IoT-Based Home Intrusion Detection System for Enhanced Smart Environment

Aman Shah, Rukmani Panjanathan, Graceline Jasmine, C. Rajathi, Modigari Narendra, and Benson Edwin Raj

Abstract An interconnected collection of smart devices which is expanding at a very rapid pace as many devices and sensors are being added to the inter or getting connected to it is referred to as Internet of Things or IoT for short. One of the most widely used part of IoT is integrating it in home security. The IoT increases the ability to control and monitor all the operations occur at home. This work aims at using the IoT features in creating an inexpensive home security system which tracks the digital footprint of all the visitors. Home security is an essential part of today's world, especially with all the technological advancements. Traditional systems detect the intrusion but not the intruder. The systems can be easily fooled by using physical props. Objective of this work is to enhance the current security system to detect the identity of the intruders digitally which can later be used by authorities to trace them easily.

Keywords Intrusion detection · Smart environment · IoT · Security

A. Shah · R. Panjanathan (✉) · G. Jasmine · C. Rajathi
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India
e-mail: rukmani.p@vit.ac.in

A. Shah
e-mail: aman.shah2017@vitstudent.ac.in

G. Jasmine
e-mail: graceline.jasmine@vit.ac.in

C. Rajathi
e-mail: rajathi.c2019@vitstudent.ac.in

M. Narendra
Department of Computer Science and Engineering, Vignan Deemed to Be University, Andhra Pradesh, India

B. E. Raj
Higher Colleges of Technology, Fujairah Women's Campus, Fujairah, UAE
e-mail: braj@hct.ac.ae

A. Kumar et al. (eds.), *Proceedings of the International Conference on Cognitive and Intelligent Computing*, Cognitive Science and Technology,
https://doi.org/10.1007/978-981-19-2350-0_78

1 Introduction

A home security system device protects both the expensive things and people's personal safety. Given the fact that IoT allows us to gather data from various types of sources including appliances, cars, humans, pets, etc., it is described as "Infrastructure of Information Society." In the world, all the objects which equipped with a physical IP, which allow exchange of information, can be able to be part of IoT system. IoT connections use the World Wide Web to allow items to communicate with one another using their logic and circuits; it is not the same as the Internet. In past few years, the number of gadgets being connected to World Wide Web has seen a tremendous boom. All these gadgets integrated with the Internet are associated with IoT and its infrastructure. This allows exchange of useful data and information between one another, and this is exactly why it is useful to use such preexisting hardware infrastructure which is our advantage for the proposed security system.

Utilizing Wi-Fi module as a test sniffer to gather all virtual impressions close by and classified into individual and non-individual. Individual gains admittance to house and others not. The logs of the occasion are dispatched to the proprietor through e-mail, and it is caught utilizing PyShark. JSON is used to impart among module and the server.

Wi-Fi module works by sniffing the incoming network packets to get the MAC address of devices in its vicinity. Face detection algorithm with OpenCV is used to distinguish faces of known family members quickly and accurately from possible intruders or outsiders. The details will be stored for future reference. The dual nature of the system allows us to first get the MAC address of the intruders even when their Wi-Fi [1] in the phones is off and even if they are covering their faces.

2 Related Work

IEEE 802.11 standard defines Wi-Fi probe requests as an active mechanism with which cellular gadgets can request data from access points and speed up the Wi-Fi connection process [2]. Researcher recognized the privacy risk which the previous label access point is not limited to the previous person. Wireless Sensors Networks (WSNs) with Internet of Things (IoT) and increasing home security ideas and solutions and also packages have been addressed. The researchers show that the concept of exploiting Wi-Fi probe request in which smartphones sends de-anonymize the starting place of the user [3]. Home Area Network [4] offers the function to continue connection for communication and data transfer. In [5], a method is recommended for estimating the range of cellular gadgets present at a positive vicinity and time through Wi-Fi probe. The study [6, 7] enforces real-time surveillance, tracking development of the house protection based on ZigBee era and GSM/GPRS network [3, 7]. Smart telephones have emerged as an essential part of our everyday lives because of their competencies of having access to the net in the use of Wi-Fi and cellular

record networks. These Wi-Fi devices continuously give out data packets known as probe requests, which may be traced in the use of Wi-Fi sniffers. In this thesis, first we investigate taking pictures of Wi-Fi probe request packets in the use of the assist of Wi-Fi Pineapple gadgets and examine how we will use sign electricity statistics of probe request records for indoor occupancy tracking by PyShark [1]. To enforce actual house protection, the shrewd faraway tracking machine turned into advanced for domestic protection primarily based totally on "ZigBee" era and GSM/GPRS community [6]. Wi-Fi probe requests present a unique privacy risk which researchers have recognized; this includes and is not limited to leaking a person's previous access point labels and their movements. Even though this shows us the privacy risks of using Wi-Fi probe requests, it is still in widespread use and other alternative technologies have not been used over this. In this work, the author quantifies Wi-Fi probe requests' threat to privacy by conducting an experimental study of the most popular smartphones in different settings.

3 Proposed System

The traditional tracking system is slow and difficult to get accuracy. The proposed system provides the advancement by using Wi-Fi module. Wi-Fi module tracks the footprints of the intruders by the devices. The Wi-Fi module present inside the house captures the probe requests sent by the devices to connect to any wireless network. All the MAC addresses of the members living in the house are stored in a list. The non-members like guests or intruders' MAC addresses will be identified and emailed to the owner so that he can keep a track of the people entering his house. Wi-Fi module is used to sniff the Wi-Fi probe requests from the visitor. Our system will identify the members and non-members from the retrieved MAC addresses. After differentiating them, the list will be shared via JSON and will be updated accordingly in the UI.

3.1 Architecture of the Home Intrusion Detection System for Enhanced Smart Environment

Wi-Fi module is utilized as a probe sniffer which collects the virtual footprints of all the close by gadgets and sends them to the station to get processed which categorizes them as individuals or non-individuals of the house. The individuals are granted get entry to get into the house, while the non-individuals are not. The log of these types of events is dispatched to the proprietor through e-mail. Alongside the Wi-Fi module which works by sniffing the incoming network packets to get the MAC address of devices in its vicinity, the system also utilizes a fast and efficient face detection algorithm with OpenCV using a model shipped with the library in order to detect faces using deep learning. It allows to quickly and accurately distinguish faces of

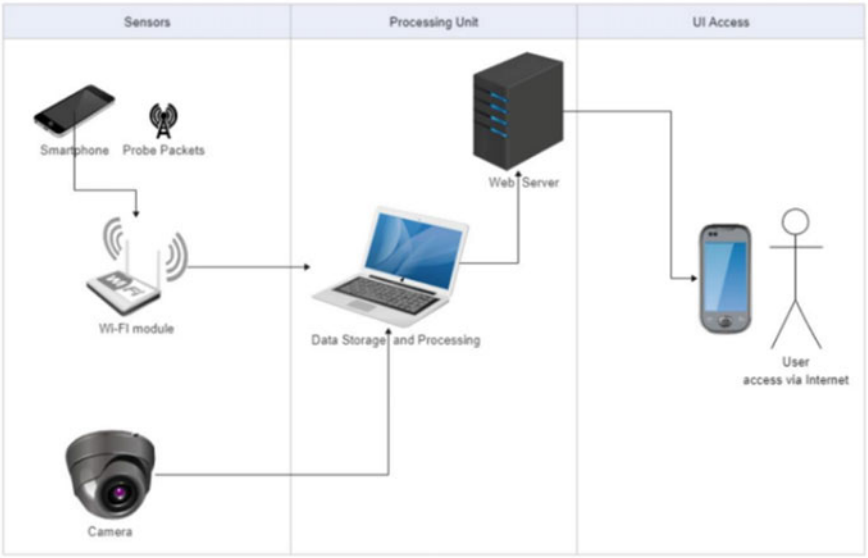

Fig. 1 System overview

known family members from possible intruders or outsiders. The system would then store the faces of all unknown individuals in a database for future use in order to help identify and apprehend the intruders. Wi-Fi module is used to sniff the Wi-Fi probe requests from the visitor. Our system will identify the members and non-members from the retrieved MAC addresses. After differentiating them, the list will be shared via JSON and will be updated accordingly in the UI. The overall flow is detailed in Fig. 1.

If the intruder is not carrying a smartphone, the system also has a video surveillance module with facial recognition model using OpenFace deep neural network to accurately recognize or identify intruders from family members. This dual nature of our system allows to detect any possible intrusions in the house in an intuitive but not intrusive manner. The system can be further upgraded to include additional modules like adding additional sensors like motion detectors, glass-break sensors, infrared sensors, etc. on an Arduino Uno microcontroller or a Raspberry Pi controller to allow installation of multiple sensors and to trigger an alarm or a notification using wireless connection via Wi-Fi or local Internet (Fig. 2).

4 Experimental Results

The MAC address is detected to sniff the packets detected to be intruders. The possible intruders are detected and are stored in the database. The webpage is rendered to find

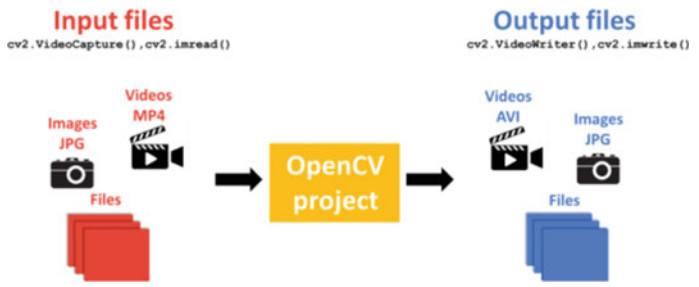

Fig. 2 Workflow for identifying intruders

the members and non-members using the MAC address. The output of the MAC detection is shown in Fig. 3.

Each image is iterated over and over in the training dataset to extract the face from the image using openCV face detection model and localize the faces in the training dataset. A blob is created for the face from the image and then passes it through the embedding model to create a 128-d quantification for it and store the embedding and name of the person to a list. The serialised face detector and the face embedding model are loaded in order to recognise and produce facial embedding for faces that appear in the video frames that the camera is recording. Create the webcam video stream and extract each frame for facial recognition. The recognized face and the accuracy are shown in the Fig. 4a. If an unknown face is seen by the model which does not match the faces listed in the training dataset, it saves it in memory as a possible intruder along with the date and time for future identification and is shown in Figs. 4b and 5.

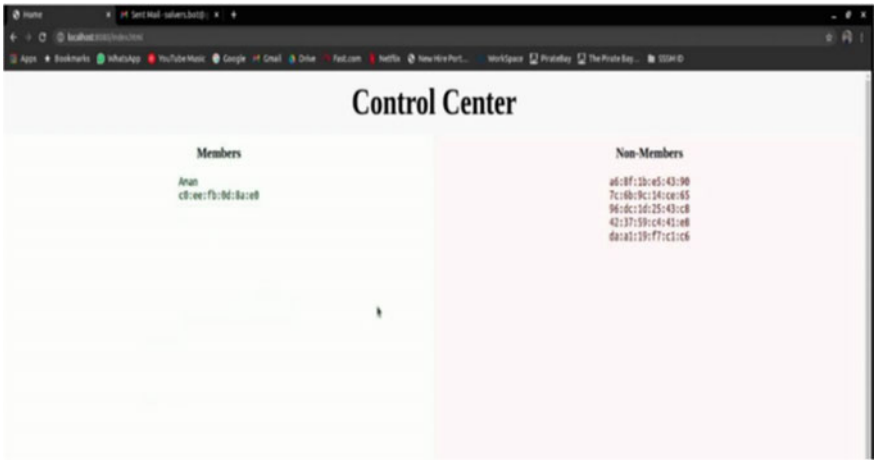

Fig. 3 Output of MAC detection

(a) (b)

Fig. 4 **a**, **b** Recognized face and accuracy

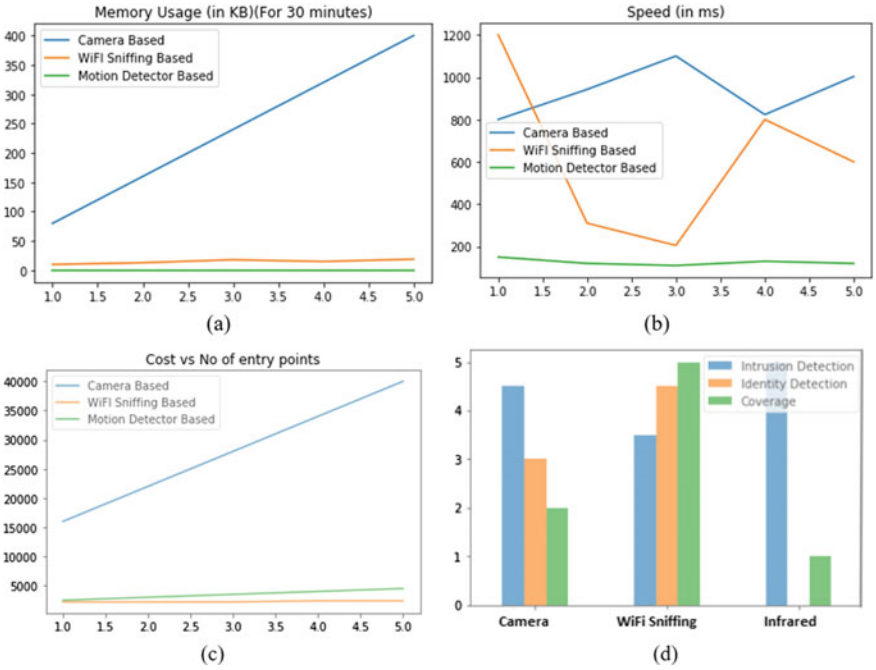

Fig. 5 **a**, **b** Memory usage and speed, **c**, **d**. Cost versus No of entry points and coverage

5 Conclusion

The Wi-Fi module present at homes will identify the members and non-members by capturing the Wi-Fi probe requests sent by their devices and checking with the database. By tracking the digital footprint of the people visiting the house, it is easier to track the identity of the intruder in case of any criminal activity like theft. The facial recognition model is working as intended such that it detects and recognizes

faces in indoor settings efficiently and stores any unidentified faces in its database. The video feed from the cameras can also be stored but currently we are storing only images for efficient storage management.

The created framework additionally can be used in business and business programs which incorporate workplaces, stockrooms, and various areas wherein a couple of locales are held for legitimate representatives just or various areas wherein insurance and safety measures are of number one concerns which incorporate net server room of a huge MNC from wherein organization records might be taken.

References

1. Anbarasi J, Mala A (2015) Verifiable multi secret sharing scheme for 3D models. Int Arab J Inf Technol (IAJIT) 12
2. Jadhav L, Pai V (2018) Smart home automation and security using internet of things
3. Ketchen DJ, Shook CL (2006) The application of cluster analysis in strategic management research: an analysis and critique. Strateg Manag J 17(6):441–458
4. Basem B, Ghalwash AZ, Sadek RA (2015) Multilayer secured SIP based VoIP architecture. Int J Comput Theory Eng 7(6):453
5. Ding C, Tao D (2017) Pose-invariant face recognition with homography-based normalization. Pattern Recogn 66:144–152
6. Julien F, Raya M, Felegyhazi M, Papadimitratos P (2007) Mixzones for location privacy in vehicular networks. In: Association for computing machinery (ACM) workshop on wireless networking for intelligent transportation systems (WiN-ITS)
7. Kerns AJ, Shepard DP, Bhatti JA, Humphreys TE (2014) Unmanned aircraft capture and control via GPS spoofing. J Field Robot 31(4):617–636