windows as well as permits the user to arm or disarm the system by one click feature. The user will be able to add and remove sensors to the system. This system will be controlled by a central hub. The central hub is a software solution that will run on laptop. The central hub will consist of a User Interface (UI) on which the user will receive Notifications. User can see all the devices that are added in system, for example if the user adds a new one or want to delete previously added device, this will be done on the central hub. The central hub controls all the devices that are mounted in home, apartment or office. User must have Netbeans installed on his laptop in order to make the UI function. There will be no programming required on the user side.

The below figure is the main page for the smart home security system that shows the status and the buttons that will be used to make the prototype work.



The user features for the system are listed below:

- ADD BUTTON
- REMOVE BUTTON
- ARM BUTTON
- DISARM BUTTON
- ENABLE BUTTON
- DISABLE BUTTON

ADD BUTTON

Add button allows user to add a new device to the system. The next page that shows up when the add button is clicked is the available device panel that shows the MAC address of the devices that are in the network. After getting the MAC address for the required device, the user can give a name to the device (for example: Front door, Back door.). Then a message prompt appears for confirmation if the user wants to add the device or not.

REMOVE BUTTON

Remove button will allow user to remove the device from the shs-prototype if needed. The user can select a device and click the remove button and the device will be removed from the system.

ARM BUTTON

Arm button will allow user to arm the system after the device is added to the shs-prototype. Only after the user arms the system, the devices get activated. When the arm button is pressed the status of the prototype changes to system is armed with a voice alert “System is Armed”

DISARM BUTTON

Disarm button will allow user to disarm the entire system. The status of the system then changes to system is disarmed with a voice alert “System is Disarmed”. There will not be any notifications generated if the system is disarmed.

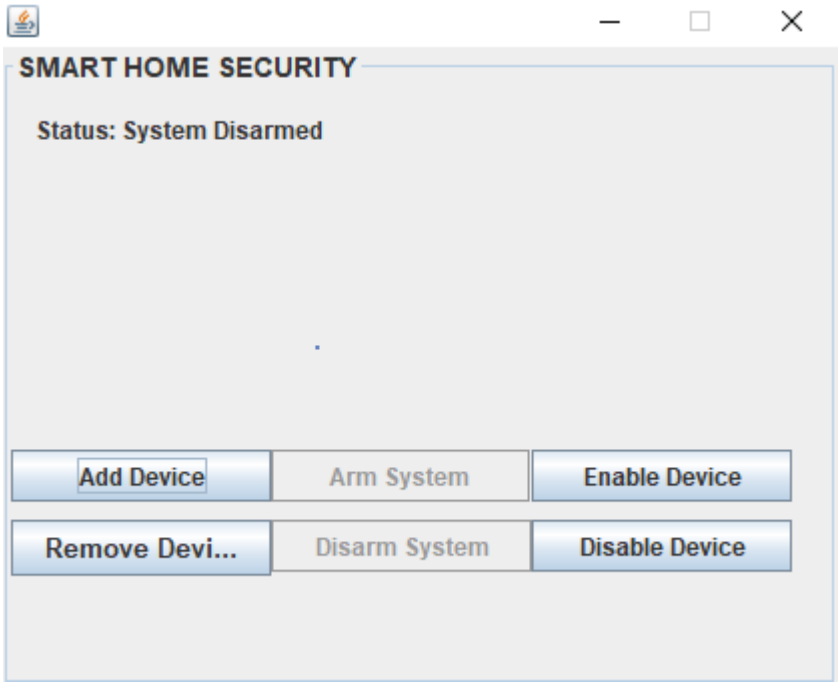
ENABLE BUTTON

Enable button panel will show all the disabled devices. A user can select a required disabled device and click on the button enable. Now the disabled device gets enabled and will appear in disable panel.

DISABLE BUTTON

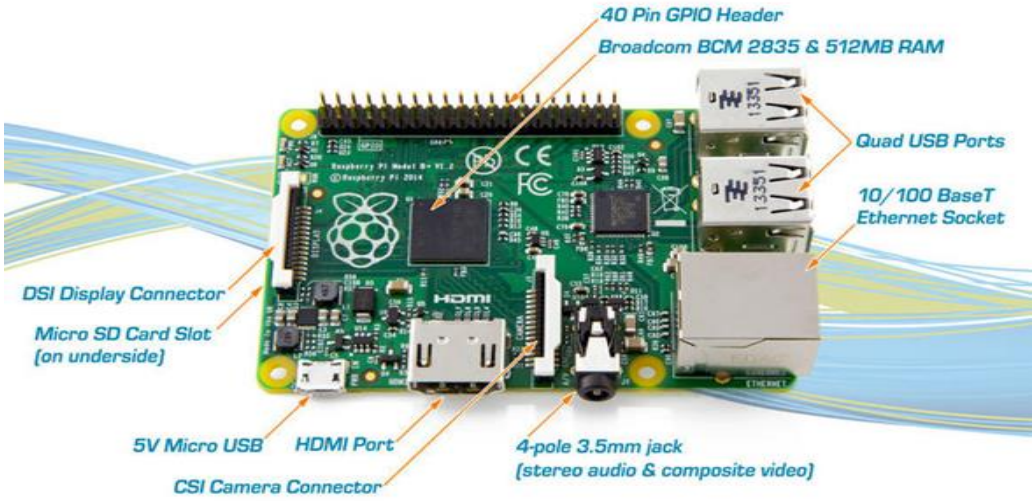
Disable button panel shows all the enabled devices. Select a device name which should be disabled and click the disable button. The device which was disabled will get enabled and will appear in the enable panel.

Main Screen



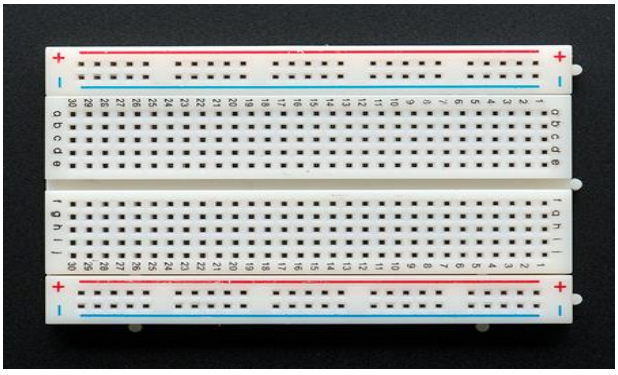
Hardware requirements

1. Raspberry Pi 3 Model B Motherboard



- 1.2GHz 64-bit quad-core ARMv8 CPU, 1 GB RAM
- 802.11n Wireless LAN, 10/100Mbps Lan Speed
- Bluetooth 4.1, Bluetooth Low Energy
- 4 USB ports, 40 GPIO pins, Full HDMI port, Combined 3.5mm audio jack and composite video

2. Bread Board



A breadboard has many holes, normally spaced 0.1 apart that you can insert leads/wires into that will be held in place by metal contacts inside. This allows fast prototyping of circuits, without the need to solder anything together.

Breadboard is used as a mediator between the raspberry pi and sensors, cameras or the reed switch that helps in connecting the GPIO (general purpose input output) pins with the sensors.

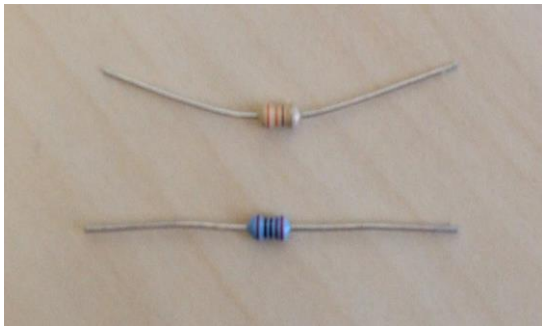
3. Jumper Wires

Jumper wires are of three types: male and female wires, male and male wires, female and female wires.

4. Door magnetic reed switch

A reed switch is an electrical switch operated by an applied magnetic field.

5. Resistor



Resistors are used to change the amount of current flowing through a part of the circuit. This is often used as a means of protecting components which cannot handle large currents.

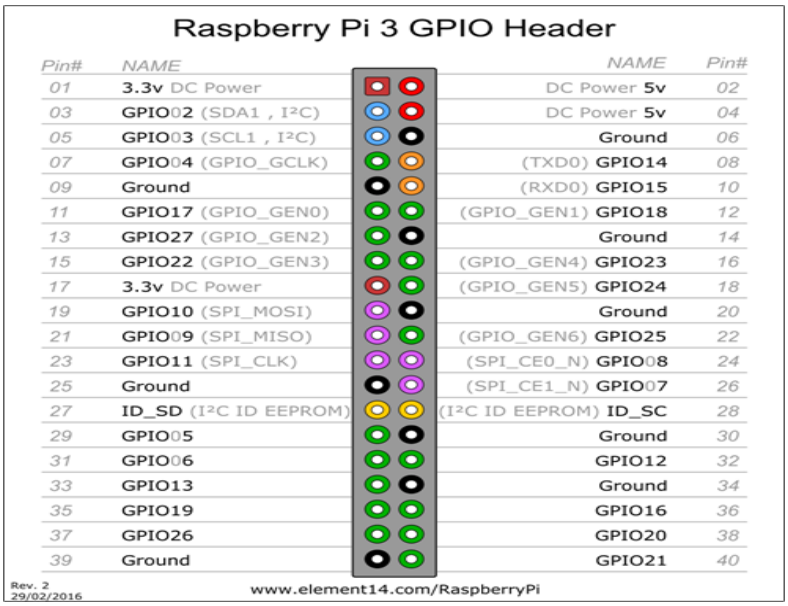
6. HDMI cable

A HDMI cord helps the user in the initial installation of the software's that are required to be downloaded.

7. Keyboard and Mouse:

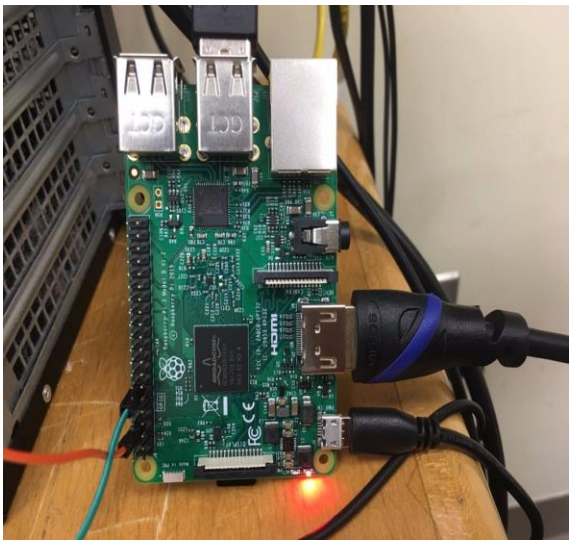
To connect with raspberry pi to install softwares and perform the required task to make the system to run.

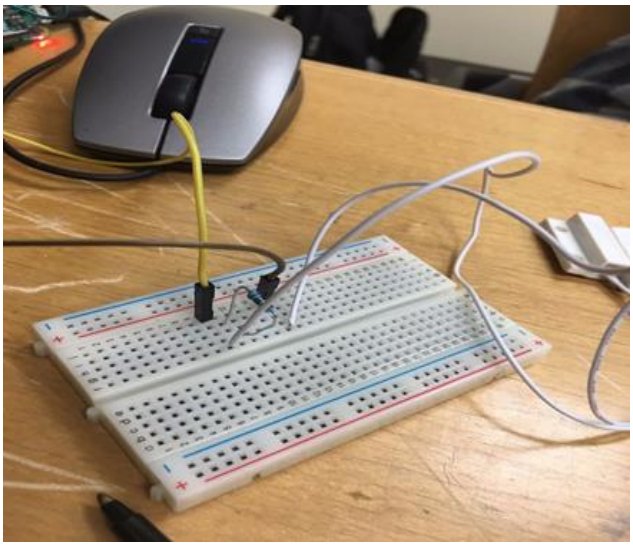
GPIO Pins

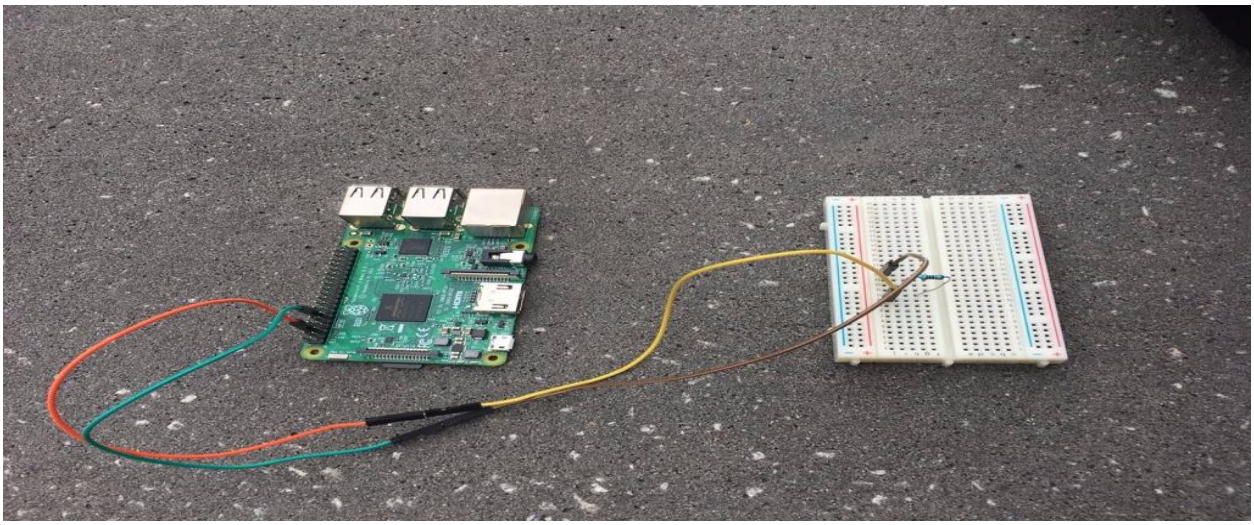


The user will have to connect the raspberry pi and the Breadboard using jumper wires.

The user need to connect to pin 6 (GND) and pin 12 on the Raspberry Pi and on the Breadboard the pins will be 10 and 15 respectively to make the system work.







SOFTWARE INSTALLATION:

- **On laptop/Desktop**

  NetBeans: Install the NetBeans software on the laptop to run the GUI.
  - Clone the smart-home-security code From GitHub: Link https://github.com/samspad/smart-home-security-shs-12_12_17

How to Install NetBeans

NetBeans 8.0.2 is highly recommended as it has pre-installed libraries.

NetBeans step by step procedure to download software:

1. NetBeans IDE 8.2 Installation Instruction:

https://netbeans.org/community/releases/82/install.html

2. NetBeans IDE 8.2 Download:

https://netbeans.org/downloads/

* To use NetBeans for java you need to first install Java Development Kit.

* Download “NETBEANS IDE”

* Run the installer then run the downloaded installer.

For the Local Computer, the User Can Download the NetBeans Software from the Following Link. NetBeans 8.0.2 is highly recommended as it has most of the pre-installed libraries.

https://netbeans.org/downloads/

In the Link Provided above, select the Java EE format and click Download.

Putty

ssh from laptop to raspberry pi the user needs to navigate to:

- Select **Menu** > **Preferences** > **Raspberry Pi Configuration** > **Interface options**
- Ensure SSH is Enabled.
- How to connect mac through putty:
- Go to terminal / command prompt
- Type : ssh username@hostname ex: ssh pi@172.16.192.251

On Raspberry Pi:

1. NOOBS
2. VNC Server

NOOBS Installation

Requirements to install NOOBS on the Raspberry Pi:

- A computer with an SD card slot
- An SD or microSD card of at least 8GB

Step 1: Download NOOBS and extract it

NOOBS should be downloaded as a .zip file, so before doing anything else, the file should be extracted.
It can be downloaded from the following link:
https://www.raspberrypi.org/downloads/noobs/

Step 2: Format an SD card

To format the SD card, download any “SD Formatter” software. After installing the software the user needs to format the card inserted in the computer.

Step 3: Put the NOOBS files on the SD card

Now, just drag and drop the NOOBS files into your formatted SD card. You want the files only, so if your .zip extracted to a folder, open that folder and select only the folder contents inside.

Step 4: Put your SD card into your Raspberry Pi and boot it up

Once you have NOOBS on your SD card, using it is incredibly easy. Just put the SD card into your Raspberry Pi and start it up. This will initiate the installation.

VNC Installation

A VNC viewer (or client) is installed on the local computer and connected to the server component such as Raspberry Pi, which must be installed on the remote computer. The server transmits a duplicate of the remote computer's display screen to the viewer.

It can be installed from the following link on the local computer:
https://www.realvnc.com/en/connect/download/viewer/

The user have to Add the IP address of the Raspberry Pi in the Installed VNC Viewer and the user will be asked to provide admin ID and Password. Upon providing the details, the user will be remotely connected to the Raspberry Pi and can see the screen on the computer.

For the Raspberry Pi the user can just open the terminal from the taskbar and write:

Command: sudo apt-get update

Command: sudo apt-get install realvnc-vnc-server realvnc-vnc-viewer

Next Step,

- On your Raspberry Pi, boot into the graphical desktop.
- Also ensure that VNC is Enabled.
- Select **Menu** > **Preferences** > **Raspberry Pi Configuration** > **Interfaces**

Then,

Type the Following Command in Terminal

Command : Sudo Raspi-config

VNC Server/Viewer is installed for Raspberry Pi. To test the connection, enter the IP address from the VNC server into VNC viewer and click connect.

Steps to run the server on startup in Raspberry Pi:

- Download the code from Github for the server to run on the pi https://github.com/samspad/smart-home-security-shs-ux
- Save the file in **Documents** folder in the root directory of the raspberry pi
- In Documents folder unzip the downloaded server file
- Then in terminal type the following command line code:
  Command: sudo nano /etc/rc.local
- In the new popup file locate the keywords ‘fi’ and ‘end’ at the end of the file
- Type the following file path in between ‘fi’ and ‘end’ keywords:
  Command:
  (sleep 10; python3 /pi/home/Documents/smart-home-security-server/shs-server.py)&
- Then press ctrl+x to save the file and hit enter
- Then reboot the system:
  Command: sudo reboot
- We are rebooting the system to make sure the server runs.
- After the system reboots wait for 10 second after the pi startup

Creating a Hotspot

Mobile hotspot from laptop will allow you to share the network connection with other devices over Wifi, Ethernet, or any cellular data connection. Follow the steps below to create your personal connection:

- Select the **Start** button, then select **Settings** > **Network & Internet** > **Mobile hotspot**.
- For **Share my Internet connection from,** choose the Internet connection you want to share.
- Select **Edit** > enter a new network name and password > **Save**.
- Turn on **Share my Internet connection with other devices**.
- To connect on the other device, go to the Wifi settings on that device, find your network name, select it, enter the password, and then connect.

Once the devices are connected, to see and verify the MAC address of all the available devices in network by following the step below:

- Open **Terminal** by right clicking on **Start** button > click on **Command Prompt**
- In the **Terminal** type > **arp -a >** hit **Enter**

Quick View of System Functions

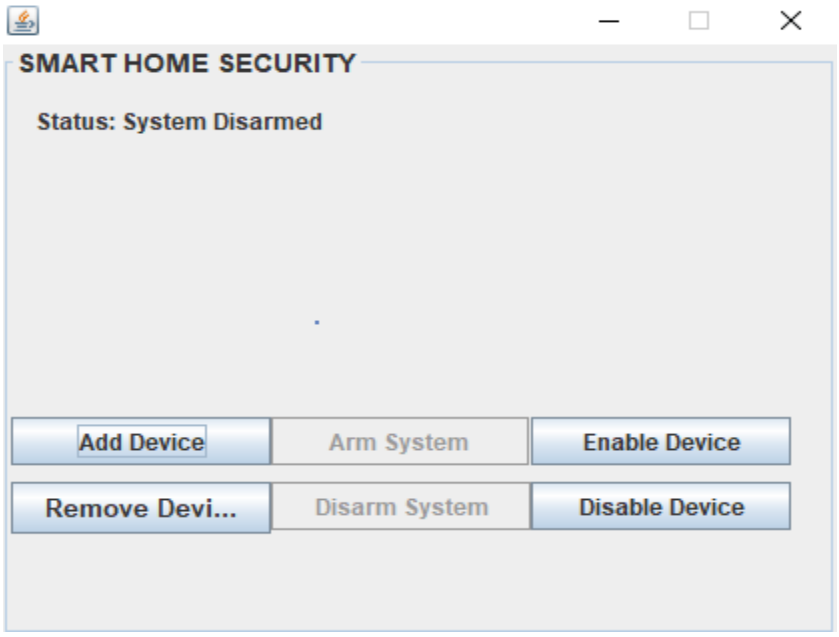
SECURITY FUNCTIONS
Check System status: .....See “Homepage” Top Left Corner.
To arm the System: .....Select “Arm” Button and the Message will be shown.
To Disarm the system: ..... Select “Disarm” Button and the Message will be shown
To Enable a Door or Window: .....Select “Enable” and select the specific device to enable.

To Disable a Door or Window……...Select “Disable” and select the specific device to disable.

OTHER FUNCTIONS (accessible to the Master User only)
To Add a Device: ..... Select “Add” Provide a Device ID and Name and that device will be automatically added.
To Remove a Device…….. ……. Select “Remove” and choose the device to remove, that device will be automatically removed.

SMART HOME SECURITY MAINPAGE:

HOMEPAGE



Description
The home page of the smart home security system consists of a status bar that changes the state based on the systems state. The SHS prototype comprises of six buttons add button, remove button, arm button, disarm button, enable button, disable Button.

ADD DEVICE PANEL

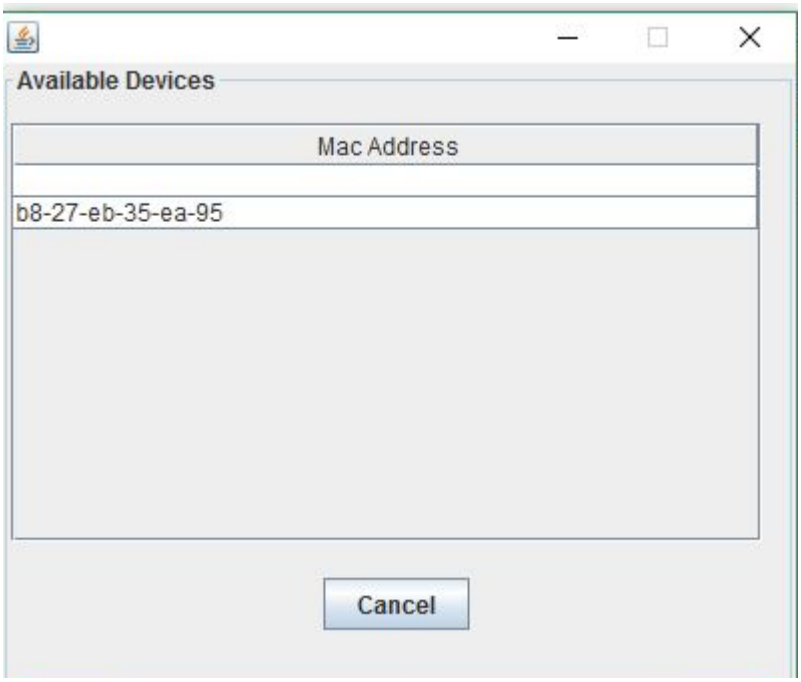


Figure 1: Add device panel

Add Device Button Functionality: In the above figure 1 when the user clicks on the add button a list of mac addresses is shown that are connected to the same network. The user can select the device mac address and assign a name for the device and click the save button.

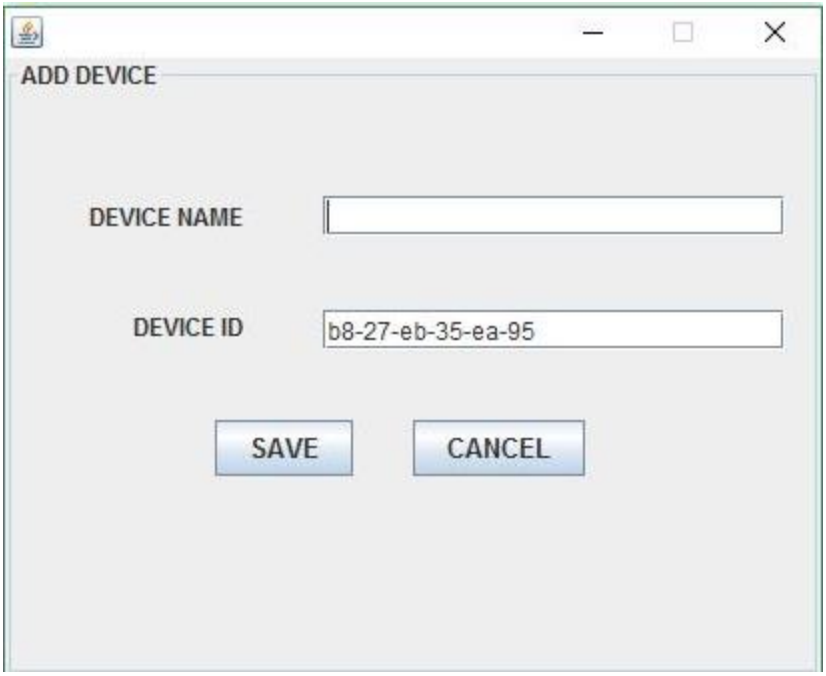


Figure 2: Add device panel

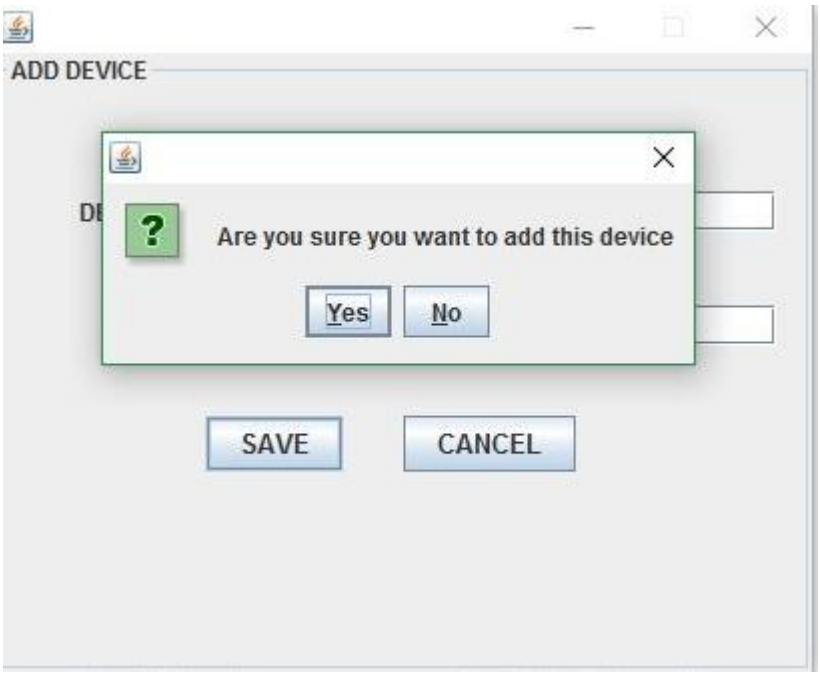


Figure 3: Add device panel confirmation message

Once the user has assigned the name to the device a message prompt is shown that asks for user acknowledgement by showing two buttons yes and no. Once the user decides to press yes, the devices is saved automatically.

REMOVE DEVICE PANEL

Figure 4: Remove device panel

Remove Device Button Functionality:
The remove device panel shows all the devices that have been added to the prototype. This panel allows the user to select a device and remove it from the system.

Figure 5: Remove device panel

Once the User Clicks on the Device that He/She Wants to remove, the System will remove the device automatically.

ARM DEVICE PANEL

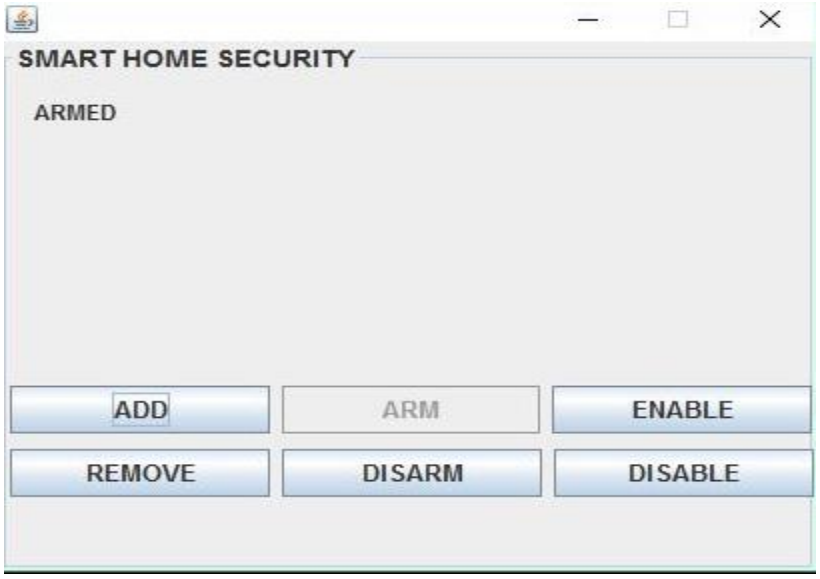


Figure 6: System Armed

Arm Button

In the above figure 6, When arm button is clicked a voice notification/alert is played “System is Armed” and the status is changed to system armed. This button activated the system and when an event is generated the user gets a notification on the central base station “Door is Opened”.

DISARM SYSTEM PANEL

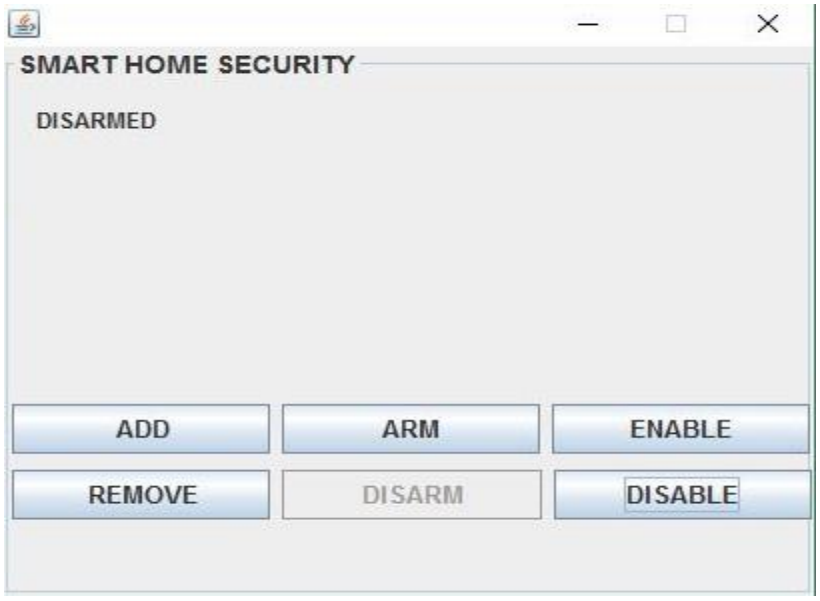


Figure 7: System Disarmed

Disarm Button

In the above figure 7, When disarm button is clicked a voice notification/alert is played “System is Disarmed” and the status is changed to system disarmed. This button deactivates the system. Once the system is deactivated, if the user opens/closes the door there will not be any notifications or alerts generated on the central base station.

ENABLE DEVICE PANEL

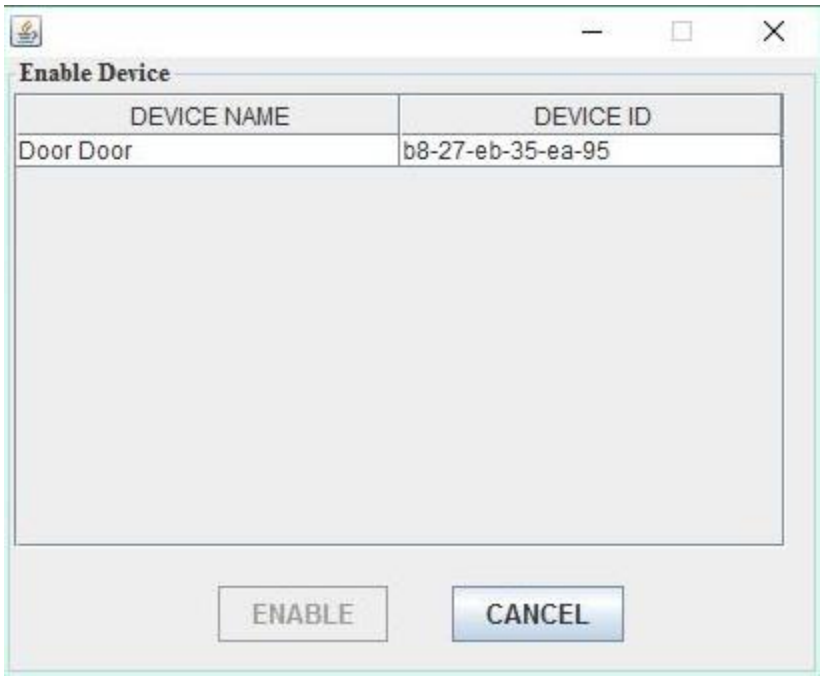


Figure 8: Enable device panel

The Enable device panel shows all the disabled devices in the prototype. If a user wants to enable a particular device, he/she should select a device and click on the enable button. Once the device is enabled the device will move from enable panel to disabled panel.

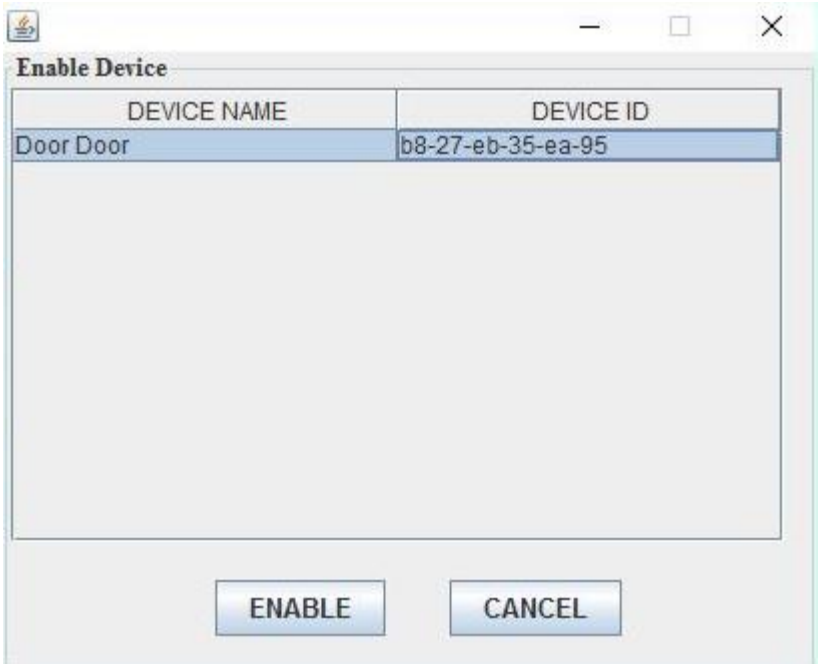


Figure 9: Enable Device Panel

Once the User Clicks the Enable Button, the selected device will be Enabled and move to Disable Panel of the system.

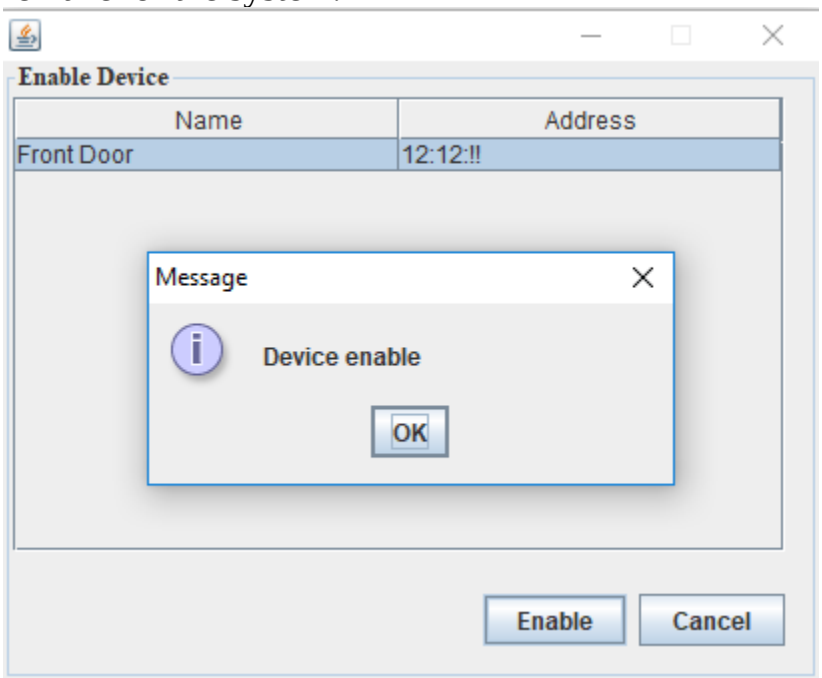


Figure 10: Enable Device Panel

DISABLE DEVICE PANEL

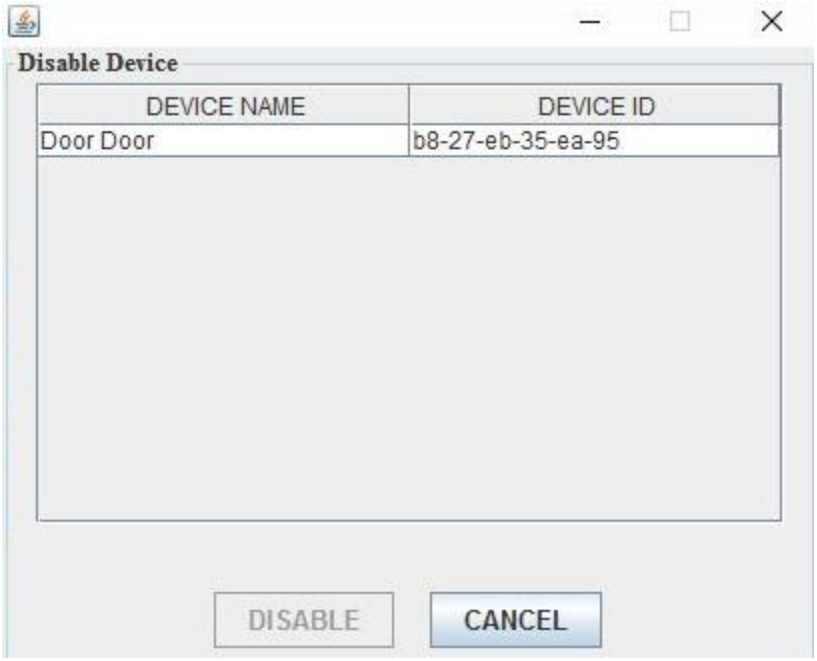


Figure 11: Disable device panel

The Disable device panel shows all the enabled devices. If a user wants to disable a particular device, he/she should select a device and click on the disable button. Once the device is disabled the device will move from disable panel to enable panel.

Figure 12: Disable device panel

Once the User Clicks the Disable Button, the selected device will be disabled and move to Enable Panel of the system.

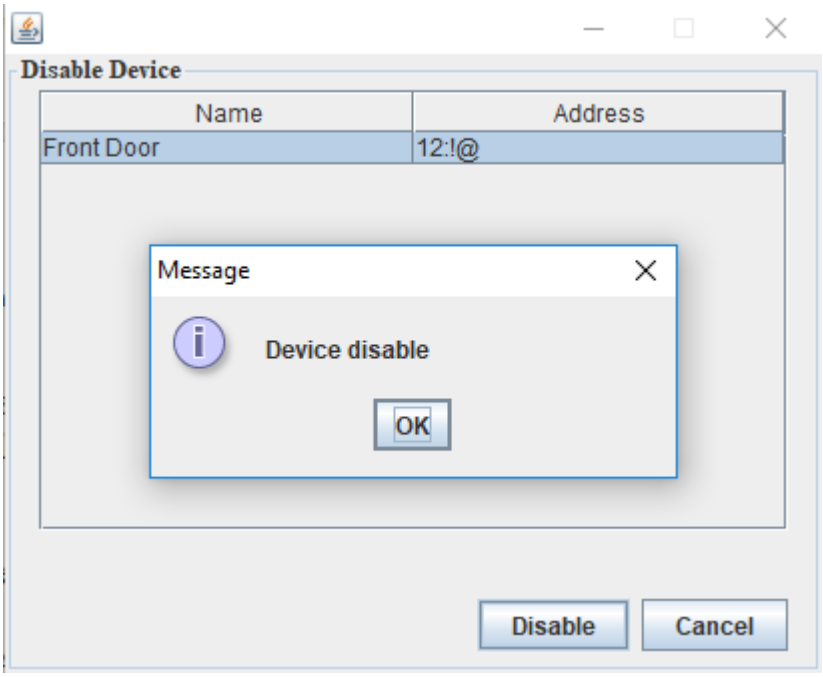


Figure 13: Disable Device Panel

NOTIFICATION PANEL

When there is a notification on the system, there will be an alert message on the Home Screen stating that “New Device Notification”.

Figure 14: Notification Panel

The user will have to click on the Alert Message to see which devices are creating the Alert.

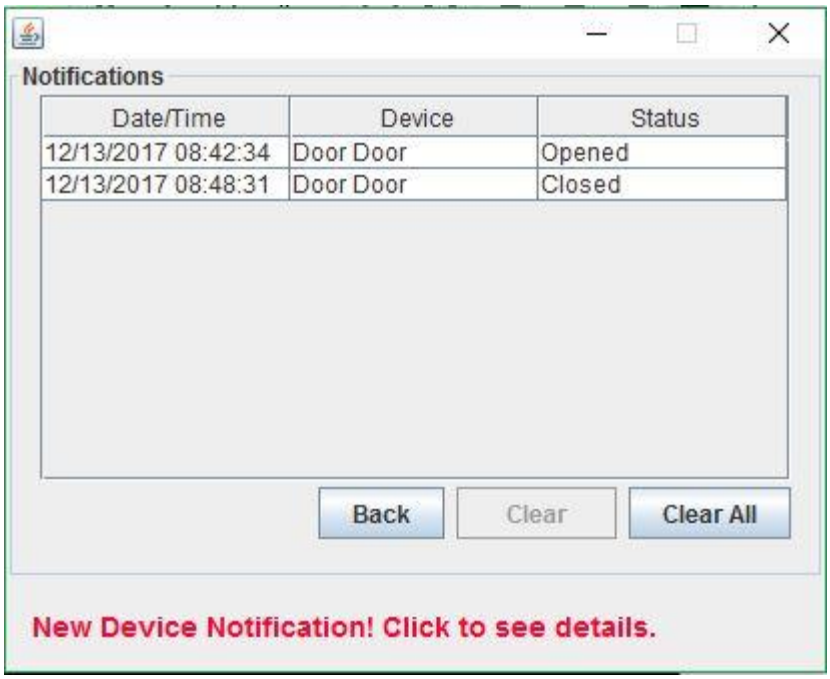


Figure 15: Notification Panel

All the notifications will be shown with date and time. The User can select a single alert and clear it or he /she can clear all the alerts by clicking on Clear all Button. If Clicked on Clear All button, All the Alerts will be Removed, and the system will take the user to the Homepage.

The User Will Return to Homepage.

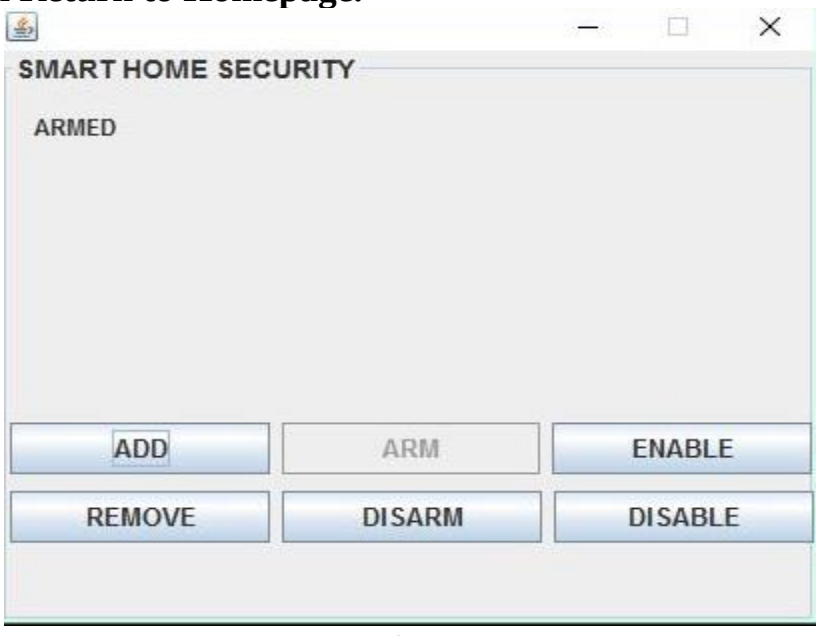


Figure 16: Homepage

SYSTEM FUNCTIONS

Maintaining your system

The components of your security system are designed to be as maintenance-free as possible. To make sure that your system is in working condition, do the following:

1. Test your system weekly.
2. Clean the Microcontrollers weekly.

Routine Care

- Treat the components of your security system as you would any other electrical equipment. Do not slam sensor-protected doors or windows.
- Keep dust from accumulating on the Microcontrollers and all protective sensors, particularly on motion sensors.
- The microcontrollers and sensors should be cleaned carefully with a dry soft cloth. Do not spray water or any other fluid on the units.

WARNING!

THE LIMITATIONS OF THIS SYSTEM

While this system is a DIY (Do It Yourself) security system, it does not offer guaranteed protection against burglary or fire or another emergency. Any alarm system, whether commercial or residential, is subject to compromise or failure to warn for a variety of reasons. For example:

1. Intruders may gain access through unprotected openings or have the technical sophistication to bypass an alarm sensor or disconnect an alarm warning device.
2. Signals sent by wireless transmitters may be blocked or reflected by metal before they reach the alarm receiver. Even if the signal path has been recently checked during a weekly test, blockage can occur if a metal object is moved into the path.
3. A user may not be able to reach a panic or emergency button quickly enough.

SMART HOME SECURITY

1 JOHN MARSHALL DRIVE
Huntington, WV 25701