International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 08 | Aug 2018 www.irjet.net p-ISSN: 2395-0072

Securing an IoT based Home using Digital Image Processing and an Android Application

Hardik Asnani[1], Suhaib Khan[2], Suhaas Nandeesh[3], Prarthana T.V.[4]

[123]*Student, B.E. Final Year, Dept. of Computer Science & Engineering, B.N.M.I.T, Bengaluru, Karnataka, India*
[4]*Assistant Professor, Dept. of Computer Science & Engineering, B.N.M.I.T, Bengaluru, Karnataka, India*

Abstract - *Making effective use of the domain of Internet of Things (IoT), Digital Image Processing and Android Platform, the proposed system provides an automatic system to control and secure home. The proposed system consists of three major modules namely the IoT based hardware components, the Server and the Android application. PIR Sensor is connected to the Raspberry Pi which is placed in the frame of the door. PIR Sensor detects the motion which leads to the image of the person being captured by the Pi Camera who intends to enter the house. The captured image is then sent to the server. Image analysis is performed by face detection followed by face recognition which matches the captured image with the stored dataset of authentic people of the house using the cascade classifier based on Viola-Jones algorithm followed by LBPHF recognizer. If the captured image matches the stored image in the dataset, then the door automatically gets unlocked without any human interaction. Otherwise, an alert message is sent to the owner via SMS. The owner, after getting the SMS, can take an action using the Android application installed in the phone. The owner has to log in to the application using a four-digit pin. The options available to the owner are Accept, Reject, and Buzzer. An accuracy level of 93.33% was achieved by the proposed system.*

Key Words: IoT; Digital Image Processing; Android; PIR Sensor; Raspberry Pi; Face Detection; Face Recognition.

1. INTRODUCTION

Security hardware of a home includes doors, locks, alarm systems, lighting, motion detectors, security camera systems, etc. that are installed on a property. Home security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm. Internet of Things (IoT) conceptualizes the idea of remotely connecting and monitoring real world objects (things) through the Internet. When it comes to the house, the concept can be aptly incorporated to make it smarter, safer and automated. The need of security systems for home is considered as one of the important aspects of our life. These systems could be motion detectors, monitoring cameras, door or window sensors, or image analysis. The security system consists of two steps:

• Sensor-based systems which uses movement sensors to detect the motion such as PIR Sensor in the proposed system.

• Motion-based systems such as Pi camera to capture the image for image analysis in the proposed system.

The captured image is sent to Raspberry Pi in the proposed system which in turn sends it to the Flask based Python Server. The captured image is processed by the face detection sub-module. Once the face in the captured image is detected, it is cropped and the processed facial image is sent to the face recognition sub-module.

The face recognition sub-module makes use of that facial image to check if it belongs to one of the residents of the house. If that image belongs to one of the resident of the house, then the door will automatically get unlocked. Otherwise, the facial image is sent to the Android application. The owner of the house receives a SMS on the smart phone. Using the Android application, the owner can see the facial image of the person standing at the door. Android application, along with image viewing capability, also provides three options:

1) Accept Button: Owner can press the Accept Button to authorize the person standing at the door to enter the house. This leads to the automatic unlocking of the door.

2) Reject Button: Owner can press the Reject Button to unauthorize the person standing at the door. This leads to the door remaining locked.

3) Buzzer Button: Owner can press the Buzzer Button if the owner suspects that the person standing at the door is an intruder. This not only unauthorizes the person standing at the door which leads to the door remaining locked but also triggers a buzzer which alerts the neighbors about a possible intruder in their locality.

2. LITERATURE REVIEW

Previous research conducted on home security system includes sending of alerts to the user. The system is modelled for intrusion and fire detection. It is equipped with a Passive Infrared Sensor (PIR) which detects motion and alerts are sent to the user by Twilio's web

service API. Twilio messaging service is a paid service and the system is not easily scalable [1]. This system alerts and sends the status to the Wi-Fi connected microcontroller managed system. Alerts and the status of the IoT system can also be received by the user on his phone from any distance irrespective of whether his mobile phone is connected to the internet or not. The system does not make use of camera. Due to this the person at the door cannot be judged by the user whether he is an intruder or a guest [2]. The system has model driven development process for home security. It remarks the uses of customer's end application such as Telegram to securely transmit information through layers of IoT architecture. The system also assists in presence detection, identification and authentication of stranger. It requires internet at both ends in order to work [3]. The system enables the user to monitor visitors in real-time, remotely via the IoT-based doorbell installed near the entrance door. If an outsider breaks into the house, the system can help identify the trespasser by acquiring CCTV evidence and the system can be used to report to the police or home security service provider immediately when a trespass occurs. The system is limited as it can use only one webcam to authenticate the visitor [4].

Another study was also conducted regarding the security issues in the IoT systems. Though IoT components contribute to address various societal challenges and provide new advanced services for users, their limited processing capabilities make them vulnerable to well-known security and privacy threats such as eavesdropping, impersonation, etc [5]. Smart home technology provides automated, intelligent, smart, innovative and ubiquitous services to residential users through Information Communication Technology (ICT). New security, authentication and privacy challenges are created. Possible security attacks are Message Alteration, Interruption, Tampering Malicious software and DoS Attacks [6].

Another research was conducted which was capable of monitoring sensors and autonomously controlling actuators, such as robots, unmanned aerial vehicles/ground vehicles (UAV/UGV) to flexibly construct security services. In this system, Agent-based infrastructure for IHSS using IoT devices and Role and task-based dynamic security service construction are proposed. In this system, intruder may breach the door, UGV might prove insufficient or chasing might be an unsuccessful [7].

This research designs and implements face detection using template matching algorithm and face recognition system based on PCA algorithm. The design is proposed for application in the smart home security system. Certain disadvantages of template matching algorithm are its more algorithmic complexity, difficult Structure and fetching of results slowly [8].

3. PROPOSED SYSTEM

The proposed system consists of three major modules namely the IoT based hardware components, the Server and the Android application. IoT based hardware components include PIR Sensor, Pi Camera, Buzzer, LED and Wireless Router for motion detection, image capturing and opening the door or keeping it closed; Server includes Flask based Python Server, face detection by HAAR Cascade Classifier for frontal face detection, face recognition by LBPHF Recognizer, Dataset, Firebase, Google Cloud SDK and Web Sockets for authentication of the person standing at the door and an Android application for authorization by the owner of the house.

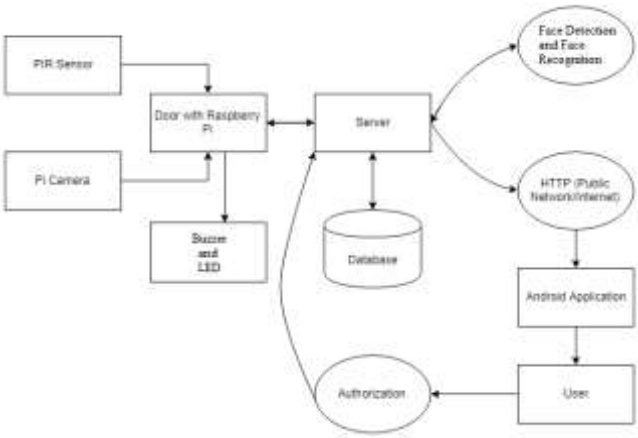

Figure 1 shows the complete System Architecture.

Fig -1: System Architecture

PIR Sensor is responsible for motion detection and once it detects the motion, it notifies Raspberry Pi about it. Pi Camera is initiated to capture the image of the person standing at the door. Once the image is captured, it is sent to Raspberry Pi for further processing. Now Raspberry Pi sends the image to the server. Server has the face detection sub-module which makes use of the HAAR Cascade Classifier for the frontal face detection. Once the face is detected, the processed image is sent to the face recognition sub-module which makes use of the LBPHF Recognizer to see if the image belongs to one of the residents of the house. If authenticated, door unlocks automatically. Otherwise, facial image of the person standing at the door is sent to the Android application. The Android Application gives the power to the owner of the house to authorize the person standing at the door. If authorized, the door unlocks and the person standing at the door gets the access to the house. If not, the door remains locked and the person standing outside the house is not allowed to enter the house. Also, if the

owner suspects that the person standing at the door could be a possible intruder, then a buzzer is triggered to alert the neighbors about the intruder in their locality. Figure 2 shows the Data Flow between Major Modules of the proposed system.

Dataset

The system uses a set of images of the people staying in the house. These images are stored in a local computer. The image from the Pi Camera is sent to the Raspberry Pi which in turn sends it to the server where the computation is done. Images are the major requirement in the process of home security. Images are taken in different lighting situations and different angles. Minimum 300 photos of each individual of the house are taken. The images can be of any resolution based on the camera. The proposed system uses Pi Camera which has the following specifications:

- 2592 x 1944 resolution (5.0 Megapixels).
- Horizontal field of view- 110°.
- Vertical field of view- 80°.

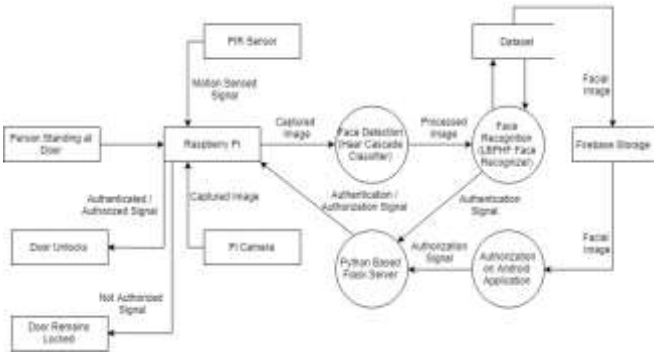

Fig -2: Data Flow between Major Modules

4. IMPLEMENTATION DETAILS

The experimental set up for the proposed system is shown in the Figure 3. The Wi-Fi Router is used to create the local network in order to facilitate the working of the proposed system.
The PIR motion sensor focuses any infrared radiation present around it toward the infrared detector. Human bodies generate infrared heat, and as a result, this heat is picked up by the motion sensor.

When the PIR motion sensor detects a person, it outputs a 5V signal to the Raspberry Pi through its GPIO and we define what the Raspberry Pi should do as it detects an intruder through the Python code. Here we are just printing "Intruder detected 1" as shown in Figure 5.

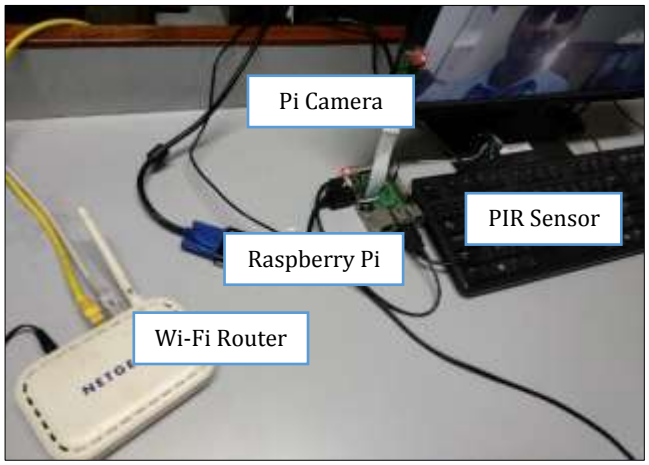

Fig -3: Experimental Setup

Once the motion is detected, the Raspberry Pi initiates the Pi Camera to capture the image of the person standing at the door. The Pi Camera starts up and captures the image. The Pi Camera is also sent to sleep so that the images captured can be processed at the server side either for authentication or for authorization. Figure 6 shows the Pi Camera Module capturing the image.
Now, the Flask based Python Server keeps on running and is waiting for the request from the Raspberry Pi. When an image is posted to the Flask Server from the Raspberry Pi, the image gets stored in the file on the Server.

Fig. 4: No Intruder Detected

Fig. 5: Intruder Detected

Face detection is a computer technology being used in a variety of applications that identifies human faces in digital images. The method used in the proposed system is a cascade classifier, which can be loaded with a pretrained xml file.

The latest image captured is read from the server and is converted to grey scale image. After that, the face is detected in the image using the Viola-Jones algorithm. Once the face in the image is detected, the facial region from the image is cropped out.

Fig -6: Pi Camera Capturing Image

Once this process is over, the process of face recognition begins. A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video frame from a video source. For face recognition to work, firstly, dataset has to be created; secondly, a trainer has to be programmed to train the recognizer and thirdly, a detector has to be programmed which matches the facial image with the trained file of histograms of the images in the dataset. Dataset creator creates the dataset generator script using the cv2 library, images of the authentic people and the cascade classifier object. Now comes the training part which is done using LBPHF recognizer. Trained data is created and stored as .yml file which is later used during face recognition and the process is as follows:

1. A new facial image is fed to the recognizer for face recognition.
2. The recognizer generates a histogram for that new facial image.
3. It then compares that histogram with the histograms it already has.
4. Finally, it finds the best match and returns the person label associated with that best match.

If the successful match is found, the Raspberry Pi opens the door for the authenticated person standing at the door. Otherwise, if the match is not found, the coloured cropped facial image is uploaded to the Firebase with the help of Google Cloud SDK. Firebase will always store the latest image sent from the Server. This image is ready to be sent to the Android application developed.

The owner of the house will now get a SMS to check the Android application to authorize the person standing at the door. The login screen consists of a four-digit passcode to be entered in order to login to the Android application as shown in Figure 7.

Fig -7: Login Screen of Android Application

The owner of the application has three choices: Accept, Reject or Buzzer as shown in Figure 8. The Android application sends a signal to the Python WebSocket which in turn sends the signal to the Flask based Python Server about the decision taken. The Accept button is used to send signal that the person is known to the owner. The Reject button is used to send signal that the person is not known to the owner. The buzzer button is used only when the image is of an intruder as suspected by the owner and also there is a chance of some unfriendly activity to occur.

5. RESULTS AND ANALYSIS

In the proposed system, following are the scenarios and their associated results:

Scenario 1: An authentic person is standing at the door.

The facial image sent to the face recognition sub-module of the Server which will confirm that the person standing at the door is an authentic one.

Result 1: In this scenario, the door will get unlocked automatically.

Scenario 2: An unauthentic person is standing at the door and the owner authorizes the person.

The facial image is sent to the face recognition sub-module of the Server which will confirm that the person standing at the door is an unauthentic one and the facial image is sent to the owner's Android application for authorization. The owner authorizes the person standing at the door by pressing the Accept Button.

Result 2: In this scenario, the door will get unlocked. Also, a Green LED will light up to demonstrate the successful authorization.

Fig -8: View Screen of Android Application

Scenario 3: An unauthentic person is standing at the door and the owner does not authorize the person.
The facial image is sent to the face recognition sub-module of the Server which will confirm that the person standing at the door is an unauthentic one and the facial image is sent to the owner's Android application for authorization. The owner does not authorize the person standing at the door by pressing the Reject Button.
Result 3: In this scenario, the door will remain locked. Also, a Red LED will light up to demonstrate the successful un-authorization.
Scenario 4: An unauthentic person is standing at the door and the owner suspects that person to be an intruder.
The facial image is sent to the face recognition sub-module of the Server which will confirm that the person standing at the door is an unauthentic one and the facial image is sent to the owner's Android application for authorization. If the owner suspects the person standing at the door to be an intruder and he also wants to alert the neighbors about this intrusion, then he can do that by pressing the Buzzer Button.
Result 4: In this scenario, the door will remain locked along with a Buzzer beeping to alert the neighbors about an intruder in their locality. Also, a Red LED will light up to demonstrate the successful un-authorization.

6. PERFORMANCE EVALUATION

The dataset of the people belonging to the house has been trained and stored as histograms in a .yml file. Once the processed image from the face detection sub-module is sent to the face recognition sub-module, then the face recognition sub-module predicts the ID and the Confidence Value of the facial image. The Confidence Value in the proposed system is set at 30. So, if the image of the person standing at the door has a predicted confidence value less than 30, then the person is authenticated and the door automatically unlocks. Otherwise, the person is unauthenticated and finally the facial image is sent to the owner's Android application for authorization of the person standing at the door.

The proposed system considered an authentic person (resident of the home) standing at the door. System was tested for 30 times out of which the system recognized the person to be an authentic one 28 times i.e., the face recognition sub-module predicted the confidence value less than 30. Hence an accuracy of 93.33% was achieved.
The proposed system considered an unauthentic person (not a resident of the home) standing at the door. System was tested for 30 times out of which the system recognized the person to be an unauthentic one 27 times i.e., the face recognition sub-module predicted the confidence value greater than 30. Hence an accuracy of 90% was achieved.

Time taken for an authentic person standing at the door for whom the door will get unlocked automatically is approximately 12 seconds. Time taken for an unauthentic person standing at the door for whom the authorization is required by the owner of the house is approximately 40 seconds using the Android application.
The proposed system is fool proof in a way that if an unauthentic person or an intruder tries to show a 2D image of the authentic person (resident of the home) to the Pi Camera in order to gain access to the house, then the face recognition sub-module is smart enough to judge that it's a 2D image and not the real person standing at the door. As a result, the predicted confidence value is greater than 30 even if the image captured was of the authentic person. This way, the proposed system cannot be fooled to gain the access to the house in an inappropriate way.

7. CONCLUSION

Internet of Things is gaining vast focus in the field of technology wherein large number of devices are being connected to each other. These devices can communicate with each other over internet in order to transfer data and are finding great usefulness in providing home security too.

The IoT based components sense the motion of the person standing at the door which in turn leads to the capturing of the person's image. This image is sent for processing by the face detection and face recognition sub-modules of the Server. If the face is recognized to be the one belonging to one of the resident of the home, the door gets automatically unlocked. Otherwise the facial image of the person is sent to the owner's Android application from where the owner can take three actions

for authorizing the person standing at the door i.e. the owner can press the Accept button, the Reject button or the Buzzer button.

When an authentic person stands at the door, the system has an accuracy level of 93.33% to unlock the door automatically. In case of an unauthentic person, the system has an accuracy of 90% to keep the door locked and sending the image to the owner's Android application for authorization. Also, the system takes approximately 15 seconds for successful authentication and approximately 40 seconds for successful authorization from Android application. The proposed system is also fool proof in a way that it is capable of differentiating between a 2D image and an actual person standing at the door. The system does not unlock the door even if the 2D image belongs to that of the authentic person of the house.

The three domains namely IoT, Digital Image Processing and Android Platform have been efficiently used to provide Home Security because home is a prised possession in one's life and it is one's prime responsibility to protect it.

8. FUTURE WORK

The proposed system is a simulation of the real-world system. All the devices used are connected to the same local network along with the smart phone containing the Android application.

Future work is suggested to be:

1. Empowering the system to perform in a real-world, by providing support for authorization by the owner, from remote locations.

2. Support for turning on an automatic light to capture images of the person standing at the door (in case of dim lighting).

3. Support for viewing the images of all the people who have visited the owner's house till date in the Android application.

4. Support for recognizing the authentic person of the house standing in a group of people in front of the camera which leads to the automatic unlocking of the door.

5. Further improvement in accuracy by making use of Machine Learning Algorithms.

REFERENCES

[1] Supreeta Venkatesan, Dr. A. Jawahar, S. Varsha and Roshne N., "Design and Implementation of an Automated Security System using Twilio Messaging Service", 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems Yogyakarta, Indonesia, November 08-10, 2017.

[2] Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose and Lakshmi Boppana, "IoT Based Smart Security and Home Automation System", International Conference on Computing, Communication and Automation (ICCCA2016).

[3] Raj G Anvekar and Dr. Rajeshwari M Banakar, "IoT Application Development: Home Security System", 2017 IEEE International Conference on Technological Innovations in ICT For Agriculture and Rural Development (TIAR 2017)

[4] Woo-Hyun Park and Yun-Gyung Cheong, "IoT Smart Bell Notification System: Design and Implementation", CACT2017 February 19 ~ 22, 2017.

[5] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino Gary Steri, and GianmarcoBaldini, "Security and Privacy Issues for an IoT based Smart Home", MIPRO 2017, May 22- 26, 2017, Opatija, Croatia.

[6] Waqar Ali, Ghulam Dustgeer, Muhammad Awais and Munam Ali Shah, "IoT based Smart Home: Security Challenges, Security Requirements and Solutions", Proceedings of the 23rd International Conference on Automation & Computing, University of Huddersfield.

[7] Zhaoqing Peng, Takumi Kato, Hideyuki Takahashi and Tetsuo Kinoshita, "Intelligent Home Security System Using Agent-based IoT Devices", 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE).

[8] Dwi Ana RatnaWati and DikaAbadianto, "Design of Face Detection and Recognition System for Smart Home Security Application", 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE).