**Entry based Security System**

Minor project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology

in

**Computer Science and Engineering**

By

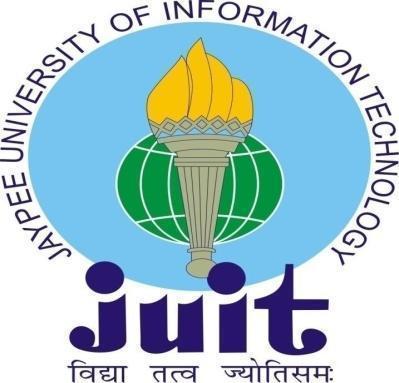
Devansh Kaushik (181322)

Deepak Kumar (181337)

Diwakar Srivastava (181330)

**UNDER THE SUPERVISION OF**

Dr. Geetanjali



Department of Computer Science & Engineering and Information Technology

**Jaypee University of Information Technology, Waknaghat, 173234, Himachal Pradesh, INDIA**

**TABLE OF CONTENT**

**Content Page No.**

**Declaration by Candidate I**

**Certificate by Supervisor II**

**Acknowledgment III**

**Abstract IV**

1. **Introduction 1-2**
2. **MINOR PROJECT SDLC 3-8**
3. **Implementation 9-17**
4. **Results 18-19**

**References 20**

**DECLARATION**

I hereby declare that this project has been done by me under the supervision of **Dr. Geetanjali**, Jaypee University of Information Technology. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

**Supervised by:**

Dr. Geetanjali

Assistant Professor (SG)

Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology

**Submitted by:**

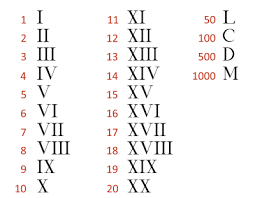
Deepak Kumar(181337)

Devansh Kaushik(181320)

Diwakar Srivastava (181330)

Computer Science & Engineering Department

Jaypee University of Information Technology



**CERTIFICATE**

This is to certify that the work which is being presented in the project report titled **“Entry Based Security System”** in partial fulfilment of the requirements for the award of the degree of B.Tech in Computer Science And Engineering and submitted to the Department of Computer Science And Engineering, Jaypee University of Information Technology, Waknaghat is an authentic record of work carried out by **“Deepak Kumar(181337), Devansh Kaushik(181320), Diwakar Srivastava (181330)”** during the period from January 2021 to May 2021 under the supervision of **Dr. Geetanjali**, Department of Computer Science and Engineering, Jaypee University of Information Technology, W aknaghat.

Deepak Kumar(181337)

Devansh Kaushik(181320)

Diwakar Srivastava (181330)

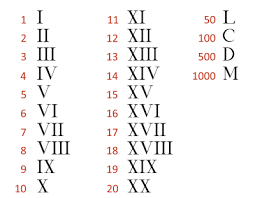
The above statement made is correct to the best of my knowledge.

Dr. Geetanjali

Assistant Professor (SG)

Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology



**ACKNOWLEDGEMENT**

Firstly, I express my heartiest thanks and gratefulness to almighty God for His divine blessing makes it possible to complete the project work successfully.

I am really grateful and wish my profound indebtedness to Supervisor **Dr. Geetanjali Assistant Professor (SG)** Department of CSE Jaypee University of Information Technology,Wakhnaghat. Deep Knowledge & keen interest of my supervisor in the field of “IOT/ML” to carry out this project. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stages have made it possible to complete this project.

I would like to express my heartiest gratitude to Dr. Geetanjali Department of CSE, for his kind help to finish my project.

I would also generously welcome each one of those individuals who have helped me straightforwardly or in a roundabout way in making this project a win. In this unique situation, I might want to thank the various staff individuals, both educating and non-instructing, which have developed their convenient help and facilitated my undertaking.

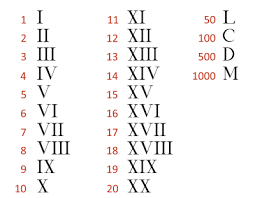
Finally, I must acknowledge with due respect the constant support and patients of my parents.

Deepak Kumar

Devansh Kaushik

Diwakar Srivastava

**`**



**ABSTRACT**

Nowadays, providing a security system for houses has become an important research during which the newest technologies are being adopted to serve this purpose. Wireless network is one of the technologies that have been used to provide remote monitor and control for the home appliances.

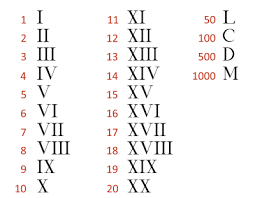
This project aims to propose an alternative to the traditional lock-key system with an IoT security system using face recognition. As the IoT integrates the interconnectedness of human culture, our 'things', with the interconnectedness of our digital information system, Team Dauntless decided to develop their first project using IoT and app development. IoT devices are programmed in such a way that they assist in creating an automated system, for instance, self-driving cars.

These IoT devices contain HD cameras, thermal sensors, smart navigators, speed controller, rain sensors, wireless connectivity, and proximity sensors. Face recognition is implemented using OpenCV. OpenCV is the most popular library for computer vision. Originally written in C/C++, it now provides bindings for Python. OpenCV uses machine learning algorithms to look for faces within an image . Because faces are so complicated, there isn’t one simple test which will tell you if it found a face or not. Instead, there are thousands of small patterns and features that have got to be matched. The algorithms break the task of identifying the face into thousands of smaller, bite-sized tasks, each of which is easy to solve. These tasks are also called classifiers.

The python programming modules are orderly scheduled using Crontab. The software utility crontab, also referred to as cron job may be a time-based job scheduler in Unix-like computer operating systems. Users who set up and maintain software environments use cron to schedule jobs to run periodically at fixed times, dates, or intervals. So with the backend as openCV, the face capturing and alerts send/receive is done using raspberry pi.

Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation in association with Broadcom. It is widely utilized in many areas, like for weather monitoring, due to its low cost, modularity, and open design. It is typically employed by computer and electronic hobbyists, thanks to its adoption of HDMI and USB devices. The raspberry will interact with Firebase, a Google platform for creating mobile and web applications. Firebase has multiple features, our project using a real-time database and storage, the storage for the videos being sent by the family members for application setup, thus, making the project a 3-way interaction - the device (raspberry pi), mobile application and database/storage (firebase). This system finds a good application in areas where physical

presence is not possible all the time.



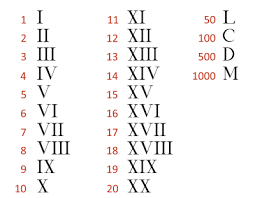
**TABLE OF FIGURES**

**Content Page No.**

1. **Use case diagram of user’s functionality 7**
2. **Data flow diagram of the data input-output 8**
3. **State Transition Diagram 9**

**of the Entry based security system**

1. **Flow graph of the Entry based security system problem 13**
2. **App Login and the members page 14**
3. **Members addition page and video upload page 14**
4. **Uploaded video on the Firebase Storage 15**
5. **Downloaded video 15**
6. **Images in local storage after frame capture 16**
7. **Applying randomLightFilters on every image 17**
8. **Face detection and Face recognition 17**
9. **Notification for Manual access 18**



**Chapter 01**

**INTRODUCTION**

* 1. **Introduction**
  2. **Objective of the Minor Project**
  3. **Motivation of the Minor Project**
  4. **Language Used**
  5. **Technical Requirements ( Hardware)**
  6. **Deliverables of the Minor Project**

**Introduction**

The project focuses on making a simple and secure IoT-based door entry system using facial recognition. The device is connected to the application that keeps all resident users connected for the latest updates and alerts. The user can easily enter just by facial recognition, if already added when the device was set up. Otherwise, the device will send an alert to the family members’, who can verify the request by the application.

The device and the application interact through a real-time database, which handles the user data and allows multiple users to be connected to the same device. This project aims at increasing safety of the door entry compared to the key-lock system and promoting the use of electronic locks with our IoT device.

**Objective**

To increase safety of entry doors by an IoT-based facial recognition system linked to end user’s smartphones by an application and a real-time database.

**Motivation**

With home security as an essential need for every household, we all know how easy it is to break the key-lock system that one uses everyday, thinking how that lock wouldn’t let anyone in, behind one’s backs. And yet, every 3 minutes a house gets robbed and the realization of ensuring the safety of our homes is too late.

With keeping this thought as motivation, Team Dauntless has started its’ first project to replace the traditional key-lock system with face recognition-based entry door system, which will not only increase the safety of preventing forced breaks into your homes, but also remove the everyday hassle of keeping a large bunch of keys in your pockets everyday, whenever anyone steps out even for a minute. Also, End users will never miss a door bell with the notifications of every entry request being directly sent to their smartphones.

Furthermore, as the team will tend to keep the majority of its focus on AI/ML and IoT, applying our skill set to a variety of fields such as security will add to the team’s understanding and proficiency.

**Languages Used**

Python, Java, Bash

**Technical Requirements (Hardware)**

Raspberry pi 3B+, webcam, SD Card, cables, 5V 2.5A power supply

**Deliverables of the Minor Project**

The device (raspberry pi) initiates the back-end operations as soon as one rings the doorbell. The device, attached behind the door peephole (preferably) takes several images of the user and returns the prediction as a string, which can either be the recognized user’s name tag or a default string, unknown. The prediction is sent back to the device which then, either unlocks the door or sends a priority notification to the application, installed in all the family members' phones. Any family member can accept/deny the entry request, the first one will be accepted. All the python programme (backend) scheduling is done using Crontab, a Linux utility software.

**Chapter 02**

**MINOR PROJECT SDLC**

**2.1 Feasibility Study on Minor Project**

**2.2 Requirements on Minor Project**

**2.2.1 Functional Requirements**

**2.2.2 Non-Functional Requirements**

**2.3 Use Case Diagram of the Minor Project**

**2.4 DFD Diagram of the Minor Project**

**2.5 State Transition Diagram of the Minor Project**

**2.1 Feasibility Study on Minor Project**

**Research Papers:**

1. Smart Door System for Home Security Using Raspberry pi3

Author: Naser. Abbas Hussein, Inas Al Mansoori

Limitation: Once initialized, database can’t be altered. Access control only for a single user.

1. IOT based Smart Home Security System with Alert and Door Access Control using Smartphone

Author: Shaik Anwar, D. Kishore

Limitation: Authorized user also have to go through verification, without internet door will not open for authorized user

1. Smart Door Security System using Raspberry Pi with Telegram

Author: Shivani Desai, Virendra D. Pawar

Limitation: Authorized user also have to go through verification, without internet door will not open for authorized user

**Source Documentations:**

1. Image Processing by OpenCV ([Image Processing](https://docs.opencv.org/master/d7/dbd/group__imgproc.html))
2. Real Time Database by Google/Firebase ([Firebase Realtime Database docs](https://firebase.google.com/docs/database))
3. Face Recognition model by OpenCV( [Face Recognition with OpenCV](https://docs.opencv.org/3.4/da/d60/tutorial_face_main.html) )

**2.2 Requirements on Minor Project**

**2.2.1 Functional Requirements:**

OpenCV module:

* cascadeClassifier: to detect faces in images using Haar Cascade Frontal Face.
* videoCapture: to read the output of the camera
* cvtColor: to convert images to gray
* imread: to read the images
* LBPHFaceRecognizer: using LBPH machine learning algorithm to train dataset

RandomLightFilter module

* adding filters to images such as addParallelLights, addSpotLights ...

Firebase SDK:

* Pyrebase: it helps to integrate firebase SDK
* initializeApp: to establish the connection to firebase
* Real-time database: to store data and get instant change in project
* Storage: to store all users videos

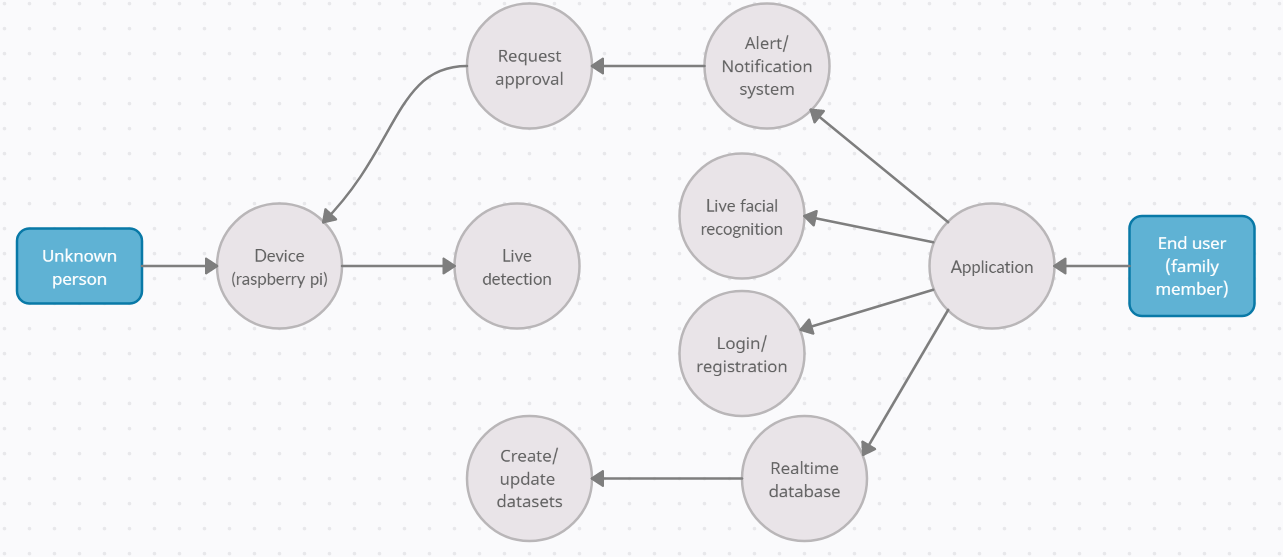
Crontab

* it’s an operating system function that helps in application scheduling

**2.2.2 Non-Functional Requirements**

* Videos have to be less than and equal to 10sec and recorded in mobile with vertical alignment
* Model update daily at 9 pm means new user recognize after 9 pm
* All capture images deleted after train the model
* mobile minSDk=29 to install the app
* Model takes 10min to train
* Notification used First-Come-First-Serve basis to grant access
* Raspberry Pi with Wifi, 1Gb ram, webcam

**2.3. Use Case Diagram**



**Figure 1 : Use case diagram of user’s functionality**

Figure 1 depicts a use case diagram of user’s functionality and the android app provides end-users to add new members and upload video, this video is used by the server to detect faces and train ML models, and send them to the Raspberry Pi device.

If a person is detected in-camera, the recognizer recognizes the person with the help of the model created by the server. If the label is unknown then a notification is sent to the app with an image and asks the end user to grant the permission otherwise permission is granted.

**2.4. Data Flow Diagram**



**Figure 2: Data flow diagram of the data input-output**

Figure 2: Data flow diagram of the data input-output shows how theEnd users can upload the video to the app and the app will send video to the server for training the model, after that the server will send the model to Raspberry Pi.

Raspberry Pi uses the model to detect the unknown person if not detected, notification will be sent to the end user to grant the permission.

**2.5 State Transition Diagram of the Entry based security system**



**Figure 3: State Transition Diagram of the Entry based security system**

Figure 3: State Transition Diagram of the Entry based security system shows how the Recognition start when some press the button then predict the label using model if label is unknown then notification send to mobile app with images after that user check the image accept or decline the request

**Chapter 03**

**IMPLEMENTATION OF THE MINOR PROJECT**

**3.1 Date Set Used in the Minor Project**

**3.2 Date Set Features**

**3.2.1 Types of Data Set**

**3.2.2 Number of Attributes, fields, description of the data set**

**3.3 Design of Problem Statement**

**3.4 Algorithm / Pseudo code of the Project Problem**

**2.5 Flow graph of the Minor Project Problem**

**3.6 Screenshots of the various stages of the Project**

**3.1 Data Set Used in the Minor Project**

The Data Set we are using is composed of images and videos , we are taking videos as user input via the android app and will be scrapping that video for images to train our model. The user detection has been done using the Haar Cascades’ frontal face detection which takes the image and uses the image for the recognition process using LBHP(Local Binary Pattern Histogram) Recognizer.

**3.2 Data Set Features**

**3.2.1 Types of Data Set**

**Videos :** The video dataset which is used is in .mp4 format , user uploaded images are required to be of 10sec duration for the further frame capture process.

**Images :** The images dataset which is used is in .jpg format , images being

trained are in the grayscale and the images to be recognised are in RGB scale.

**3.2.2 Number of Attributes, fields, description of the data set**

**Image Attributes :** We convert the image from RGB to grayscale for the training process, for the recognition we are using the image in RGB . Images are stored in .jpg format for the training as well as recognition process .

**3.3 Design of Problem Statement**

In order to replace the traditional door locks with electronic systems, the access can be given in various ways such as password lock, voice encryption or facial recognition. Deploying an optimised facial recognition system seemed to be a better choice than voice encryption, with an application to reduce complications and give users a simple yet secure system. Hence the problem statement became:

To increase safety of entry doors by an IoT-based facial recognition system linked to

end user’s smartphones by an application and a real-time database.

**3.4 Algorithm / Pseudo code of the Project Problem**

* User installs the android app , registers and uploads videos of members so that they can be recognised.
* Uploaded video is sent to the firebase-storage and from there it is downloaded to the local storage (raspberry pi) via the downloader.py module.
* When the videos are downloaded , we start the next process of frame captures from the video using the newUser.py and store it in a local database to use in the training process.
* In the training process we are using the images in LBPH trainer function to create the .yml file which is further used in recognition.
* Recognizer.py module (triggers on the doorbell when pressed) clicks 10 pictures of the person trying to get into house and processes those images through the trainer.yml file to recognize the person , if its an authorized user it’ll be granted access, if not person's image will be sent to the android app for the manual access.
* For the manual access, we use Notification.py module to send the notifications to the android app from the RaspberryPi using firebase , connection is established in real time , once the entry is granted or rejected to the requestor it’s shown using green or red LED light.

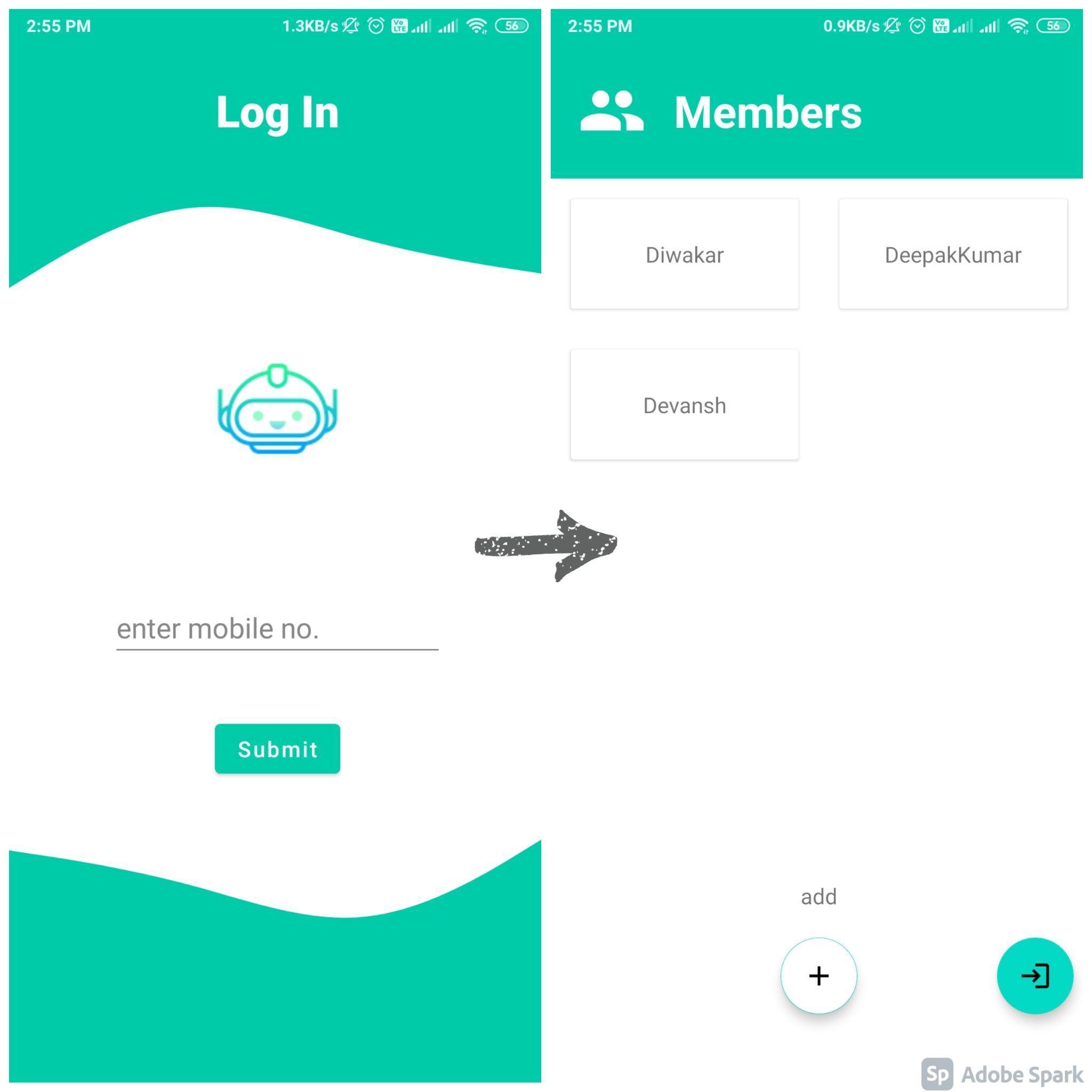
**3.5 Flow graph of the Entry based security system problem**



**Figure 4 : Flow graph of the Entry based security system problem**

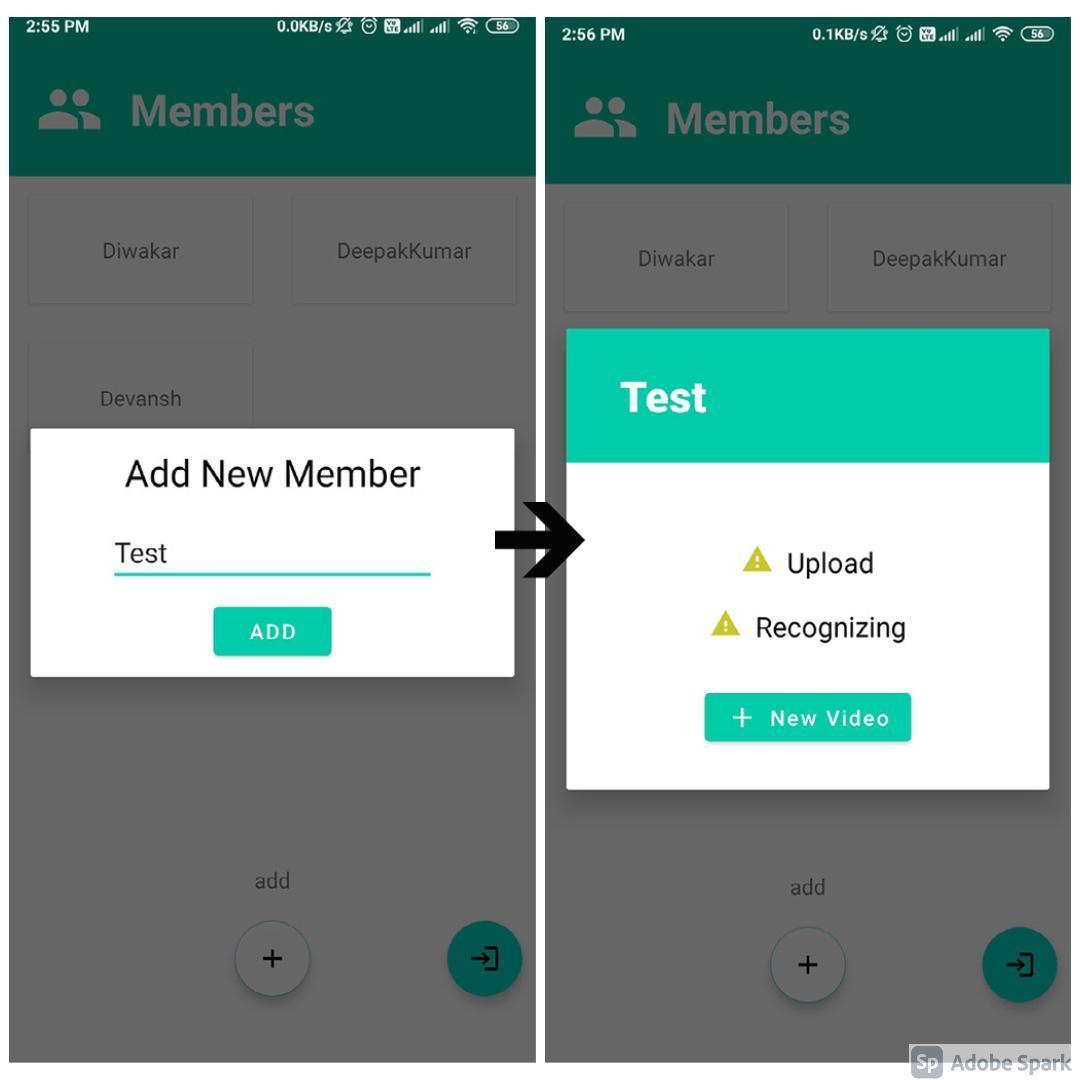
Figure 4 : Flow graph of the Entry based security system problem shows the total mechanism of data processing ,facial detection,face recognition , interaction between firebase , local device(Raspberry pi) and the android app.

**3.6 Screenshots of the various stages of the Project**



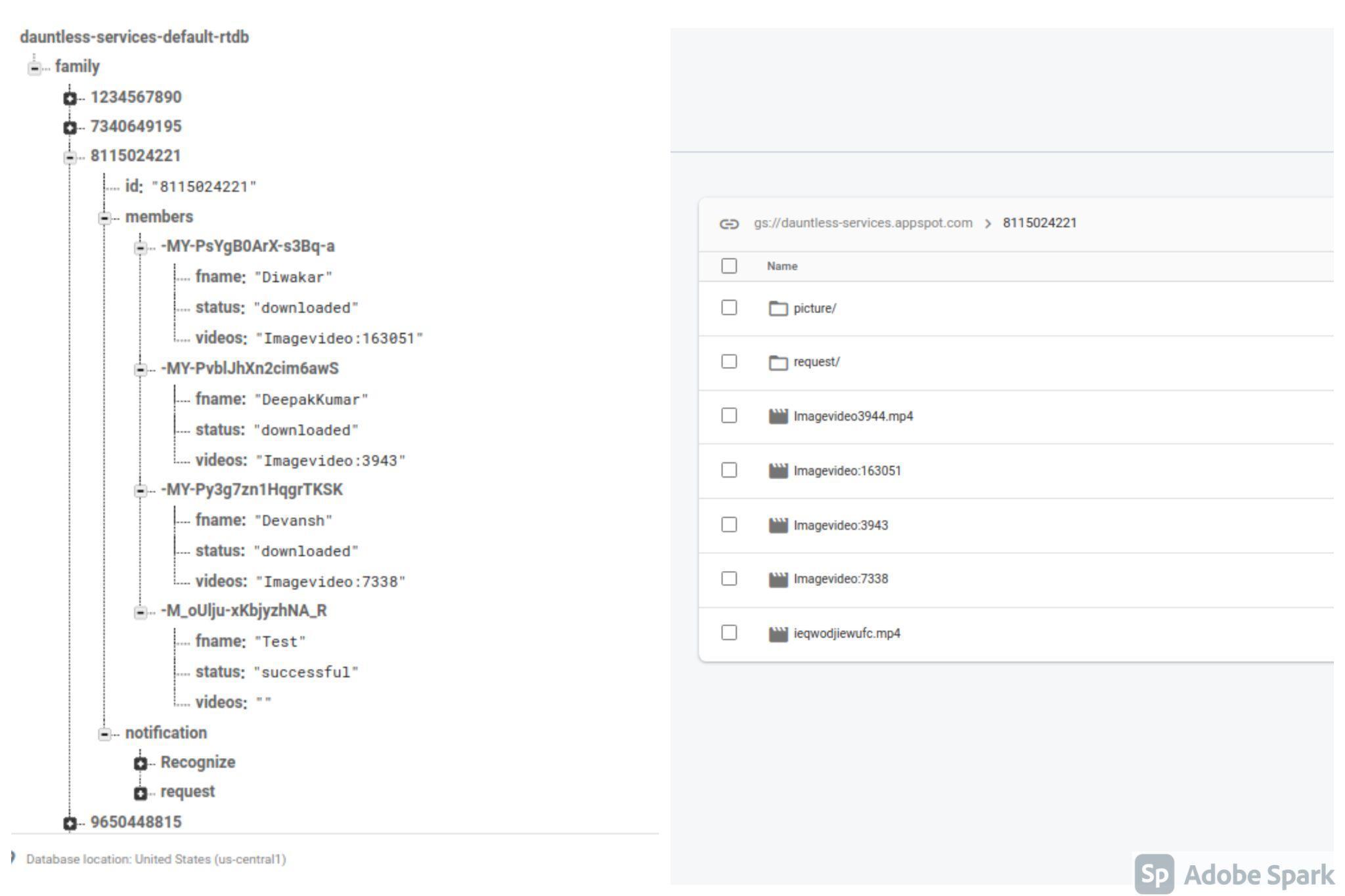
**Figure 5: App Login and the members page**

The Figure 5: App Login and the members pageshows the first step of registering with the android app and adding as the members.



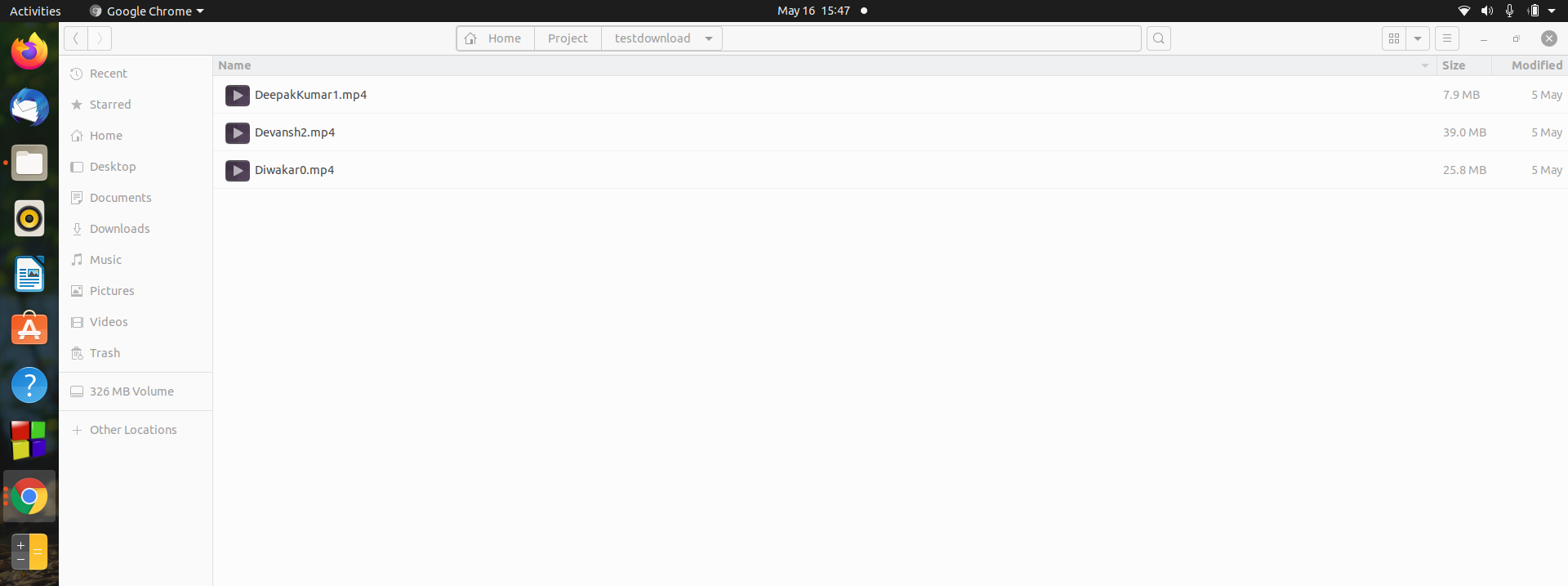
**Figure 6: Members addition page and video upload page**

The figure 6: Members addition page and video upload pageshows the addition of members as well as video upload .



**Figure 7: Uploaded video on the Firebase Storage**

Members added as well as the video uploaded by the user’s is stored on firebase database and the firebase storage are shown in Figure 7: Uploaded video on the Firebase Storage, later videos are downloaded to the local storage by our downloader.py module.



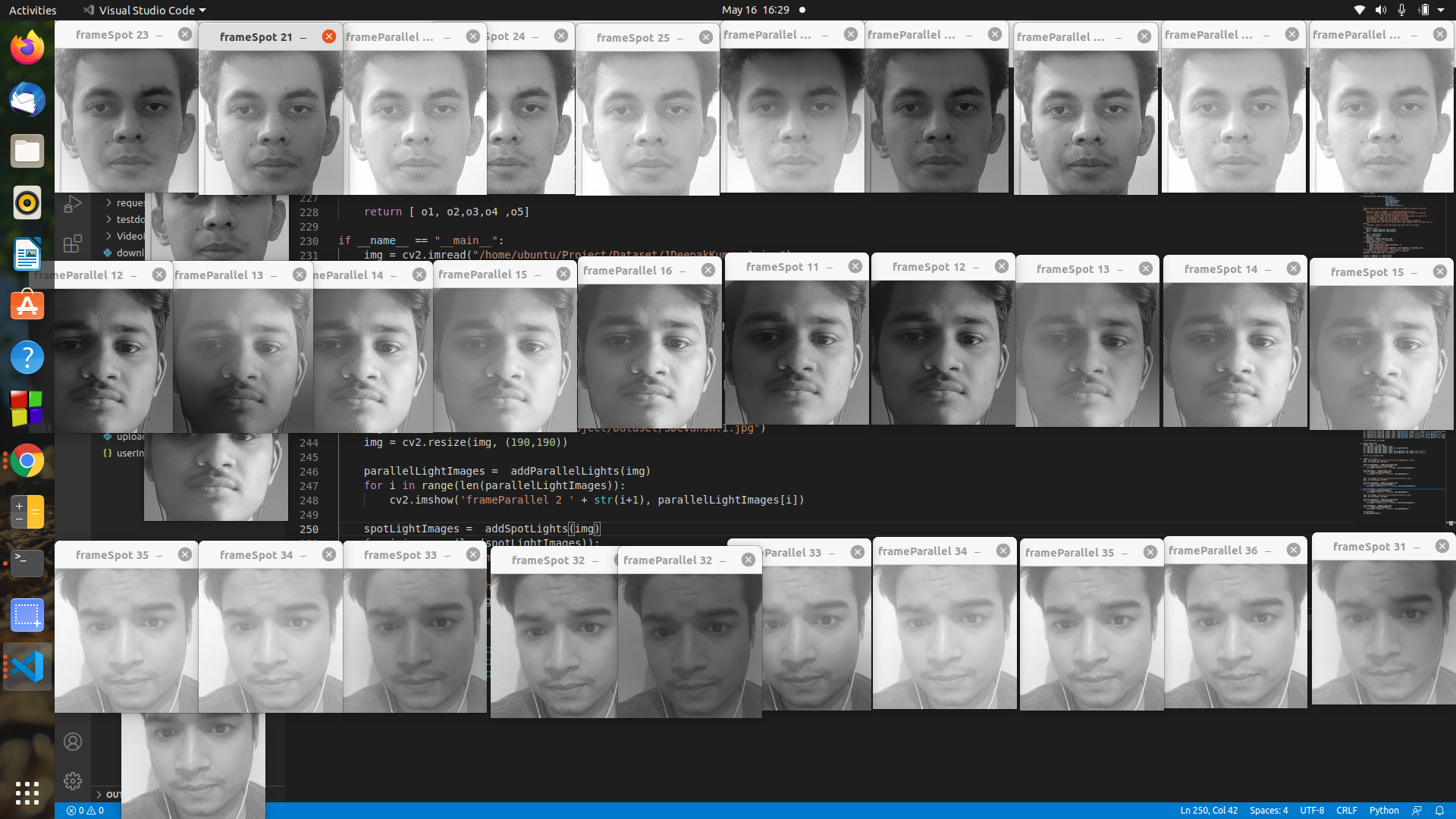
**Figure 8: Downloaded video**

The videos stored on the firebase storage are downloaded to the local storage to later process for the frame capture shown in Figure 8: Downloaded video.



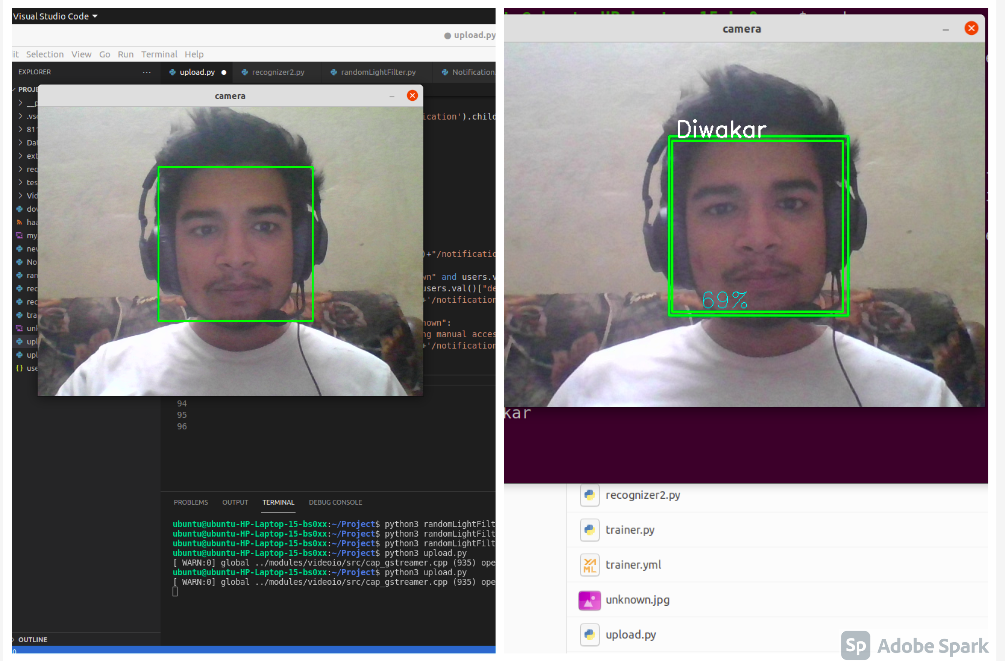
**Figure 9: Images in local storage after frame capture**

After processing the video through the newUser.py module we get these grayscale images which are further used to train the model as shown in Figure 9: Images in local storage after frame capture.



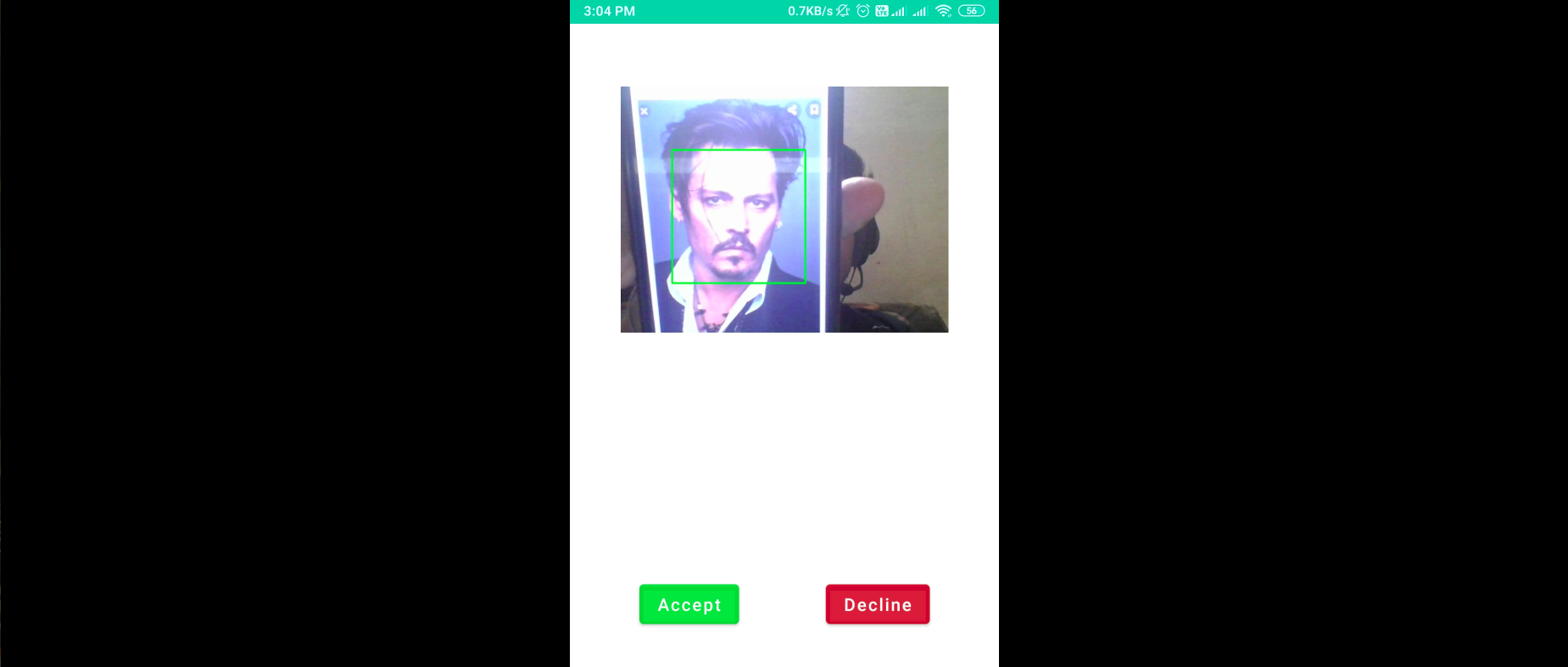
**Figure 10: Applying randomLightFilters on every image**

Applying image augmentation(as shown in Figure 10: Applying randomLightFilters on every image) to populate the dataset using image transformation and using the images to train the model .



**Figure 11: Face detection and Face recognition**

As the doorbell rings , recognizer.py detects the face of the person in front of the door and captures 10 frames of the individual to be used for recognition as in Figure 11: Face detection and Face recognition , using those images the model recognizes the individual and returns the ID of the person or returns ‘Unknown’.



**Figure 12. Notification for Manual access**

In Figure 8. Notification for Manual accessif the individual at the door is not recognised by the model and labelled as ‘Unknown’ we send notification to the user on the android app for manual access .

**Chapter 04**

**RESULTS**

**4.1 Discussion on the Results Achieved**

**4.2 Application of the Minor Project**

**4.3 Limitation of the Minor Project**

**4.4 Future Work**

**4.1 Discussion on the Results Achieved**

1. Taking 90 images for single video
2. Converting images to grey and apply some filter to populate the dataset
3. after applying filter, total 990 images per person
4. train the model with the help of LBPH algorithm
5. At the end we achieved,74% correctness to recognize person
6. finally, we can recognized person and send notification and ask end user to grant

access

**4.2 Application of the Minor Project**

Providing a security system for houses with latest technologies that have been used to provide remote monitor and control for the home appliances.

Providing an alternative to the traditional lock-key system with an IoT security system using face recognition, which will not only increase the safety of preventing forced breaks into your homes, but also remove the everyday hassle of keeping a large bunch of keys in your pockets everyday,

**4.3 Limitation of the Minor Project**

* Raspberry Pi has only 1Gb ram because of that it’s not able to train the model with high dataset
* ML Model recognize the images with only 74% accuracy
* Dependency on the cloud server i.e; without the internet new users can’t be added.
* End users can not receive notification if the user's mobile or Raspberry Pi have no access to the internet.
* Project is not completely immune to exception handling.

**4.4 Future Work**

* Increasing ML Model efficiency
* Manage code more efficient by following Architecture such as MVC
* Handling exceptions with specificity.
* Adding more functionality to the app such as live cam, Alarm alert

**LITERATURE SURVEY**

In this section, we will discuss various entry based security mechanisms proposed by various researchers.Hussein et al, [1] proposed the Smart door system for home security using raspberry pi3 and the idea is door access using face recognition or pin. If valid, the input door opens; if no photo is sent to the owner by email and the owner grants permission accordingly but the limitation of this method is Once initialized, the database can’t be altered. Access control only for a single user.

Anwar et al, [2] proposed the IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone and PIR motion detect motion and camera take images and send it via email via TCP/IP, Authorized user can view video stream through smart phone application also send void note but the limitation of this method is Authorized user also have to go through verification, without internet door will not open for authorized user.

Desai.S, [3] proposed theSmart Door Security System using Raspberry Pi with Telegram

and the idea is PIR motion detect motion and camera take images and send it via email via TCP/IP, Authorized user can view video stream through smart phone application also send void note but the limitation of this method is Authorized user also have to go through verification, without internet door will not open.

**REFERENCES**

1. Hussein, N. A., & Al Mansoori, I. (2017, September). Smart door system for home security using raspberry pi3. In 2017 International Conference on Computer and Applications (ICCA) (pp. 395-399). IEEE.
2. Anwar, S., & Kishore, D. (2016). IOT based smart home security system with alert and door access control using smartphone. International Journal of Engineering Research & Technology (IJERT), 5(12), 504-509.
3. Desai.S, Pawar.D.V ,(2019,June).Smart Door Security System using Raspberry Pi with Telegram . In International Research Journal of Engineering and Technology (IRJET) (Volume :06 Issue:06).
4. Aman, F., & Anitha, C. (2017, August). Motion sensing and image capturing based smart door system on android platform. In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 2346-2350). IEEE.
5. Chaurasia, A., Dwivedi, U. K., Chaurasia, A., & Jain, S. K. (2020). A New Approach to Smart Knock Detection Based Security System for Door Lock. In International Conference on Intelligent Computing and Smart Communication 2019 (pp. 907-914). Springer, Singapore.
6. Sahani, M., Nanda, C., Sahu, A. K., & Pattnaik, B. (2015, March). Web-based online embedded door access control and home security system based on face recognition. In 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015] (pp. 1-6). IEEE.
7. Komol, M. M. R., Podder, A. K., Arafat, A., & Nabeed, T. (2019). Remote sensing global ranged door lock security system via mobile communication. Ijwmt, 9, 25-37.
8. Gupta, R. K., Balamurugan, S., Aroul, K., & Marimuthu, R. (2016). IoT based door entry system. Indian Journal of Science and Technology, 9(37).
9. Ibrahim, A., Paravath, A., Aswin, P. K., Iqbal, S. M., & Abdulla, S. U. (2015, December). GSM based digital door lock security system. In 2015 International Conference on Power, Instrumentation, Control and Computing (PICC) (pp. 1-6). IEEE.
10. Nag, A., Nikhilendra, J. N., & Kalmath, M. (2018, April). IOT Based Door Access Control Using Face Recognition. In 2018 3rd International Conference for Convergence in Technology (I2CT) (pp. 1-3). IEEE.