International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

Face Recognised Based Atm Authentication Using Artificial Intelligence

Dahlia Rane P , Gnanadeepam B
COMPUTER SCIENCE AND ENGINEERING
PANIMALAR ENGINEERING COLLEGE, CHENNAI - 600123.
ANNA UNIVERSITY: CHENNAI 600 025 AUGUST 2021

Submitted: 05-10-2021 Revised: 18-10-2021 Accepted: 20-10-2021

I. INTRODUCTION

1.1OVERVIEW

The face recognition process includes mainly three-task: acquisition, normalization and recognition. The term acquisition means, the detection and tracking of face-like image patches in a dynamic scene. Normalizations the segmentation, alignment and normalization of the face images, and finally recognition isthe representation and modeling of face images as identities, and the association of novel face images with known models

1.2 PROBLEM STATEMENT

Identify a person's face image from face database. Given an image, to identify it as a face and/or extract face images from it. To retrieve the similar images (based on a heuristic) from the given database of face images.

II. LITERATURE SURVEY

V. Jotsov and V. Sgurev, "Applications of Puzzle methods for intrusion detection in ATMs," 2012 6th IEEE International Conference
Intelligent Systems, Sofia, Bulgaria
Special attention is paid to applications of Puzzle method in ATMs. To make a more independently functioning ATM, the proposed methods should be applied to data/knowledge/metaknowledge elicitation, knowledge refinement, analysis of different logical connections aiming at information checks.

A.T. Siddiqui, "Biometrics to Control ATM scams: A study," 2014 In ternational Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], Nagercoil, India, 2014, pp. 1598-1602 , doi : 10.1 109/ICCPCT.2014.7054755.
Biometric is one of the technologies which we can combine with the current techno logy. We can use fingerprints, iris scan, palm scanning along with the PIN authentication and verifications. Even we can use voice recognition also. Combination of s uch technologies may help in reducing the ATM frauds and hence can improve the security level of other financial transactions.
M. M. E. Raj and A. Julian, "Design and implementation of anti-the ft ATM machine using embedded systems,"2015 InternationalConference on Circuits, Power and Computing Technologies [ICCPCT-20 15], Nagercoil, India,2015, pp. 1-5 , doi: 10.1109/ICCPCT. 2015.71593 16.
M2M platform suggests new system architecture for positioning and monitoring applications with wider coverage and higher communication efficiency. The aim of t he proposed work is to implement a low cost stand-alone Embedded Web Server (EWS) based on ARM11 processor and Linux operating system using Raspberry Pi. It offers a robust networking solution with wide range of application areas over internet. The Web server can be run on an embedded system having limited resources to serve embedded web page to a web browser. The setup is proposed for ATM sec urity, comprising of the modules namely, authentication of shutter lock, web enabled control, sensors and camera control.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

In existing system RFID card is used as ATM card, IR sensor in order to Sense the presence of the card holders and to turn on Fan and Light, if ATM is tampered then SMS is sent to two main stations via GSM.Based on WI fi detecti on get security, that network access is not that much secured.

Disadvantage of existing System

Card less transaction is not possible RFID based ATM access are prone to security issues.

3.2 PROPOSED SYSTEM

The system is implemented on the open source Computer Vision (Open CV) software are which is used for Image processing operation.

High level security mechanism is provided by the consecutive actions such as initially system captures the human face and check whether the human face is detected properly or not. If the face is not detected properly, it warns the user to adjust him/ her properly to detect the face. Still the face is not detected properly the system wil l lock the door of the ATM cabin for security purpose. **Advantages of Proposed System:**

- Increasing security to the ATM machines
- Illegal transactions can be reduced

3.3 TECHNOLOGY STACK

- Python
- Open CV
- Numpy
- Data Set

IV. SYSTEM DESIGN

4.1 USE CASE DIAGRAM

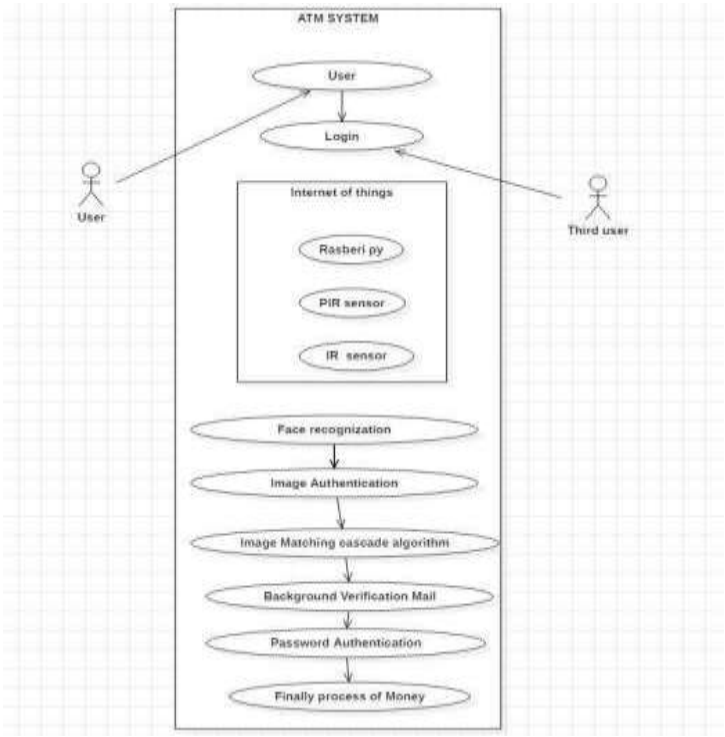


FIG 4.1 use case diagram

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

4.2 CLASS DIAGRAM

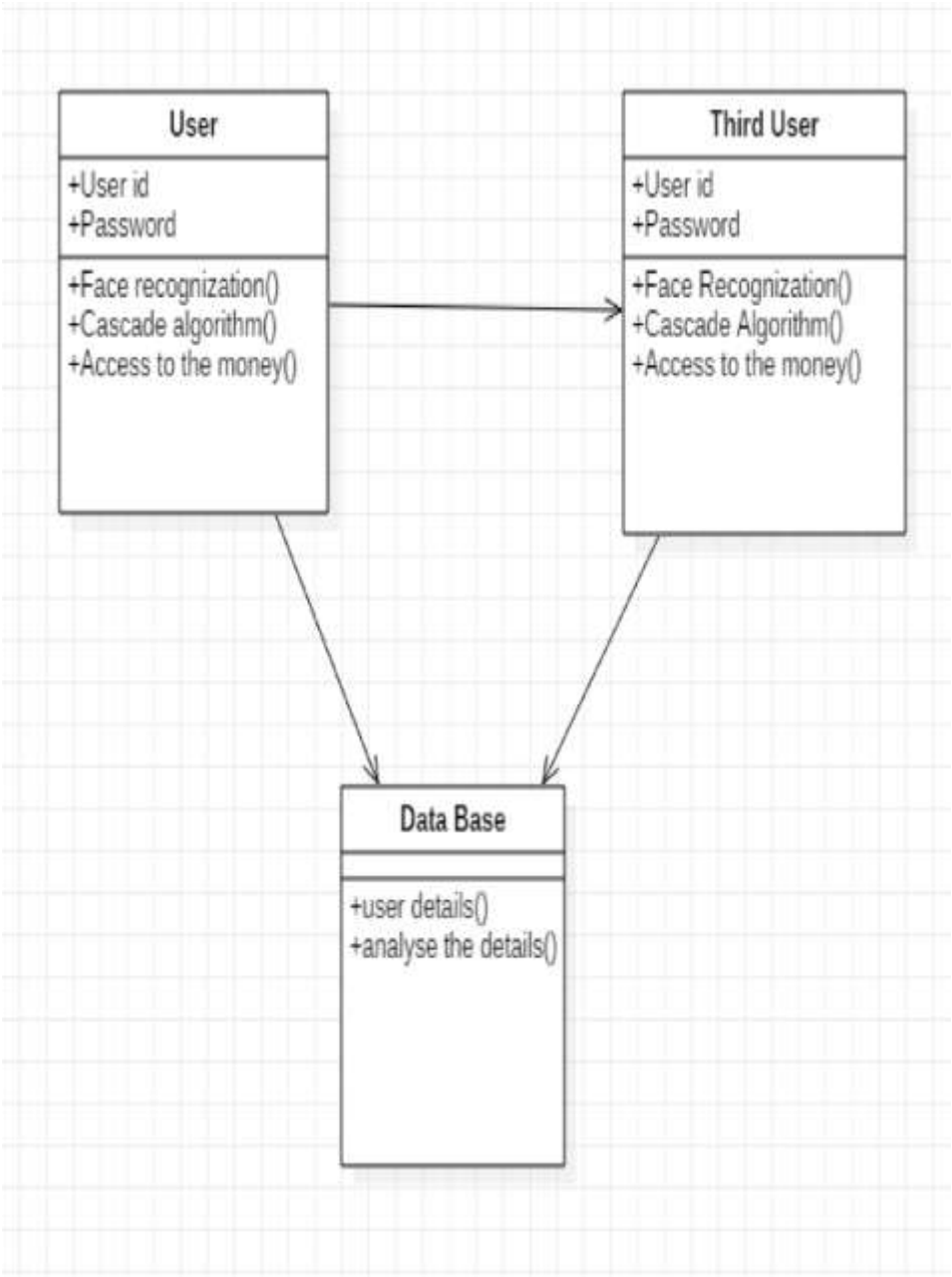


FIG 4.2 class diagram

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

4.3 SEQUENCE DIAGRAM

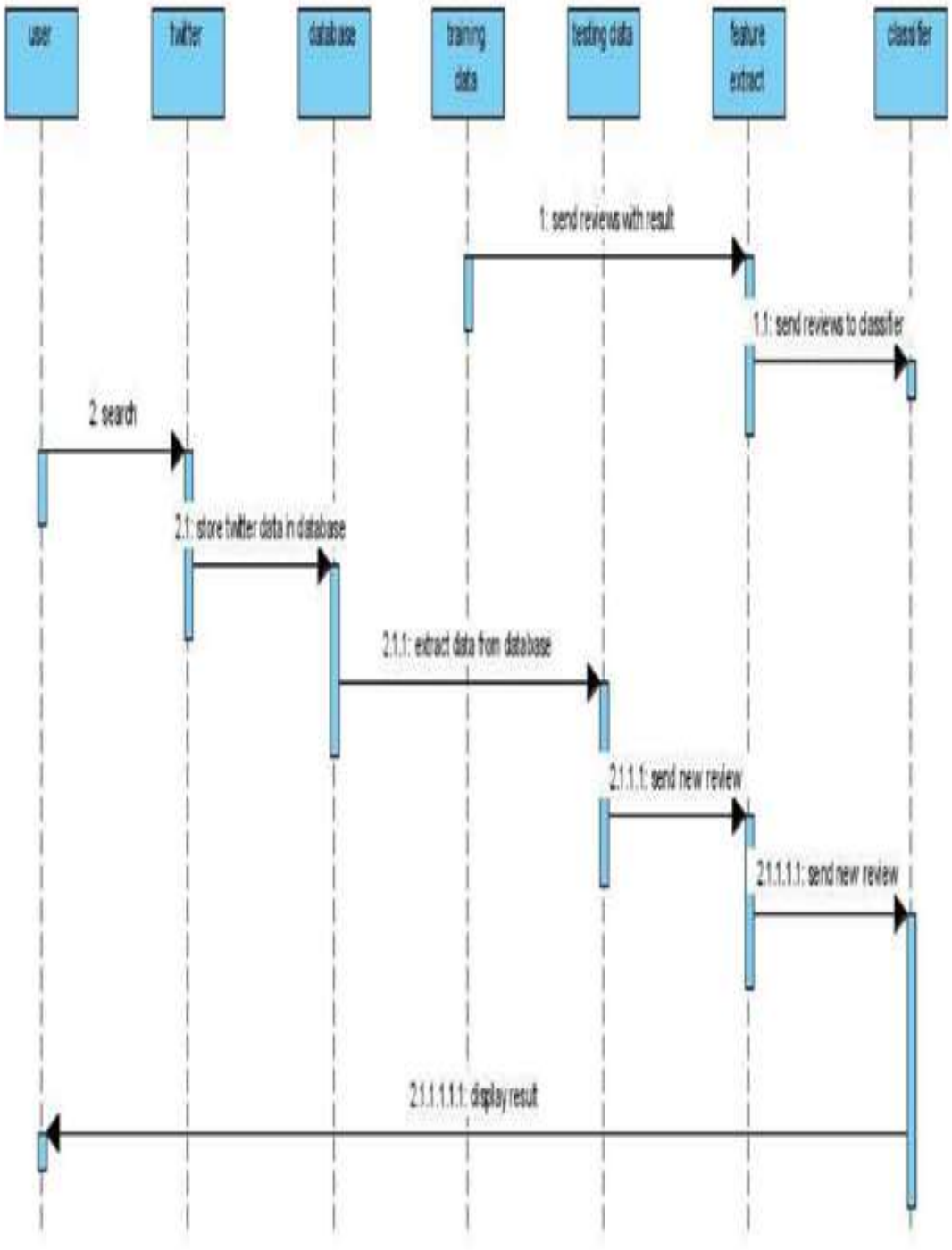


FIG 4.3 Sequence diagram

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

4.4 ACTIVITY DIAGRAM

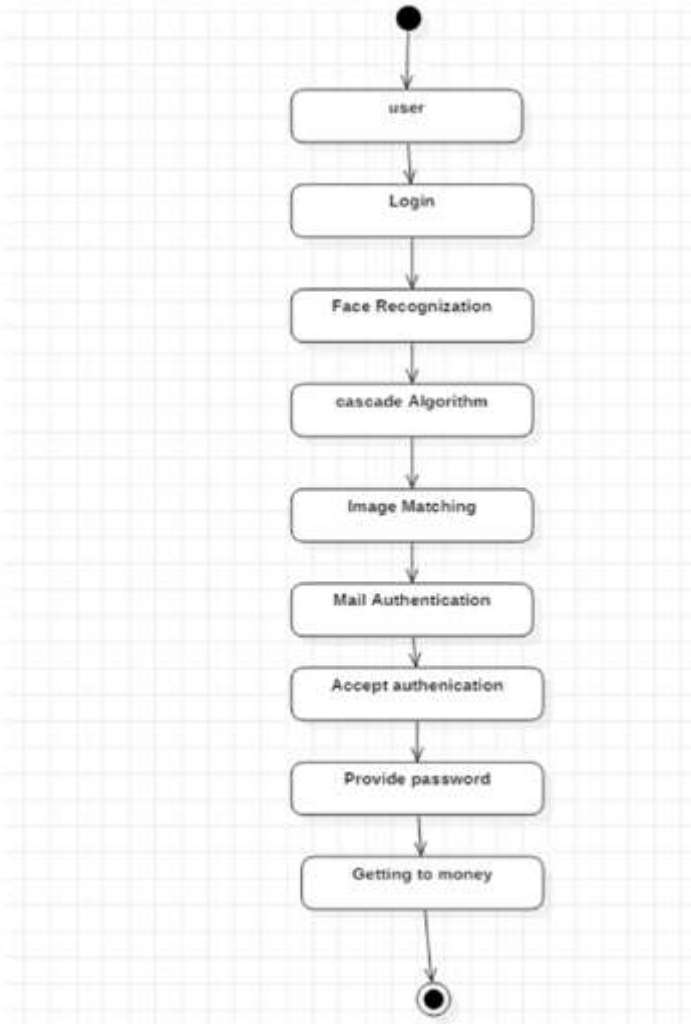
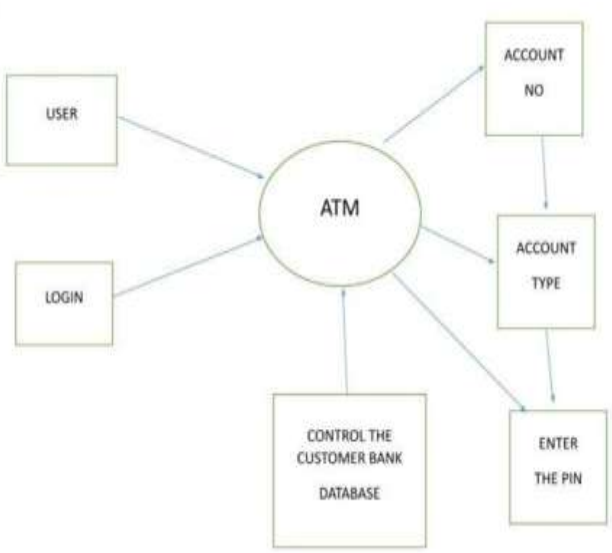


FIG 4.4 Activity diagram

4.5 DATA FLOW DIAGRAM

DFD 0

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252



DFD 1

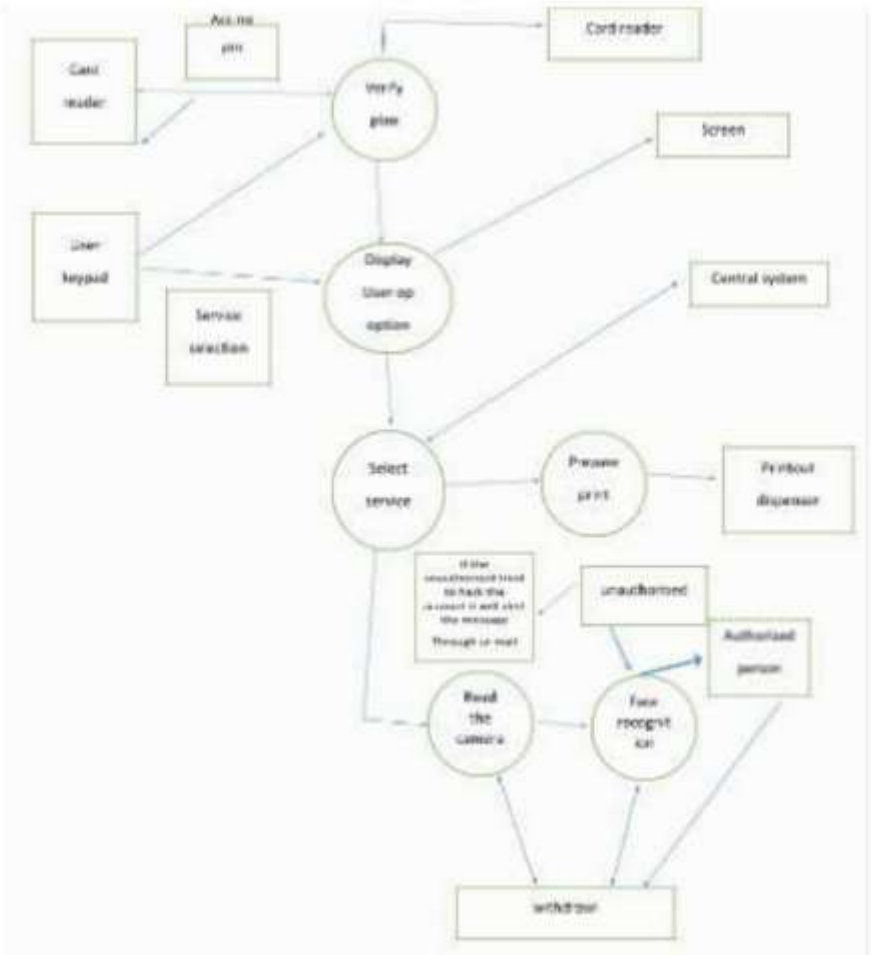


FIG 4.5 Data Flow diagram

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

V. SYSTEM ARCHITECTURE

5.1 ARCHITECTURE OVERVIEW

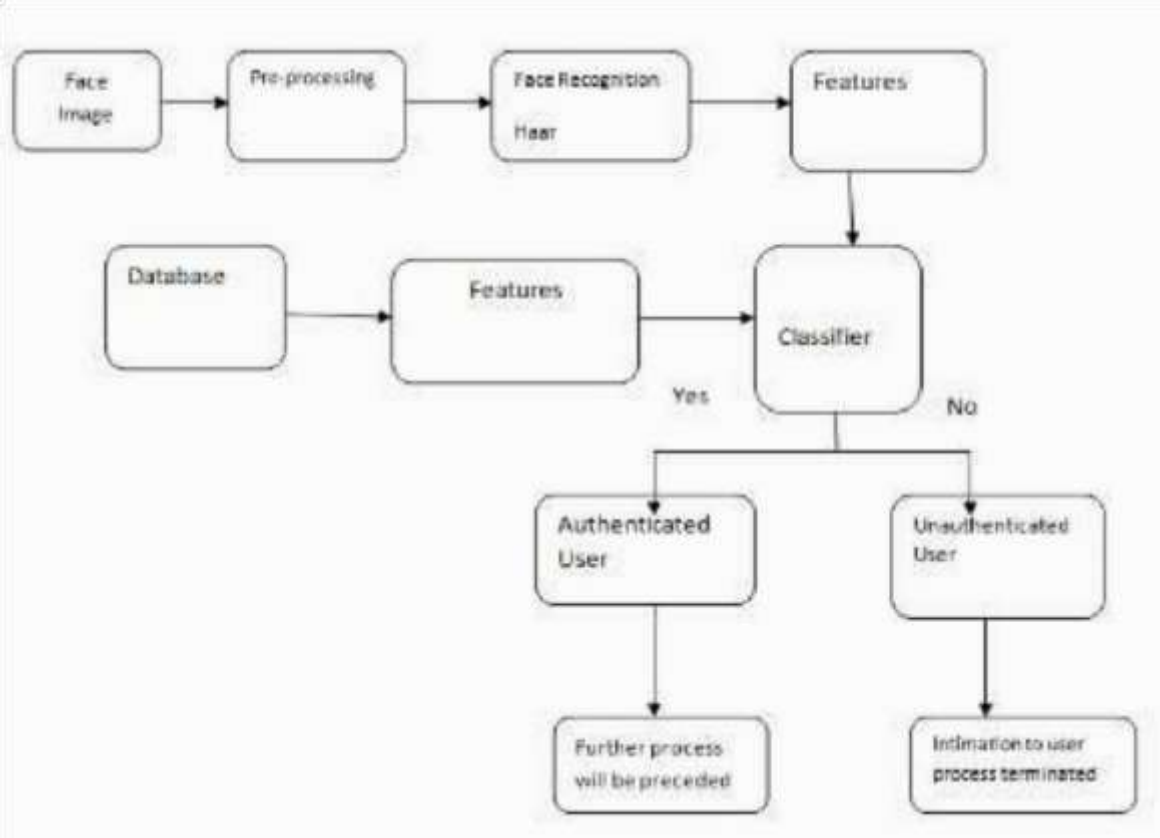


FIG 5.1 Architecture diagram

In the architecture diagram the face image is been captured and preprocessed and the Face Recognition process takes place and Features.Meanwhile based on the Database the features of the face is been matched.And the main process takes place that is the classifier in which if the features of a person matches with the data base there it gives permission to the authenticated user and the further process will be prevented.But the features process in the captured image and the face recognised image does not match means it will not give permission to access for the unauthenticated user and informes to the user by sending a mail and stops the process and it is terminated.

5.2 MODULE DESCRIPTION

1. Face image

The face is been recognized and prepare it based on facial features.

2. Database

It is a set of information and stored images.It helps to compare the captured image with the already stored images in the database.

3. Classifier

Based on the comparison of the captured image and stored images it gives the authentication if both or same.If the both images does not matches that it will not grant permission.

VI. SYSTEM IMPLEMENTATION

FACE RECOGNIZATION CODING

```
# facerec.py import cv2, sys, numpy, os
importurllib
importnumpy as np
import time
importos from subprocess import call
import time
importos
import glob
importsmtplib
import base64 from email.mime.image
importMIMEImage from email.mime.multipart
importMIMEMultipart from email.mime.text
importMIMEText import sys

gmail_user = miniproject1315@gmail.com
gmail_pwd = "panimalar"
```

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

```
FROM = 'miniproject1315@gmail.com' TO = ['ranedahlia@gmail.com']
 #must be a list defmail():
msg = MIMEMultipart()
time.sleep(1)
msg['Subject']="SECURITY"

   #BODY with 2 argument

   #body=sys.argv[1]+sys.argv[2]
body="THIS IS FROM MINI PROJECT REGARDING SECURITY ALERT"
msg.attach(MIMEText(body,'plain'))
time.sleep(1)
###IMAGE
fp = open("1.jpg", 'rb')
time.sleep(1)
img = MIMEImage(fp.read())
time.sleep(1)
fp.close()
time.sleep(1)
msg.attach(img)
time.sleep(1)
try:
server = smtplib.SMTP("smtp.gmail.com", 587)
 #or port 465 doesn't seem to work!
print ("smtp.gmail") server.ehlo()
print ("ehlo") server.starttls()
print ("starttls")
server.login(gmail_user, gmail_pwd) print ("reading mail & password")
server.sendmail(FROM, TO, msg.as_string())
print ("from")
server.close()
print ('successfully sent the mail') except:
print ("failed to send mail")

size = 4 haar_file = 'haarcascade_frontalface_default.xml' datasets = 'datasets'

print('Training...')
# Create a list of images and a list of corresponding names
(images, labels, names, id) = ([], [], {}, 0) for (subdirs, dirs, files) in os.walk(datasets):
forsubdir in dirs: names[id] = subdirsubjectpath = os.path.join(datasets, subdir)
for filename in os.listdir(subjectpath):
path = subjectpath + '/' + filename label = id
images.append(cv2.imread(path, 0))
labels.append(int(label)) id += 1
(width, height) = (130, 100)

# Create a Numpy array from the two lists above
(images, labels) = [numpy.array(lis) for lis in [images, labels]]

# OpenCV trains a model from the images # NOTE FOR OpenCV2: remove '.face' model = cv2.face.FisherFaceRecognizer_create()
model.train(images, labels)

# Part 2: Use fisherRecognizer on camera stream face_cascade = cv2.CascadeClassifier(haar_file)
 ##with open("1.txt", mode='a') as file: webcam = cv2.VideoCapture(0)

##url="http://192.168.43.1:8080/shot.jpg" while True:
   (_, im) = webcam.read()
##    imgPath=urllib.urlopen(url)
##
imgNp=np.array(bytearray(imgPath.read()),dtype=np.uint8)
##    im=cv2.imdecode(imgNp,-1) gray = cv2.cvtColor(im, cv2.COLOR_BGR2GRAY)
faces = face_cascade.detectMultiScale(gray, 1.3, 5)
for (x,y,w,h) in faces:
cv2.rectangle(im,(x,y),(x+w,y+h),(255,255,0),2)
face = gray[y:y + h, x:x + w]
face_resize = cv2.resize(face, (width, height))
#Try to recognize the face prediction = model.predict(face_resize) cv2.rectangle(im, (x, y), (x + w, y + h), (0, 255, 0), 3)

if prediction[0]<100:
#port.write('B') print (names[prediction[0]])
cv2.putText(im,names[prediction[0]],(x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255, 0))
if names[prediction[0]]==" or ":
print(names[prediction[0]])
else: print("unknown person")
cv2.imwrite('1.jpg',im) mail()
a=input("Enter the pin:")
if a=="1234":
print("Correct user") else:
cv2.putText(im,'Scanning',(x-10, y-10), cv2.FONT_HERSHEY_PLAIN,1,(0, 255,0)) print("unknown person")
cv2.imwrite('1.jpg',im)
mail() a=input("Enter the pin:") if a=="1234":
print("Correct user") cv2.imshow('OpenCV', im)
key = cv2.waitKey(10)
```

CREATE DATA CODING

```
#creating database import cv2, sys, numpy, os importurllib.request import numpy as nphaar_file =
```

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

```
'haarcascade_frontalface_default.xml' datasets = 'datasets' #All the faces data will be present this folder sub_data = 'project'
####sub_data = 'hai' #These are sub data sets of folder, for my faces I've used my name path = os.path.join(datasets, sub_data) if not os.path.isdir(path):
os.mkdir(path)
(width, height) = (130, 100)
# defining the size of images face_cascade = cv2.CascadeClassifier(haar_file) webcam = cv2.VideoCapture(0)
#'0' is use for my webcam, if you've any other camera attached use '1' like this
##url="http://192.168.43.1:8080/shot.jpg"
# The program loops until it has 30 images of the face. count = 1 while count < 101: (_, im) = webcam.read()
## imgPath=urllib.urlopen(url)
##
imgNp=np.array(bytearray(imgPath.read()),dtype= np.uint8)
## im=cv2.imdecode(imgNp,-1) gray = cv2.cvtColor(im, cv2.COLOR_BGR2GRAY) faces = face_cascade.detectMultiScale(gray, 1.3, 4) for (x,y,w,h) in faces:
cv2.rectangle(im,(x,y),(x+w,y+h),(255,0,0),2)
face = gray[y:y + h, x:x + w]
face_resize = cv2.resize(face, (width, height))
cv2.imwrite('%s/%s.png' % (path,count), face_resize) count += 1
cv2.imshow('OpenCV', im) key = cv2.waitKey(10) if key == 27: break
```

SEND MAIL CODING

```
#import RPi.GPIO as GPIO from subprocess import call import time
importos import glob import smtplib import base64 from email.mime.image import MIMEImage from email.mime.multipart import MIMEMultipart from email.mime.text import MIMEText import sys

gmail_user = " miniproject1315@gmail.com " gmail_pwd = "panimalar" FROM = 'ranedahlia@gmail.com'
TO = ['sheelapatrick2010.com']
#must be a list
#IMAGE msg = MIMEMultipart()
time.sleep(1) msg['Subject'] ="SECURITY"
#BODY with 2 argument
#body=sys.argv[1]+sys.argv[2]
body="THIS IS FROM MINI PROJECT REGARDING SECURITY BREACH"
msg.attach(MIMEText(body,'plain')) time.sleep(1)
###IMAGE
fp = open("1.jpg", 'rb')
time.sleep(1) img = MIMEImage(fp.read()) time.sleep(1) fp.close() time.sleep(1) msg.attach(img) time.sleep(1) try:
server = smtplib.SMTP("smtp.gmail.com", 587) #or port 465 doesn't seem to work!
print ("smtp.gmail") server.ehlo()
print ("ehlo") server.starttls() print ("starttls") server.login(gmail_user, gmail_pwd) print ("reading mail & password") server.sendmail(FROM, TO, msg.as
_string()) print ("from") server.close()
print ('successfully sent the mail') except:
print ("failed to send mail")
```

VII. SYSTEM TESTING

Test Cases & Reports

Security module

```
Training...
mini
unknown person
smtp.gmail
ehlo
starttls
reading mail & password
from
successfully sent the mail
Enter the pin:1234
Correct user
mini
unknown person
```

FIG A.1 Test case of Security module

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

Image module

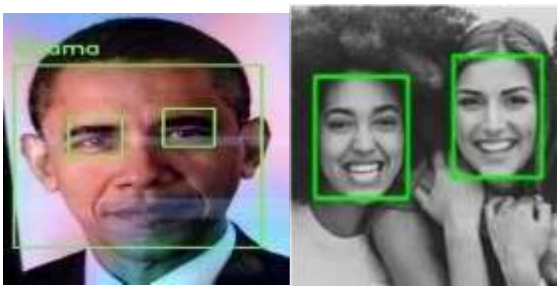


FIG A.2 Test case of Image module

VIII. CONCLUSION

Conclusion and Future Enhancements

Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. This completely eliminates the chances of fraud due to theft and duplicity of the ATM cards.

Face recognition as means of identifying and authenticating account owners at the Automated Teller Machines gives the needed and much anticipated solution to the problem of illegal transactions. In this paper, we have tried to proffer a solution to the much dreaded issue of fraudulent transactions through Automated Teller Machine by face reorganization that can be made possible only when the account holder is physically present. Thus, it eliminates cases of illegal transactions at the ATM points without the knowledge of the authentic owner. Using a facial feature for identification is strong and it is further fortified when another is used at authentication level.

IX. APPENDICES

A.1 SAMPLE SCREENS

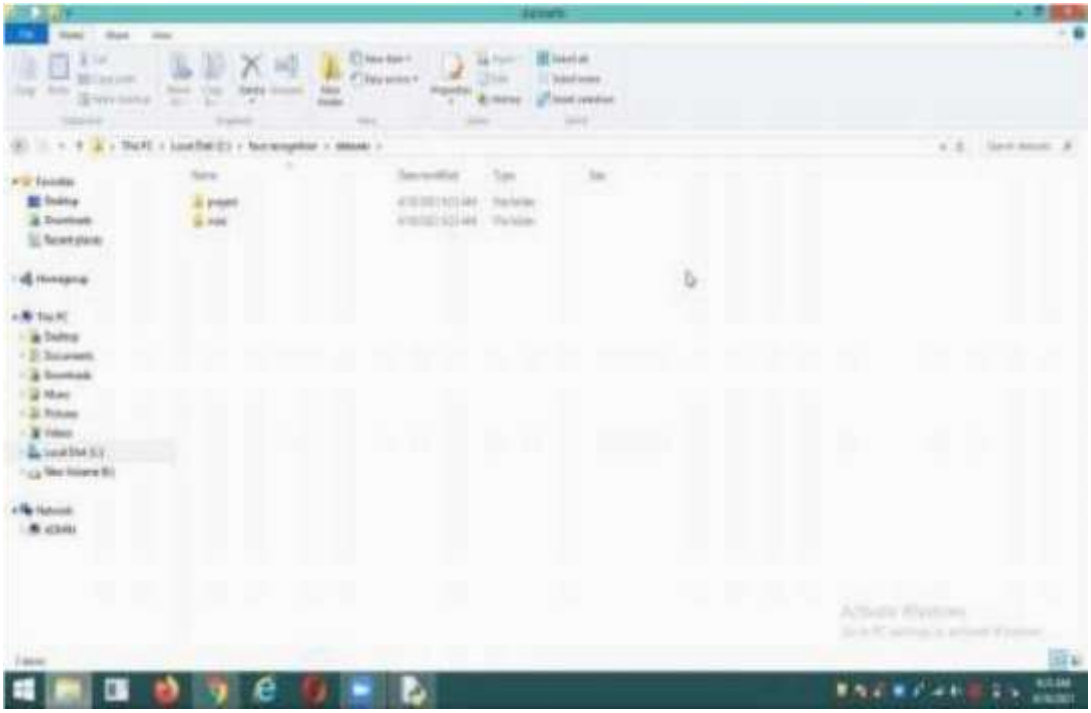


FIG A.3 Creating a Folder for Data Sets

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

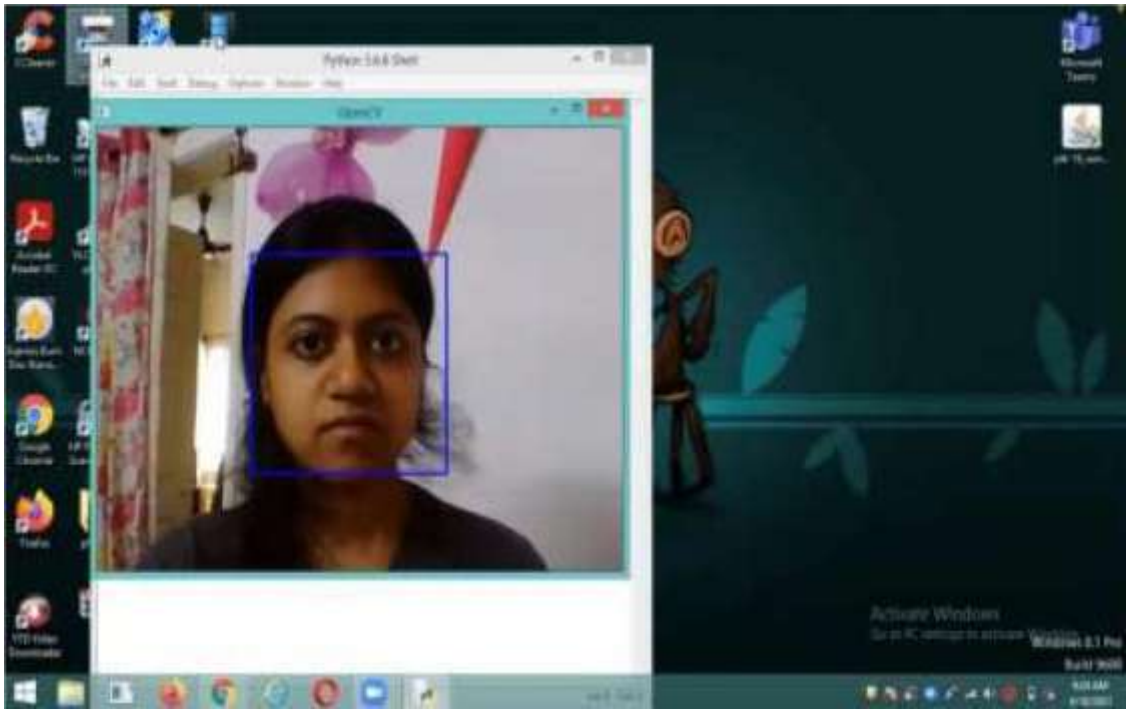


FIG A.4 Capturing Face for Data Set

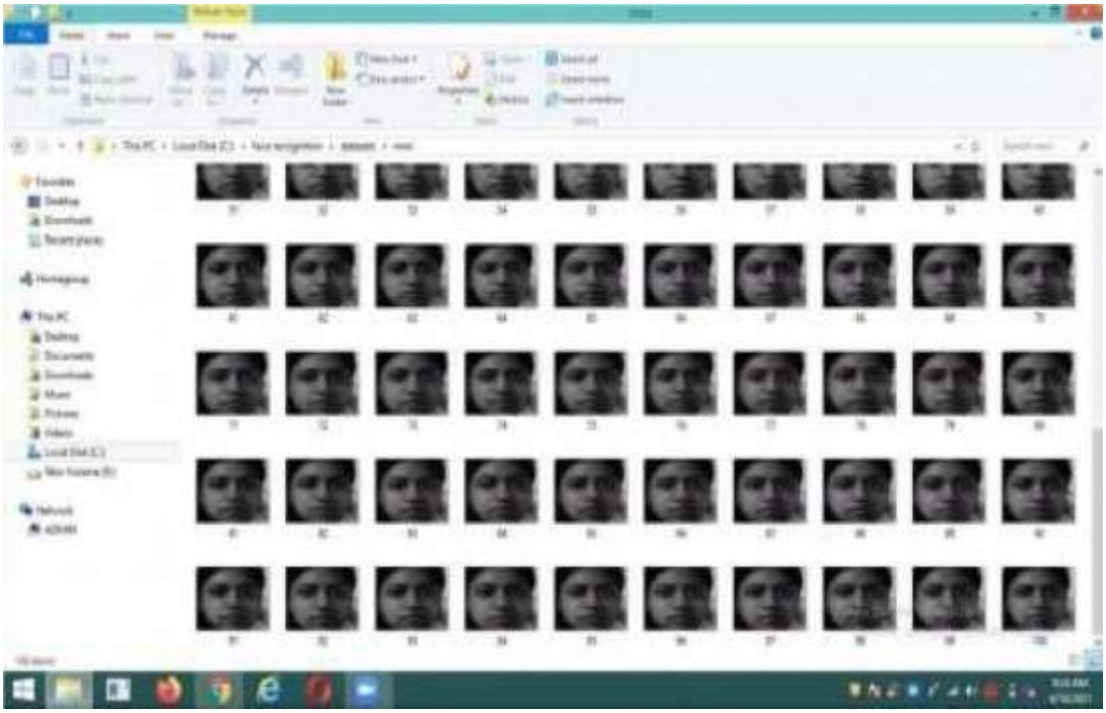


FIG A.5 Saved Data Set

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 10 Oct 2021, pp: 764-776 www.ijaem.net ISSN: 2395-5252

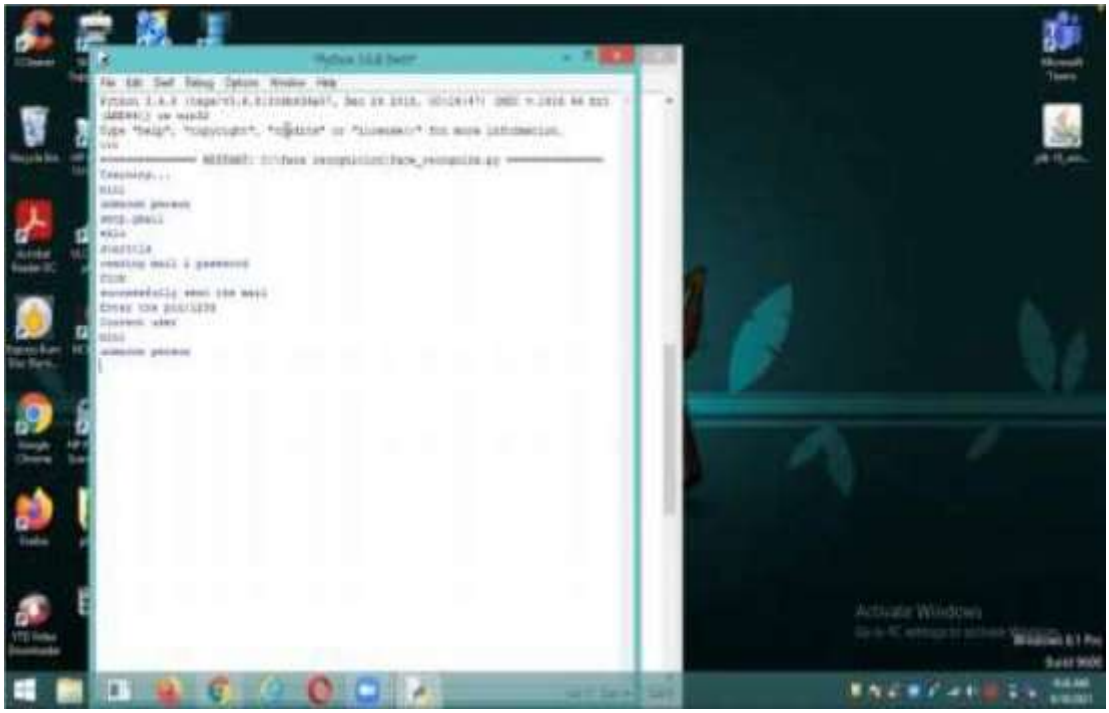


FIG A.6 Enter ATM Pin Number

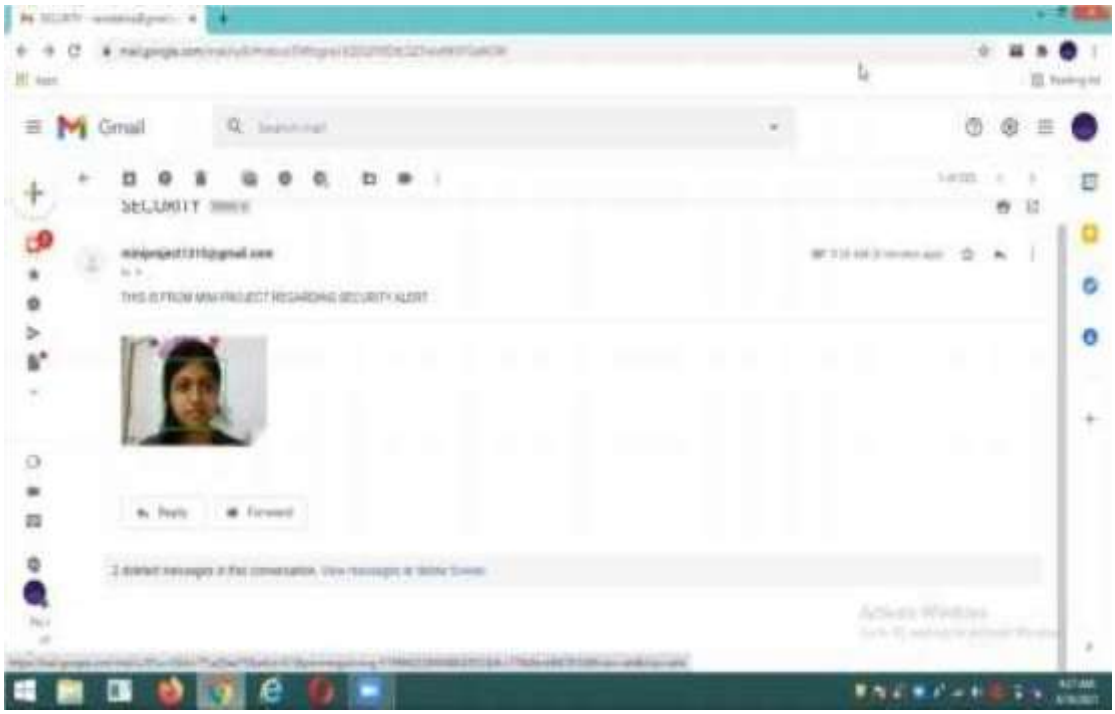


FIG A.7 Generated Security Mail

REFERENCES

[1]. V. V. Jog, D. Jain, R. Arora and B. Bhat, "Theft prevention ATM model using dormant monitoring for transactions," 2013 IEEE Conference on Information & Communication Technologies, Thuckalay, India, 2013, pp. 1156-1159, doi: 10.1109/CICT.2013.6558274.

[2]. V. Jotsov and V. Sgurev, "Applications of Puzzle methods for intrusion detection in ATMs," 2012 6th IEEE

International Conference Intelligent Systems, Sofia, Bulgaria, 2012, pp. 481-488, doi:
[3]. 10.1109/IS.2012.6335180.
[4]. A. T. Siddiqui, "Biometrics to Control ATM scams: study
[5]. A,"2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], Nagercoil, India, 2014, pp.1598-1602, doi: 10.1109/ICCPCT.2014.7054755.
[6]. M. M. E. Raj and A. Julian, "Design and implementation of antitheft ATM machine using embedded systems," 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT2015], Nagercoil, India, 2015, pp. 1-5, doi: 10.1109/ICCPCT.2015.7159316