IoT HOME SECURITY SYSTEM

ECE 442: Internet of Things and Cyber

Physical Systems

Part 1: Project Proposal

Due Date: 05/26/2022

Problem Statement:

Home security systems are often limited to the coverage, false alarms, and power usage. The limited area of surveillance leaves the entrance unprotected and to overcome this we are developing a smart alarm system which can activate the camera with facial recognition using motion to decrease power consumption and false alarms. The system also includes contact sensors which can cover a wider range of surveillance.

Design Overview & Approach:

In this project, we aim to build a modular home security system with facial recognition and quick alert capabilities to deter and mitigate potential malicious intrusions. The system prototype will focus on a single entry point, i.e., the main door, but is modular enough to be adapted to any other entry point to suit user needs.

The overall system design includes a magnetic contact sensor, an ultrasonic sensor, a light and camera on the front-end, a central Raspberry Pi node, a database for saved FaceID profiles and for data collection and storage, and an Android app for alerts and remote control of the system.

Entry Point Security:

The front-end of the security system consists of an ultrasonic sensor to sense nearby movement, which triggers a light and camera that scans an individual's face and runs it through a saved FaceID database of authorized individuals to determine access permissions which, when successful, temporarily disables the magnetic contact sensor. If the individual fails the facial recognition scan (after 5 consecutive failed attempts), the contact sensor stays on and an alert is sent to the homeowner with a picture of the individual, and if the individual then tries to open the door, the magnetic contact sensor sends an intruder alert to the user.

In case of poor recognition of a registered individual, a keypad is installed and programmed to disable the contact sensor alarm when the user-defined keycode is inputted.

The Companion App:

The companion app will be designed to monitor, add and access the system. The app can be used to pair additional nodes to the system. It can be used to arm and access the status of the system, allowing users to arm/disable it as required. Designed with ease of accessibility and usage simplicity in mind, it is programmed with 'soft' alerts (if a failed facial recognition scan is detected) and intruder alerts (if a forceful entry is detected), and also has functions to forward alerts to others or autodialing the police. The app also allows users to access and control the stored status logs and data such as the picture of the potentially malicious individual.

Communication:

The system will use WiFi and Bluetooth either via an ESP8266 or Zigbee module. The sensors can be connected wirelessly to the microcontroller to increase the range of the system. The system can be accessed by connecting the primary mobile via Bluetooth or WiFi, and when authorized by the user, can grant system access to newly paired nodes.

Data Collection & Storage:

We will be implementing two types of data storage. The data of the sensors will be collected via the microcontroller and sent to the Raspberry Pi. The data will be stored first locally on the Raspberry Pi then sent/uploaded to the cloud. The data received via the microcontroller and sent to the Raspberry Pi will be processed and stored. The local storage is included incase of an internet shortage. The Raspberry Pi will upload the collected data.

Technical Challenges:

1. Fault Tolerance: We considered scenarios in which parts of the system might fail or get bypassed by the intruder such as if the intruder manages to force the front door open, a contact sensor that is placed at the door will trigger and cause the system to send a notification to the user if they are home or call the authorities immediately if they are not. Another scenario would be if the intruder managed to cut off power and/or the internet to the system, it will use backup batteries that are installed on it and prioritize taking as much facial evidence of the intruder such that it will make finding them easier for the authorities.
2. Facial Recognition: With the core mechanism of this system being facial recognition, accuracy is vital and depends on the image resolution of the camera. Implementing facial recognition software will be challenging initially because faces are three-dimensional and constantly in motion, not static like a fingerprint, and hence facial profiles must be thorough by seeing face from different angles to increase the scan accuracy.

Hardware:

Components	Description	Price
Magnetic Contact Sensor	It will be connected to the main door and will act as a fail safe in case the intruder passes the sensors, facial recognition, and pin code entry. When the sensor's	$5.99

	magnetic field breaks it will cause the system to send a notification to the user’s phone if they are home or immediately call the authorities if the user is not.	
Ultrasonic/PIR sensor	To detect motion and activate the camera to capture the image and decrease the power consumption of the system.	$4.99
Camera	We plan to incorporate a usb camera which will capture the individual. The camera will be used to enable facial recognition to disarm the system.	$20.99
LED light	Will trigger once the ultrasonic sensor is tripped. It will allow the camera to get a clearer picture of the individual. This will help the facial recognition in determining who is at the door	$10.66
Arduino Uno	It will be used as a central node to communicate between the sensor nodes and raspberry pi.	$25.99
Raspberry Pi	It will be used to run facial recognition software. It will also be used as a local server to store and run the system during a power/internet outage.	$50.00
Battery	To be used as backup power for the nodes.	$2.99/each

Software Components:

Programming Languages:	Python and C#
Applications	Description
Arduino (C#)	It will be used to code the microcontroller and sensors to work according to the algorithm. When the contact sensors are armed and detect disturbance, it will send an alert to the owner/authorities.
OpenCV (Python)	It will be used to configure the camera with facial detection software to recognize individuals either as friends or intruders.
IFTT	It will be the MQTT broker in which our system will be hosted. As the initial setup for displaying the system to update the status of the system.
Raspbian (Linux)	It will be used as the base of our system onto which we will design our local server and set up our system.

Timeline:

Week 1: Discussed our ideas (Everyone)

Week 2: Decided on a topic (Everyone)

Week 3/4: Buy necessary hardware (sensors) and assemble them to the arduino. Working on facilitating facial recognition. Developing the companion application. Connecting the hardware to the local server (Raspberry Pi).

Week 5/6: Test the system. Reworking any issues that arise during testing. Finalizing the system for submission.

Work Distribution:

Team Member	Task	Due Date
Hamad Abdelrahim	Design and work on the implementation of the sensors and microcontroller Arduino Uno.	06/01/2022
Alan Palayil	Design and work on the implementation of the algorithm to be used in the system.	06/01/2022
Nikhil Aditya Chaganti	Design and work on the implementation of the facial recognition software on Raspberry Pi.	06/01/2022