IoT Based Home Security

Jinal Bakhai
Annie Eapen
Aishwarya Rao
Nidhishree Mendon
Dr.Vijaya Padmanabha

Internet of Things (IoT) allows real-world objects to be connected and managed through the internet. IoT is used to make any device smart and is thus a booming concept worldwide. Being a part of the era of the internet, it has become easier to experiment and develop new ideas. Many such ideas have been implemented, changing people's lifestyles in general. Smart home technology is known to bring about more comfort and convenience at our homes. We have decided to stretch this concept out further to implement the concept of IoT into the security of our homes. The proposed model focuses on the security and ease of allowing access to the house. The leverage obtained by choosing this over other forms of home security is the ease of allowing access and monitoring our homes at any time and from anywhere. Our overall system is also focused on being made at a budget so that all sections of the society can experience this convenience and safety. In a world where technology is advancing at such a rapid rate, it is to be seen that everyone plays a part and stays up to date.

Introduction

The progress of science and technology happens in a logical manner where every discovery is produced from an existing one. Over the years, technology has been developing rapidly on a large scale, making human lives so much easier and more sophisticated. It is evident that technology has found its way to be incorporated into a person's daily activities; the most common forms are mobile phones and computers. Due to the popularity of these devices and the competition amongst various companies, an environment of fast and vast growth has been created.

The internet is an invention that evolved from a military form to global cyberspace. The internet, in simple words, is defined as a global system of networks. It connects a large number of computers and allows them to communicate with each other by sharing information with permission. It allows us to come up with quick solutions to problems and is seen as a widely used interface for devices to simplify people's lives further.[1] The internet revolutionized the path of technology and has further broadened the scope of development.

Internet of Things (IoT) is one of the most promising technologies today. It is a concept that allows devices in a network to be connected, controlled, and managed from anywhere around the world through the internet. The internet connection allows devices to either receive data, send data, or both. Various types of objects, such as smartphones, computers, and even home appliances, can be connected via IoT, and this allows a new form of interaction amongst the devices and its users. With the advent of IoT, home automation has become a popular area of development. [2]

These days, home security is considered to be the need of the hour. A person's home is considered to be their most trusted spot and also the most natural target for an invasion. Installing home security of any kind is considered to be a layer of protection. It lessens the resident's concerns to a certain degree because the use of Wi-Fi and 4G-LTE wireless internet access is increasing rapidly in today's world. Incorporating IoT with home security allows you to monitor the security of your home and perform necessary actions from anywhere at any given time while connected to the internet.

IoT based home security has many advantages over the many already existing alternatives. A key lock system on the doors has been one of the first modes of home security. However, this system does not hold much protection as they are easily breakable into without much difficulty. The absence of the resident also makes this operation much more accessible and can even be made unnoticeable. People have been making continuous attempts over the past decades to secure their homes from invasions. As technology progressed, new methods were found. RFID and Bluetooth were two of the standard methods chosen for home security. Though widely accepted and used, it still faces various disadvantages. IoT home security eliminates the need for carrying a physical object to provide access. It is quite common that people tend to forget to carry keys or cards used to unlock their doors. Being able to control the access into your homes through your phone, being the most relied technology, highly increases the level of convenience. IoT also eliminates the issue of the range that is faced with Bluetooth devices. Bluetooth technologies are required to be in a specific range to be able to control the devices remotely.[2] Devices connected through the internet can be accessed globally and have no limits to the range, This allows the resident to be able to know the state of security at his house at any time and be notified instantly if any unusual event takes place. It is clear that this method of using IoT in home security provides more security and is more convenient.

Through different methods of door security such as latching mechanism, card readers, guards and cameras, biometric access control is considered to be the most convenient and one of the most secure methods of access. Biometrics measures the physical or behavioral characteristics of an individual to recognize or authenticate their identity. Facial recognition is a standard physical biometric method that requires a digital camera to develop a facial image for authentication. [3] It is considered to be a quick method of detection and also has the benefit of no contact.

In this paper, we suggest an IoT based smart door lock system. The primary aim of the system is to convert an ordinary doorbell into an intelligent doorbell and increase home security by integrating IoT with facial recognition. A smart home doorbell is an integral part of a smart home that helps protect the security of the home by avoiding unwanted mishappenings such as robbery and invasion. This proposed model allows the user to control the access and monitor the state of security around the front door from the user’s smartphone. It uses facial recognition techniques to increase the convenience of access for the residents and allow faster detection along with quicker and more detailed alerts to be received by the resident.

Literature Review

Security has always played a crucial role in one's day to day lives, especially in today's fast-paced, ever-changing world. Inculcating technology into the field of security is a prominent way to increase safety and reduce workforce efforts.

The paper (Pavithra.D and Ranjith Balakrishnan, 2015).[2] ‘IoT based home appliances and control’ proposes a system that implements a continuous monitoring system to control various home appliances using a smartphone. It collects different sensor values that are analyzed with the help of the low-cost microcontroller. If any problem is detected, then the user is notified immediately, this makes it possible to fix these appliances before it reaches a state where it cannot be repaired, this even prevents the problem from becoming one that is a more significant threat to the residents.

(Kumari, 2015). [3] ‘IoT based Wireless-Alert System for Deaf and Hard of Hearing,' discusses already available methods and technologies for the deaf and also proposes a system to alert the hearing impaired about visitors. There are several appliances available in the market to help the ones in need to improve communication. Usually, such people are unaware of the arrival of uncanny visitors. Therefore it would be of great help to build an alert system that notifies these people about the appearance of their guests. The proposed system consists of 2 modules, a transmitter and a receiver where the latter represents the device installed at the door, and the receiver serves as the wearable device, which helps to alert the user. The main advantage of this system is the reduction in the waiting time of visitors and the security of the disabled.

(Lee, Lin, & Kim, 2016). [4] ‘Development of an IoT-based Visitor Detection System’ aims to build an IoT based Detection system that helps minimize the use of fixed cameras, which can indeed have blind spots. To achieve this system appropriately, the developers use Raspberry Pi2 as a controller and an IR sensor as a detector for uncanny visitors to locate the position of the visitors for more accuracy they also use two ultrasonic sensors. To solve the issue of blind spots, they used a camera module with a servo motor to change the direction of the camera to the course of the visitor. To test the working of this system, they tested each device separately to validate their functioning. In the end, the user applied a code written in python language to implement the algorithm.

(Anvekar, 2017). [6] ‘IoT Application Development: Home Security System’ is proposed to develop a feasible solution to convert a traditional doorbell into an intelligent doorbell which provides information to the owner about the guest and thereby allowing the user to answer the door through the smartphone with comfortable user interface abilities.

(Balla & Jadhao, n.d,2017). [7] ‘IoT BASED FACIAL RECOGNITION SECURITY SYSTEM’ proposed a system that uses facial recognition that can recognize if the arrived visitor belongs to the images of family and friends stored in the database and to decide whether to allow the visitor into the apartment or not. This system is usable at various locations like offices, homes, industries, etc. It can also be accessible from different places due to the application of IoT.

(Fiorenza, Bompelli, Sampath, & Ghogre, 2018). [8] ‘IoT SMART DOORBELL SURVEILLANCE' focuses on ensuring a better home security system. The proposed model is said to be made on the concepts of Arduino and OOPs. Here, the user is notified about the arrival of a guest through a mail that consists of a snapshot of the visitor and a short message. The goal is to enable users to have access and information about the surroundings of their home even they are not at home.

System Design

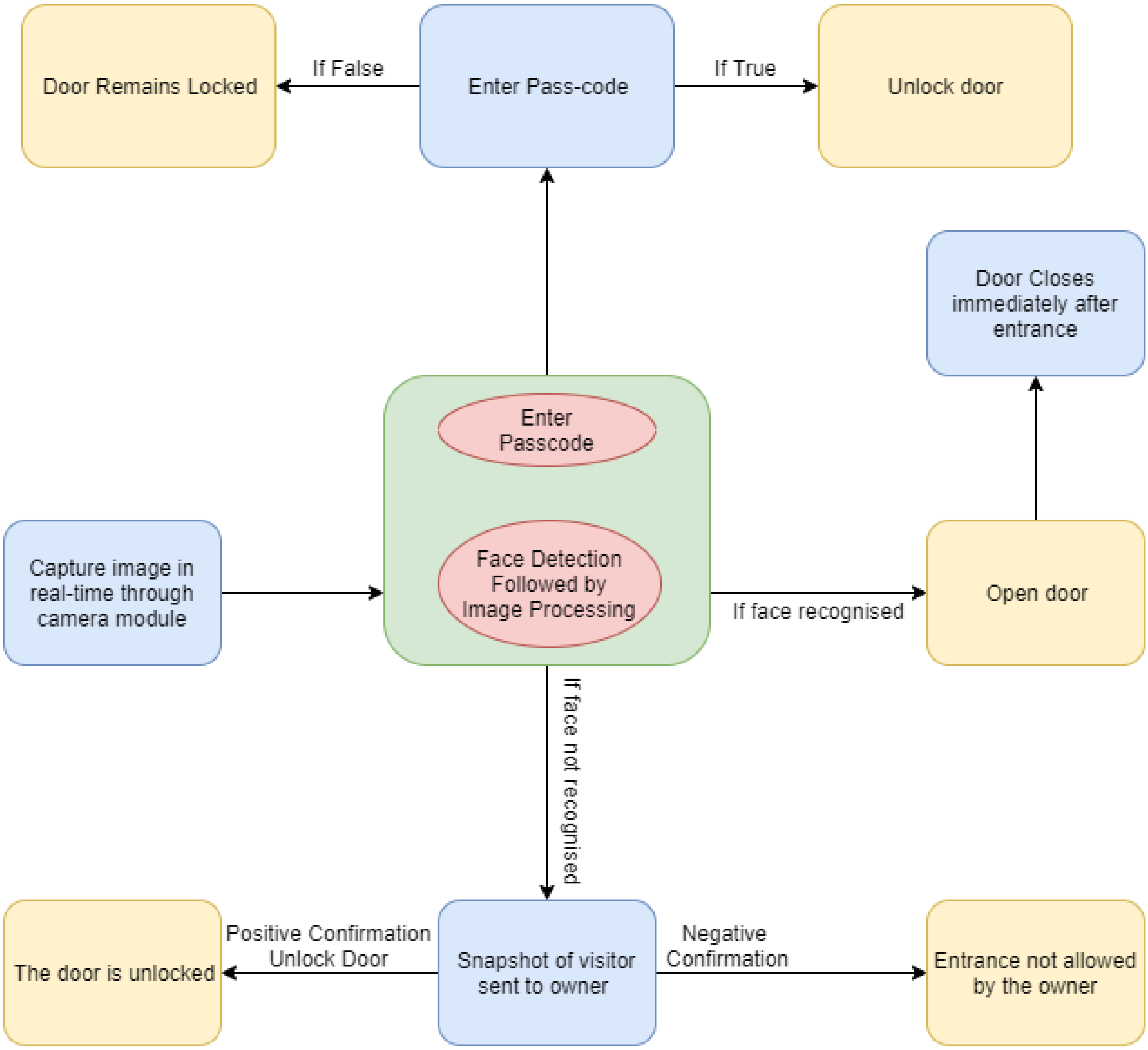
Door Remains Locked
If False
Enter Pass-code
If True
Unlock door
Door Closes immediately after entrance
Enter Passcode
Face Detection Followed by Image Processing
Capture image in real-time through camera module
If face recognised
Open door
If face not recognised
The door is unlocked
Positive Confirmation Unlock Door
Snapshot of visitor sent to owner
Negative Confirmation
Entrance not allowed by the owner

Figure 1. *Flowchart of the working model*

Experimental Procedures

A list of materials that can be used to implement the proposed model is listed below with a brief explanation for each:

Raspberry pi 3 Model B

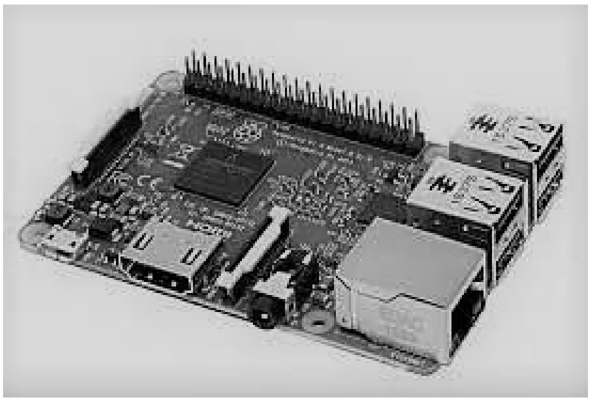

Figure 2. ***Raspberry Pi 3***

Raspberry Pi is a cost-effective micro-sized computer that lets people of all age groups explore data processing and learn programming in languages like python. Raspberry Pi 3 Model B is one of the initial models of the 3rd generation Raspberry Pi. It has the specifications like Quad Core 1.2GHz Broadcom BCM2837 64bit CPU, 1GB RAM, and BCM43438 wireless LAN and Bluetooth Low Energy (BLE) on board. It has an open-source operating system called Raspbian, which is Linux-based. It also has 40-pins from which 24 are GPIO pins used for general purposes. It has a Micro-USB power source, and it runs on a 5V power supply.

Arduino Mega 2560

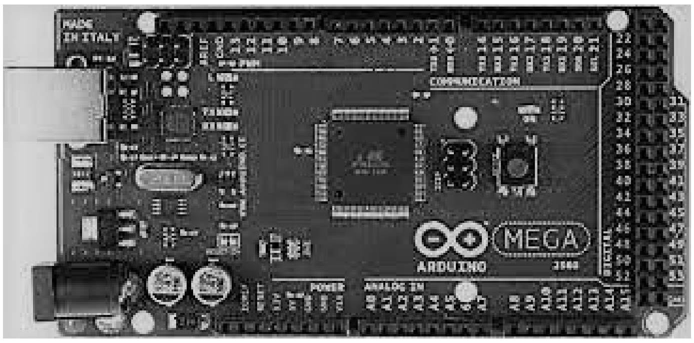

Figure 3. ***Arduino Mega***

Arduino is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software. Arduino Mega 2560 is a micro-controller board made for more complex projects. It has 54 pins out of which 14 can be used as Pulse Width Modulation(PWM) outputs, 16 analog input pins, Universal Asynchronous Receiver/Transmitter(UART) ports, 16MGHz Crystal Oscillator, a power jack, and a reset button.

Epressif ESP8266

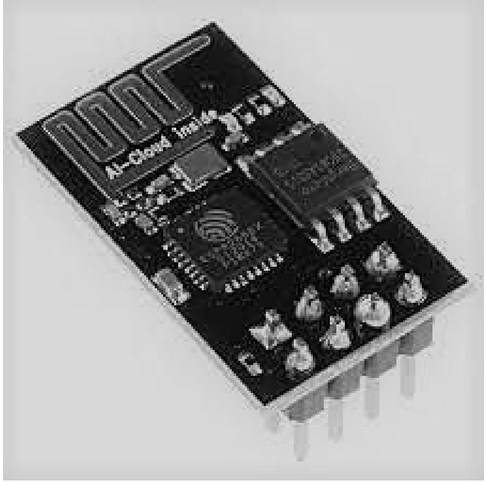

Figure 4. ***Epressif ESp8266***

Epressif ESP8266 is a cost-efficient Wi-Fi microchip that has full TCP/IP stack and micro-controller capabilities. It allows microcontrollers to connect to Wi-Fi and make effortless TCP/IP connections. It has 32KiB instruction RAM and 80KiB user data RAM, and 16 GPIO pins.

Keypad

Attach matrix 7-pin interfaces to 7 free GPIO pins. 3 column pins are set as output, which is directly connected with GPIO, while 4-row pins are set as input with a pull-up resistor.

Raspberry pi camera module

This camera module is an add on to the Raspberry Pi, which can take 1080p videos and tranquilized images. It uses the CSI interface, which is capable of extremely elevated data rates, and it carries pixel data. The sensor has a resolution of 5 megapixels and a fixed focus lens. the camera is capable of 2592 x 1944- pixel static images, and supports 1080p30, 720p60 and 640x480p60/90 video

The proposed system uses the following softwares:

Cayenne

Cayenne is a programming system for IoT which uses the drag and drop method for building programs. It also systemizes the connection of devices like motors and sensors and also keeps the drivers in place. We used the Cayenne MQTT python library which helps in sending and receiving data from the cayenne using raspberry pi.

Open CV

OpenCV is a reference center of programming languages, mainly aimed at computer visions and machine learning. It is built to provide a common base for computer vision applications and to speed up the use of the machine approach. As per our project, we used the LBPH(Lower Binary Pattern Histogram) face recognizer.

Algorithms

In the proposed model, OpenCV is being used (Open Source Computer Vision) which is an open source computer vision and machine learning software library. Haar Cascade Algorithm is primarily used for the face detection, the pretrained algorithm is offered by OpenCV.

Haar Cascade Algorithm

Haar Cascade is an object detection algorithm that uses a simple approach where the cascade function is trained to classify positive and negative images. The positive images are those where objects that need to be detected are present and negative is the opposite. It then detects objects in other images.

Haar Cascade extracts features such as ‘edge feature’, ‘line feature’ and ‘center surrounded feature’ from the images using a filter. Haar Cascades are similar to the concept of the convolutional kernel.

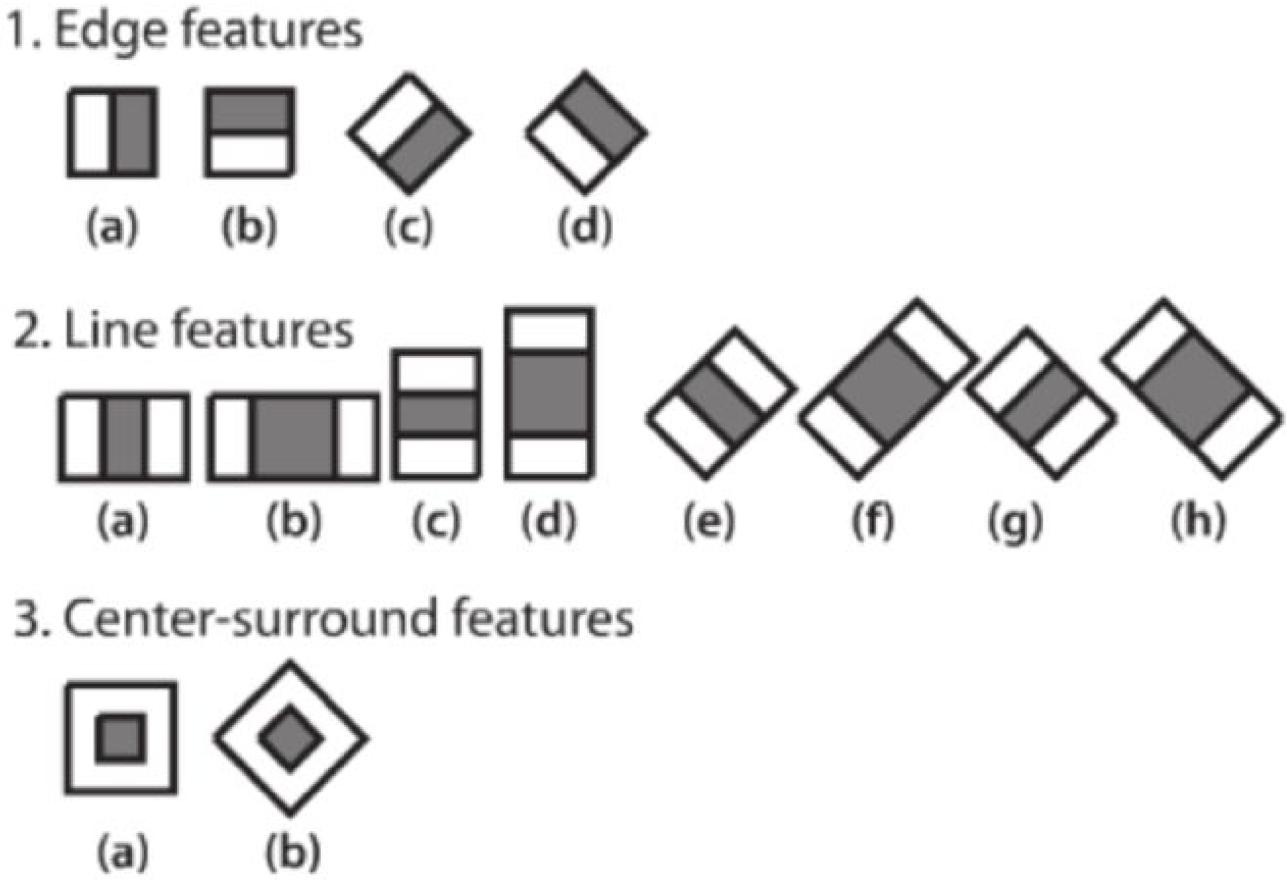

Figure 5. ***Cascade Classifier***

Each feature is represented as a single value obtained by calculating the difference between the sum of all pixels in the white rectangle from the sum of all pixels in the black rectangle (refer to fig.5). The various sizes and locations of the classifier becomes an increasing issue as the computational size increases. To overcome this issue, Image processing integral data which is a summed area table and algorithm is used for faster and more efficient sum generations.To avoid the overall complexity, OpenCV offers Adaboost machine learning algorithm as an in built feature for reducing the redundancies of classifiers. This increases the overall speed of the haar cascade classifier.

The features are divided due to the large numbers and are tested stage by stage. The initial stage generally consists less haar like features and if failed it is discarded and the following stages will not be tested. The region that passes all the stages is treated as the detected face.

Eigenface Classifier

If a single face is detected using the haar cascade classifier, the face wll be cropped out of the scene. The Eigen classifier, having been trained by the prestored library will try to recognize the cropped face and return the confidence of its prediction. We can determine when to acknowledge that the face is truly recognized by setting a threshold.

Though the input could be noisy with different angle, position and intensity of light, the image can be recognized according to the position of the eyes, face, and mouth in the face, and also considering the relative distances between each other. These features are called eigenfaces and can be extracted from original image by principal component analysis. Each face is represented by a subset of eigenfaces and the face can be reconstructed if the eigenface can be correctly calculated for each proportion. The new image is recognized based on eigenvectors and the euclidean distance between the eigenvectors.

Implementation

The physical connections of the proposed model can be done as shown in Fig.7

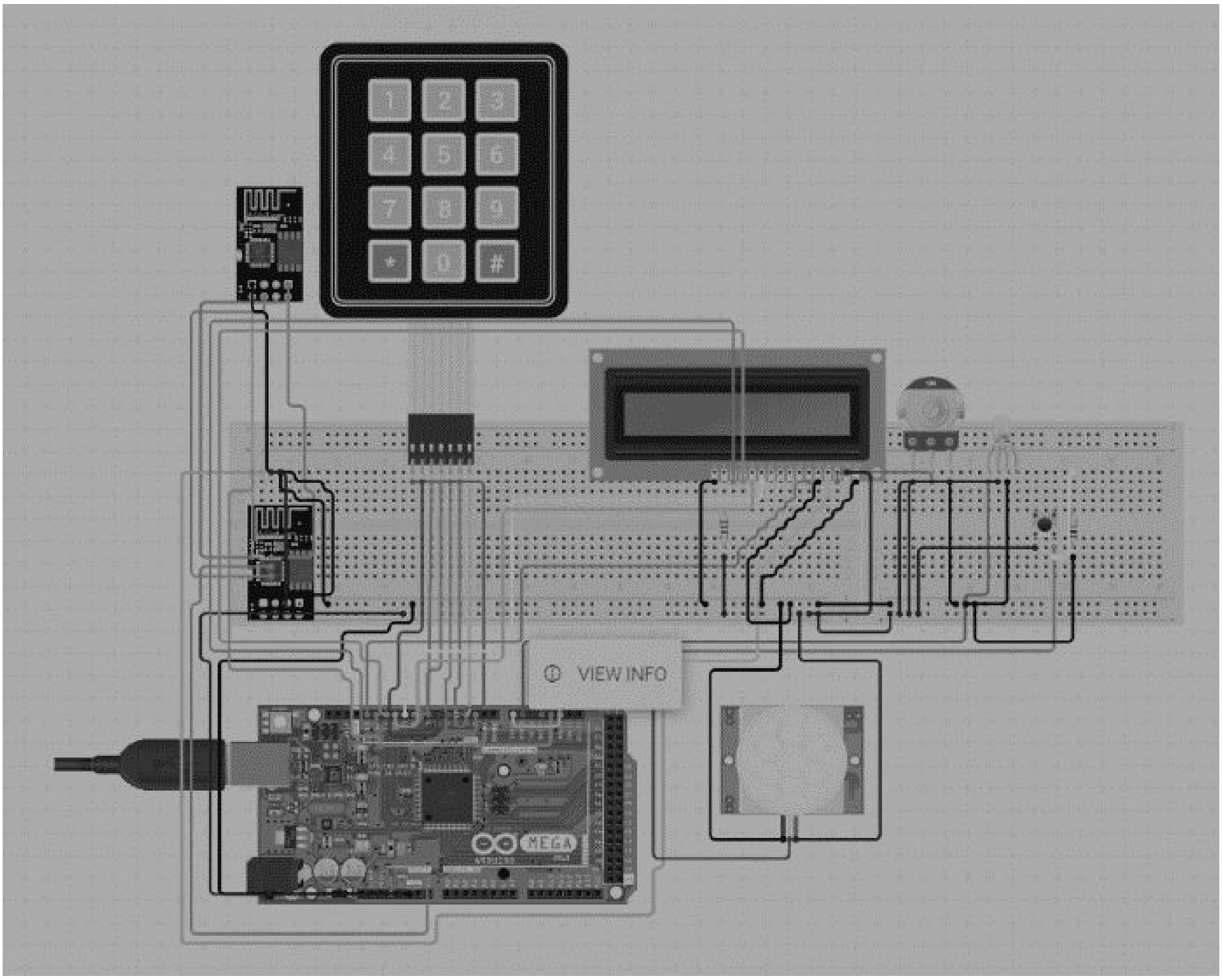

Figure 6. ***Connections***

The implementation is of the proposed model is quite simple. Initially, when the guest presses the pushbutton, the facial recognition system is triggered and comes into play. The Raspberry pi Camera Module then takes a picture of the arrived guest as coded into the Rasbperry pi. The picture is then matched with the already existing snapshots of family and friends in the database. If the face has been recognized the door is unlocked for 3s before being locked again. If the face is not recognized the user is notified through an sms and another notification along with the picture is sent to the user via email. The user can then access his the Cayenne app on his phone to perform an action from the given options of unlocking the door or taking no further action and keeping the door locked as shown in Fig.8.

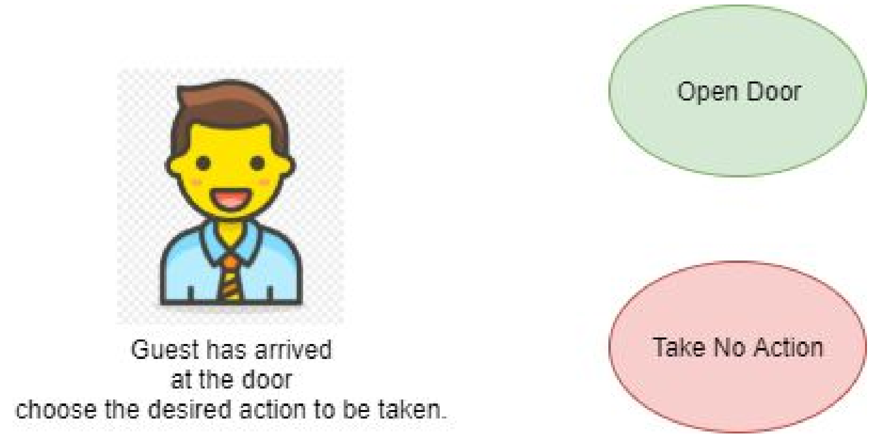
Guest has arrived
at the door
choose the desired action to be taken.

Figure 7. ***User Interface***

If the user chooses the option of “open door”, the door is unlocked for 3s before being locked again. If the option chooses to “take no action”, then the door remains locked. The model is also assigned a back-up option in case of improper functioning of the facial recognition system, this is the passcode option. As the name suggests, the arrived guest is asked to insert a passcode. If the passcode that is generated by the resident through the app when the guest lets the resident know that he has arrived. If the entered passcode is correct, the door is unlocked. If it is incorrect the door remains locked.

To perform the IoT functions, an ESP8266 wifi module is connected to the Arduino Mega microcontroller on to which the code is uploaded. The triggers produced by the devices connected to the Arduino cause the Rasperry pi to respond and the triggers from the Raspberry are sent back to the Arduino and notifications are sent to the user via sms and email.

Conclusion

In this paper, we have discussed our model, 'smart door lock,' which uses face recognition and a pin to allow access. This is a low-cost authentication system based on Raspberry pi. This system makes granting access to hassle-free and user-friendly at a low cost. The system primarily replaces traditional locks that use mechanical keys or RFID, thus being diminishing the fear of misplacing these objects. It not only eases access but also allows constant monitoring. The motion sensor notifies the user when there is any unusual activity. This, in turn, adds as an additional layer of security.

Acknowledgments

We express our sincere thanks to Dr. P Vijaya, Department of Computer Science & Engineering, Waljat College of Sciences, for her valuable guidance.

References

1. Liu, S., & Silverman, M. (2001). "A practical guide to biometric security technology." IT Professional
2. Pavithra.D and Ranjith Balakrishnan (GCCT 2015), "IoT based Monitoring and Control System for Home Automation," 2015 Global Conference on Communication Technologies
3. Kumari, Pushpanjali & Goel, Pratibha & Reddy, S.. (2015). PiCam: IoT Based Wireless Alert System for Deaf and Hard of Hearing. 39-44. 10.1109/ADCOM.2015.14.
4. H. Lee, C. Lin, and W. Kim, (2016). "Development of an IoT-based visitor detection system," *2016 International SoC Design Conference (ISOCC)*, Jeju, 2016, pp. 281-282.
5. Pooja A. Dhobi and Niraj Tevar, (2017). "IoT BASED HOME APPLIANCES CONTROL," IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC)
6. R. G. Anvekar and R. M. Banakar (2017). "IoT application development: Home security system," *2017 IEEE Technological Innovations in ICT for Agriculture and Rural Development (TIAR)*, Chennai, 2017, pp. 68-72.
7. Balla, Prashanth & Jadhao, K.. (2018). IoT Based Facial Recognition Security System. 1-4. 10.1109/ICSCET.2018.8537344.
8. Caroline Ek Fiorenza, Srushti Bompelli, Madhumita Sampath, Maithili Ghogre, Aravind Ajithkumar, "IOT SMART DOORBELL SURVEILLANCE," IJARIIE-ISSN(O)-2395-4396, VOL-4 Issue-2 2018.