



School of Information Technology and Engineering (SITE)
B.Tech (Information Technology)

Project Report

Face recognition based home security

Submitted for the Course

ITE 4003 Internet of Things

Offered during FALL 2019

(Dr.R.K.Nadesh)

By

Surya K

16BIT0029

Shweta Vijay

16BIT0423

November, 2019

School of Information Technology & Engineering

B.Tech (Information Technology)

ITE 4003 Internet of Things - FALL 2019

A Report on the Course Project **"Face recognition based home security"**

TEAM Number :

Team Member(s) :

Team Leader:

Name: Surya K

Reg.no: 16BIT0029

Mob: 7598773664

Email: suryak.2016@vitstudent.ac.in

Team 1:

Name: Shweta Vijay

Reg.no: 16BIT0423

Mob: 9442568927

Email: shweta.vijay2016@vitstudent.ac.in

Project Title:

Face recognition based home security

1. Introduction

1.1. Background

Face recognition has been adopted by retail faster than any other industry. The Automated Regional Justice Information System (ARJIS) started supplying a mobile face recognition platform in 2014. In 2017, Iphone advertised its phone to the utmost with its face recognition security. Face recognition as such is becoming a security standard that people expect. While, passwords, pins or even a simple lock can prove to be a solution to this, the uniqueness of faces can be used as an application of IOT for the benefit of home security as it is a biometric trait. In this project we make use of this unique biometric to identify visitors and send a "smart notification" to the user. Users can register individuals whom they wish to permit entry to their homes as well as instantly communicate with the visitor through audio messages. By doing so, existing facial recognition based home security systems can be enhanced.

1.2. Problem Statement

A home security system is a line of defense a home can provide against intruders. There have been many attempts to develop an apt home security system. However, most systems fail to provide optimum security.

1.3. Importance

Installing a **home security** system means to protect the home and valuables, and to keep family safe from potential break-ins by burglars. A face recognition also has the added benefit of allowing users to keep track of general data of visitors.

2. Overview and Planning

2.1. Proposed System Overview

The proposed system is a face recognition based home security that allows immediate communication with unidentified visitors. Face recognition is a unique biometric that can be used to identify visitors and send a "smart notification" to the user. Users can register individuals whom they wish to permit entry to their homes as well as

instantly communicate with the visitor through audio messages. By doing so, existing facial recognition based home security systems can be enhanced.

It has the following innovative components:

- Use of commonly used messaging apps like telegram to notify users. This allows seamless integration of the system without users having to install specific applications for the security system.
- Most commercial products don't allow users instant communication with the unidentified visitors.
- Extendable - allows developers to extend functionalities by writing web-hooks.

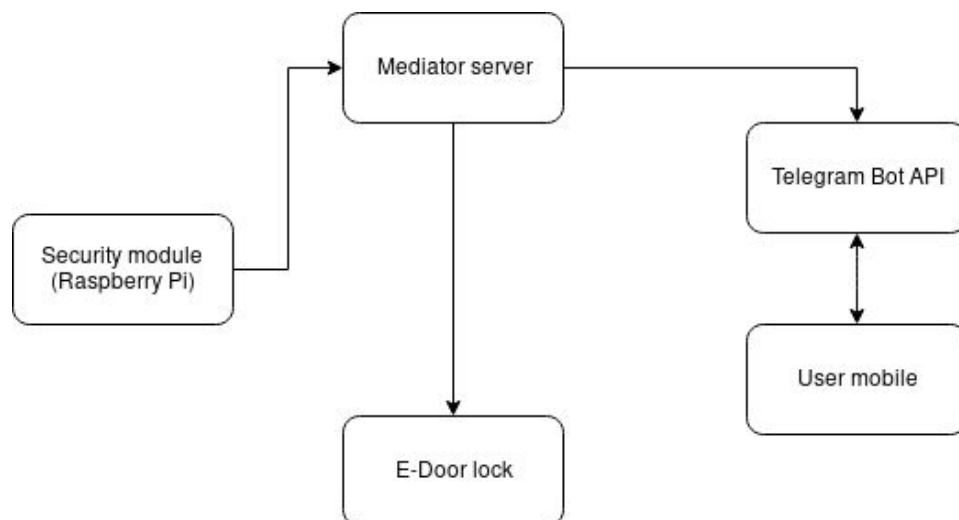
2.2. Challenges

Low latency face recognition algorithms that works in an one-shot fashion.

2.3. Assumptions

- The users of the system will use the telegram messenger.
- The users will have an active wifi access point at all times.

2.4. Architecture Specifications



Hardware Requirements

- Raspberry Pi
- Pi Camera

Software Requirements

- Telegram Bot API

- Python
- OpenCV
- DLib

2.5. Realistic Constraints and Standards

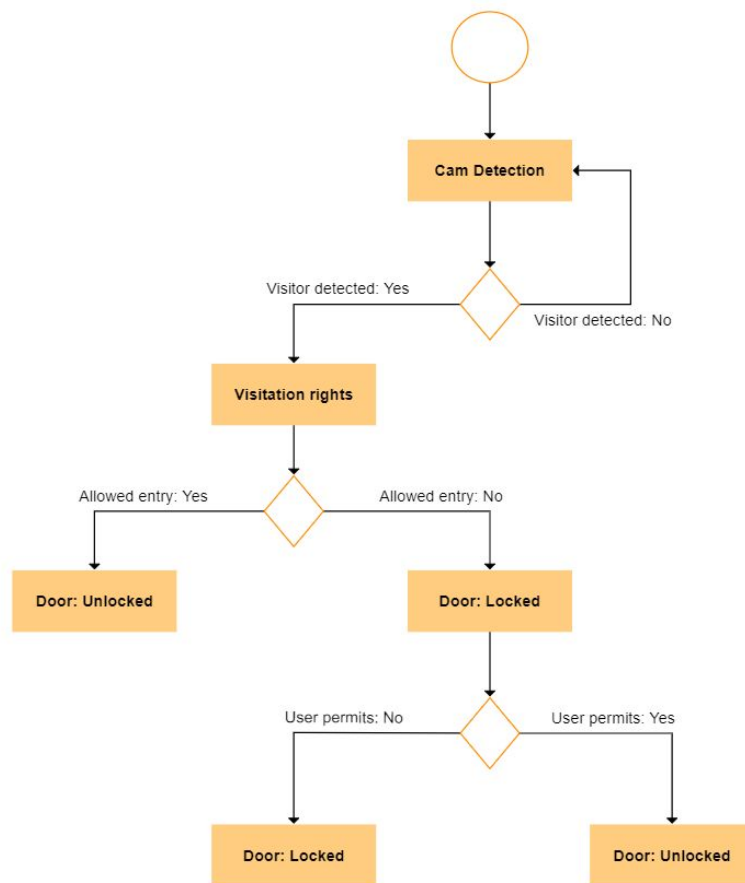
- The proposed system fails to work without an active wifi connection. The users are also required to have compatible messaging apps.
- The amount of data produced will be huge especially if a common database in the cloud is used. This can hamper processing speeds until technology catches up.

3. IoT Design Methodologies

3.1. Purpose & Requirements Specification

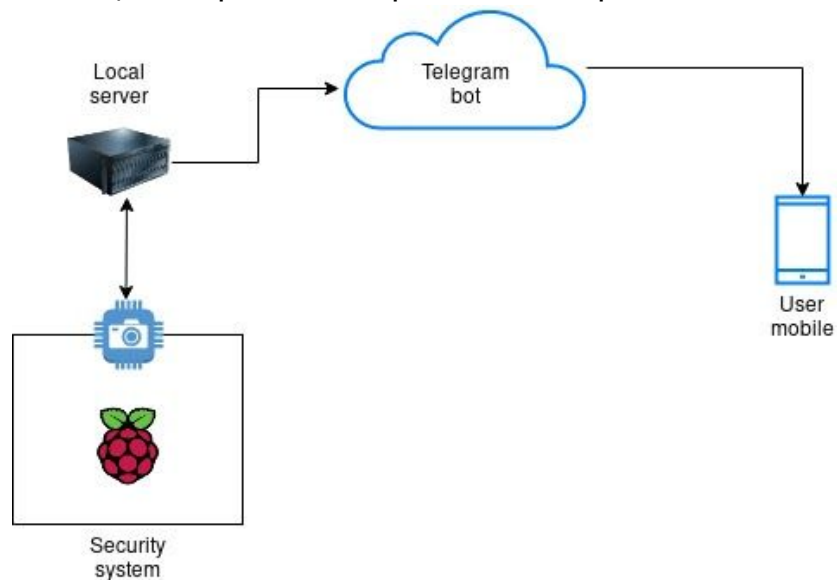
- Main purpose of the system is to provide home security
- The system must identify registered individuals and allow them entry.
- If the visitor is unidentified, then user must immediately be notified.
- Unidentified visitors should also have the option of contacting the user through the system.
- And if the system wishes to, he should be able to allow entry to the unidentified visitor from anywhere.
- Under no other circumstances should any visitors be allowed to enter the user's home.

3.2. Process Specification

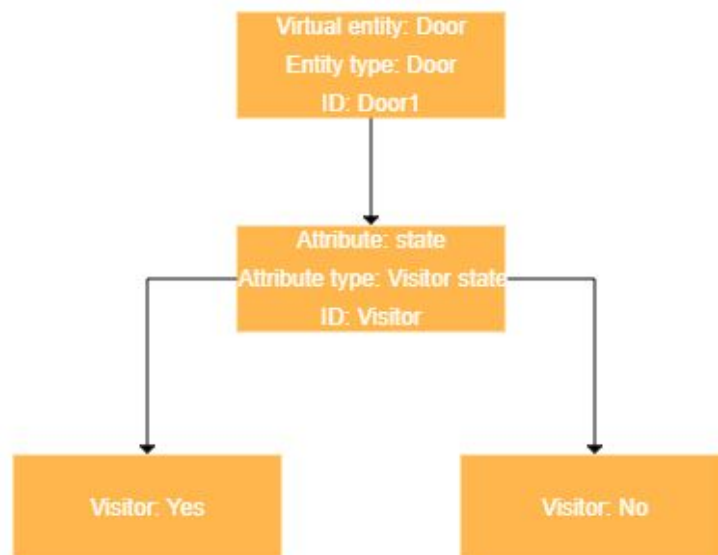


3.3. Domain Model Specification

Entities, concepts and components are represented below

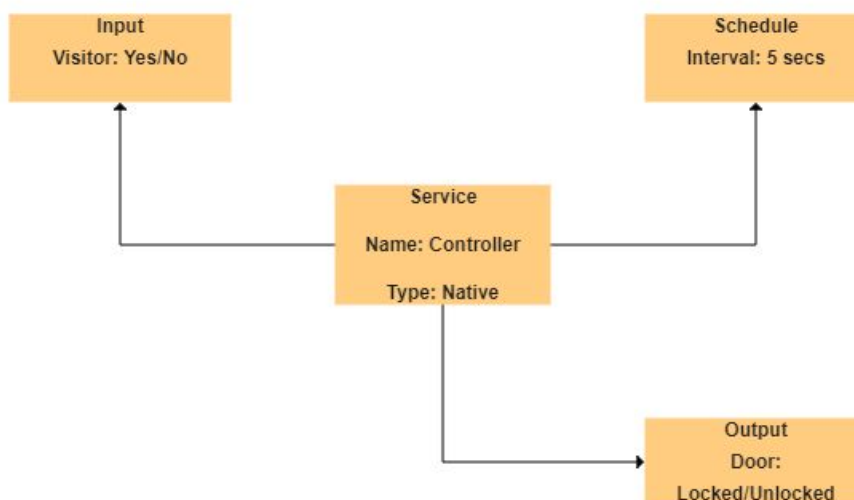


3.4. Information Model Specification



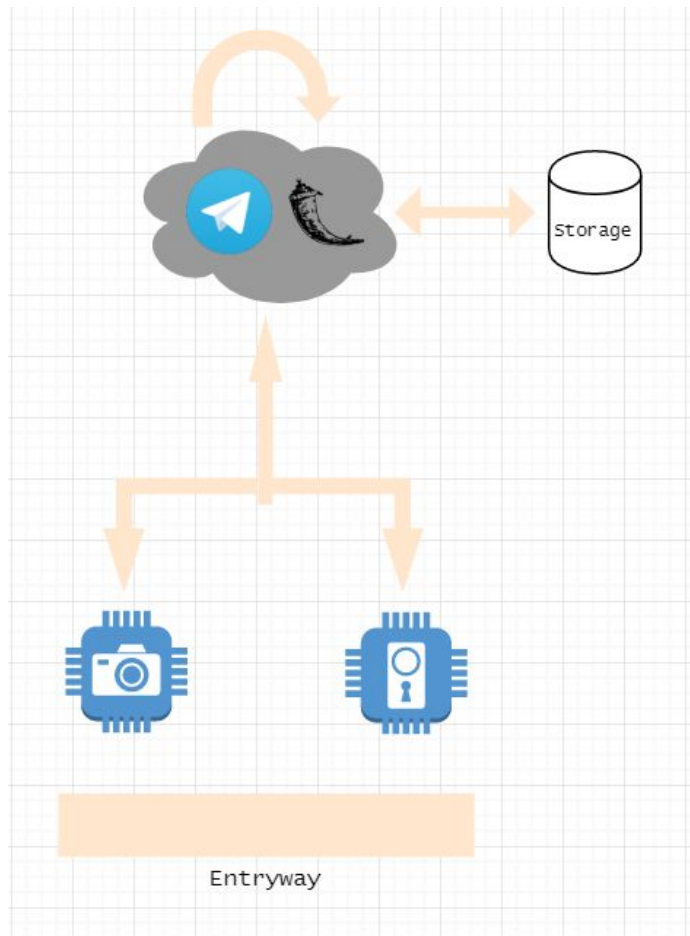
Controller: The control service monitors checks for the presence of visitors. If a visitor is present, it checks the database to see if the visitor has visitation rights. If not, the user is notified and the database is updated.

3.5. Service Specifications



3.6. IoT Level Specification

The system will be implemented at IoT Level 4, a mediator(web-server) will take the data from the camera sensor process it and relay the information to the owner. It'll also process the recognition algorithm. The registered faces will be present in a database present within the mediator. The communication between the owner and the visitor takes place through the instant messenger's (telegram) cloud service.



3.7. Functional View Specification

Device	In my "home intrusion detection system" the computing devices I am going to use are Raspberry Pi
Communication	HTTP, RTSP
Services	Controller service and Web service
Security	Telegram auth

3.8. Operational View Specification

Computing device	Raspberry pi, local server
Sensor	Camera
Actuator	Lock

Web services	REST service
Web app	Flask
Authentication/Authorization	Telegram auth
Communication protocols	Application : HTTPs, RTSP. Network : IPv4

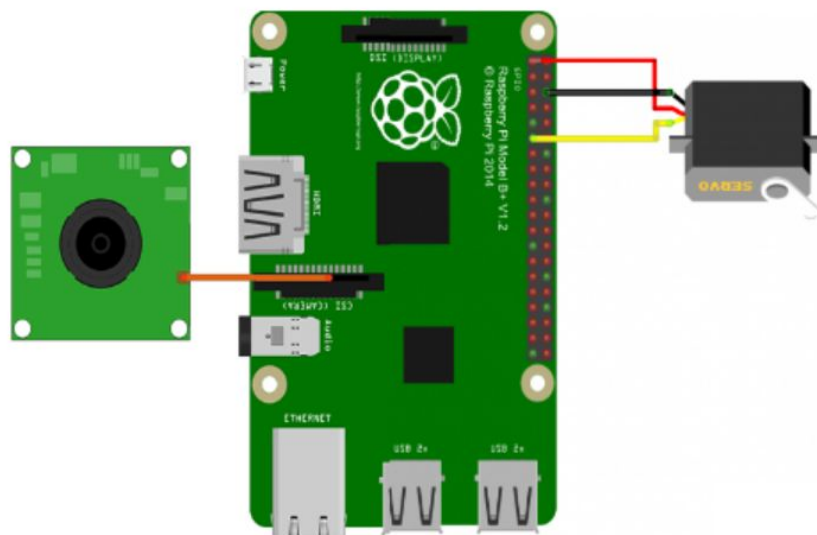
3.9. Device & Component Integration

All devices are integrated with an HTTP REST api. System is made modular, and abstracted by functionality - facerec, mediation, messenger bot. Face data is stored locally as there is limited data. The telegram servers are used in a SaaS fashion.

3.10. Application Development

The client application is simplified by leveraging the existing telegram bot interface which provides functionalities ranging from buttons to images. This prevents the need for an independent mobile application.

4. System Implementation



Circuit diagram

4.1. Module Development –Code

```
import telegram
auth_token = '417489646:AAG0ZJ09qVJhykNOyHrLb9wPdg_iGCYekaM'
bot = telegram.Bot(token=auth_token)
admin = bot.get_me()
id = '-343921014'
```

```

def send_image(img, caption = 'Visitor detected'):
    # img - image in bytes
    bot.send_photo(chat_id=id, photo=img, caption = caption)
Camera Loop:
import cv2
from io import BytesIO
import tele_interface as tele
from time import sleep
import requests
import jsonpickle

def get_image():
    cam = cv2.VideoCapture(0)
    ret, im = cam.read()
    im = cv2.imencode('.jpg', im)[1].tostring()
    io = BytesIO(im)
    return io

def send_image_to_bot(im):
    im = cv2.imencode('.jpg', im)[1].tostring()
    io = BytesIO(im)
    tele.send_image(io)

def send_image_to_server(im):
    url = 'http://localhost:5000/image'
    _, img_enc = cv2.imencode('.jpg', im)
    response = requests.post(url, data=img_enc.tostring())
    return response.json()

def camera_loop():
    cam = cv2.VideoCapture(0)
    ret, im = cam.read()

    # send image to server to run face recognition if unknown face,
    res = send_image_to_server(im)
    notify_bot = True

    if notify_bot:
        # send image to the bot
        # send_image_to_bot(im)
        pass
    cam.release()

if __name__ == "__main__":
    while True:
        camera_loop()
        sleep(1)
Server:
from flask import Flask, request, Response

```

```

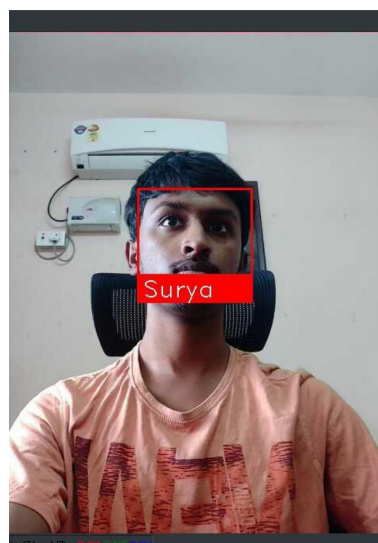
import jsonpickle
import numpy as np
import cv2
from facerec import detect_faces

# Initialize the Flask application
app = Flask(__name__)
app.debug = True

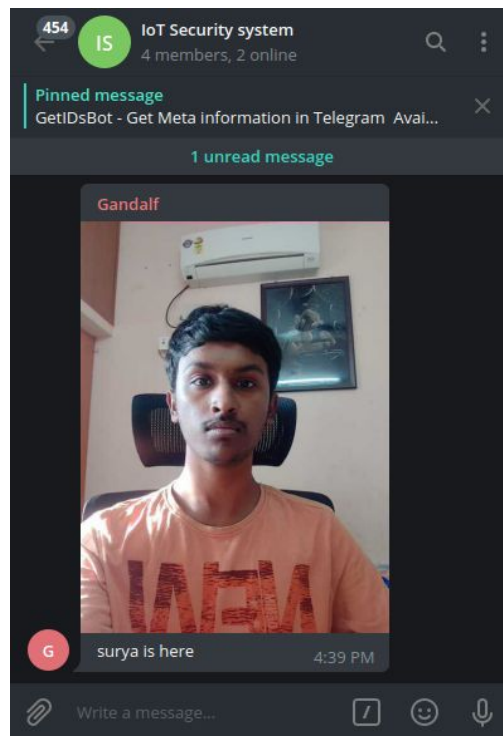
# route http posts to this method
@app.route('/image', methods=['POST'])
def test():
    r = request
    # convert string of image data to uint8
    nparr = np.fromstring(r.data, np.uint8)
    # decode image
    img = cv2.imdecode(nparr, cv2.IMREAD_COLOR)
    # recognize faces
    res = detect_faces(img)
    print(res)
    # build a response dict to send back to client
    response = {'detected_face': str(res),
                'code': 200    # 200 face found, face not found
               }
    # encode response using jsonpickle
    response_pickled = jsonpickle.encode(response)
    return Response(response=response_pickled, status=200,
                    mimetype="application/json")
# start flask app
app.run(host="0.0.0.0", port=5000)

```

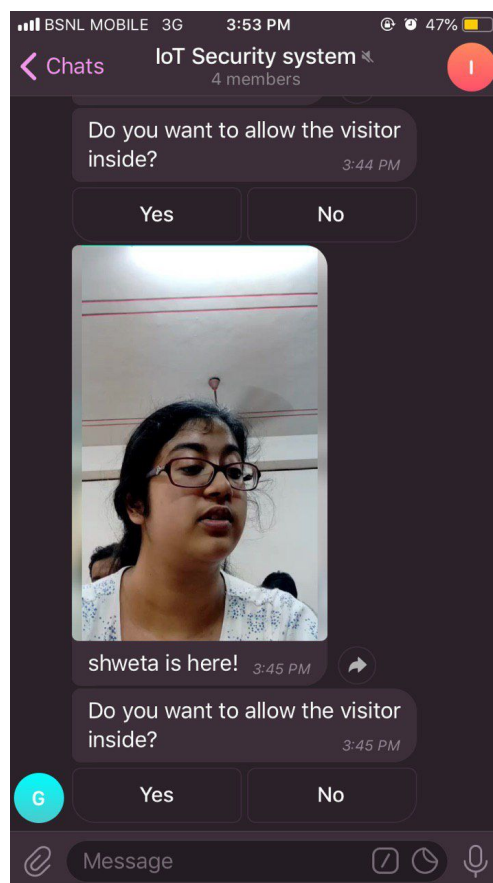
4.2. Output/Results



Face recognition module



Visitor notification bot - telegram



Visitor permit bot- Telegram



RPI attached to lock motor

5. Conclusion and Future Developments

From this project it is evident that secure face recognition based home security system can be easily implemented with the help of bots in messenger apps like telegram. This makes it easier for users as they won't be required to host servers: they can leverage publicly available infrastructure of popular platforms. It can also be concluded that a system that not only allows permitted visitors in, but also allows notifies the user and allows the user to let an unidentified visitor in is more convenient and secure.

More features can be implemented which allows for easier dynamic addition of users to the face recognition system, and integration of multiple locks. Further, we plan on implementing web hooks which allows developers to easily extend the application of the system and fine tune it for their specific needs. More research can also be done on reducing the latency of the recognition algorithm.

6. References

<https://www.cnet.com/news/top-facial-recognition-home-security-cameras-for-2019-google-nest/>

https://www.researchgate.net/publication/329884419_A_Smart_Security_System_with_Face_Recognition

<https://towardsdatascience.com/make-your-own-smart-home-security-camera-a89d47284fc7>

<https://pdfs.semanticscholar.org/cfcd/3ceae28abeddfc27e16cf19015a10d1831c.pdf>

For Evaluation only:

Status : ACCEPTED / REJECTED



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

B.Tech (Information Technology)
ITE 4003 Internet of Things –
FALL 2019
Course Project- Review- I
Evaluation Sheet
(Latest Date : 08.08.2019)

Title:

Face recognition home security

Team Name

Generic Teamname

Project Team

S.No	Register Number	Student Name	Signature	Guided By
1.	16BIT0029	Surya K		
2.	16BIT0423	Shweta Vijay		

Team Member(s) Contribution and Performance Assessment

Components	Student 1	Student 2	Student 3
Understanding Background of & Problem Statement -Abstract (05)			
Objective of the project & Requirements Analysis (10)			
Innovation component in the project (05)			
Total (20)			

Expectation for Next Reviews

Comments

Name & Signature of the Evaluator