

# Implementation of ATM Security using Biometrics

Saurabh Patil, Siddhi Bhosle, Candice D'mello, Giselle Barretto.  
Xavier Institute of Engineering, Mahim.

- Saurabh Patil is a Professor from the Computer Department at Xavier Institute of Engineering, Mahim.
- Siddhi Bhosle is a student from the Computer Department at Xavier Institute of Engineering, Mahim.
- Candice D'mello is a student from the Computer Department at Xavier Institute of Engineering, Mahim.
- Giselle Barretto is a student from the Computer Department at Xavier Institute of Engineering, Mahim.

**ABSTRACT**—Today, money transactions are done using Automated Teller Machine cards which play a key role in the nature of trade. The problem with the design of the currently used ATM Systems which includes password & PIN is that they do not have an authentication system to find an authorized user & they also do not provide any security mechanism in case of card misuse. We gained initial ideas by researching current ATM Systems to come up with this design. We then took what we found and made the most user-friendly product possible. For this project we created an ATM System using Biometrics. In this system the user will first have to authenticate himself using various Biometric techniques such as Face Recognition, Fingerprint Recognition, OTP generation using Voice Commands & finally by entering the PIN. We've also added a Machine Learning component to give it an upper hand. The system will undergo learning about the number of transactions, transaction amount & transaction location & will accordingly enable the security mechanism in case the usual limit exceeds, such as freezing the account for a particular time-period. For communication purpose we've used Kerberos which makes use of the third-party utility to authenticate the client to file server. In case of an exception, if an authorized user is unable to access his/her account then in that worst-case scenario, the user will use voice automated code word to login to his account.



## 1 INTRODUCTION:

On September 2, 1969, America's first automatic teller machine (ATM) makes its public debut, dispensing cash to customers at Chemical Bank in Rockville Centre, New York. ATMs went on to revolutionize the banking industry, eliminating the need to visit a bank to conduct basic financial trans-

actions. By the 1980s, these money machines had become widely popular and handled many of the functions previously performed by human tellers, such as check deposits and money transfers between accounts.[1]

An automated teller machine (ATM) is an electronic banking outlet that allows customers to complete basic transactions without the aid of a branch representative or teller. Anyone with a credit card or debit card can access cash at most ATMs. ATM's are widely popular for secure transactions of cash.[2]

Around the world consumers consider safety and security of their payments as a key priority. ATM frauds & Cyber Crimes are increasing radically, so we decided to increase the security level of our system compared to the existing traditional ATM Systems. We decided to incorporate various Biometrics for authentication of the user. Security solutions provided by biometrics include validating a person's physical characteristics such as fingerprints, eyes, palm or particular surfaces on the hand to recognize and validate the person or the user. The products used to provide such kind of biometric security include fingerprint sensors and retina scanners. Therefore, the reason we are moving towards biometric solutions is solely because they cannot be duplicated and are also difficult to fake. Prerequisite being the user should have physical characteristics which are fixed and constant even after a while. The basic thought of biometric validation or verification is that every individual can be recognised by his or her inherent traits. Systems can unbolt mechanically when they recognize fingerprints or faces of authorized user. Besides security, the hidden agenda behind biometric validation/verification has been convenience, as there are so many security pins to remember. Now we don't need to carry a card to withdraw or deposit cash. One of the most vital premises of security is agreement and Authorization. Therefore, most of the areas are slightly shifting towards biometric security systems. Biometrics is one step ahead in the field of security. Multifactor authentication is possible because of Biometric security systems.

Key Words: ATM, biometric, GSM, Face recognition, Fingerprint Recognition, image processing, artificial intelligence.

## 2 EXISTING SYSTEMS:

The ATM systems currently existing validates transactions through the card and by using PIN and security tokens. It allows bank users to authenticate transactions, initiate cash withdrawals and deposits, online payments, account to account transfers as well as balance enquiries. There are few Automated teller machines already available in the market. Understanding these systems will help us to gain insights about our system. We will also get an idea how our system is in comparison with them.

### 2.1 Atm System using Fingerprint Recognition

This implementation uses Fingerprint as authentication and GSM module for otp generation [5]. For fingerprint recognition Minutiae score matching algorithm is used. Minutiae are particular points in a finger image. Generally, there are two types ridge endings and bifurcations. There are more than one minutia present in an individual's finger image and they vary from person to person. The widespread deployment of minutiae matching algorithm is because of the uniqueness. GSM module is utilized when the user is recognized and OTP has to be sent to the user's mobile phone.

### 2.2 Atm system using OTP and Facial Recognition

This implementation uses Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminate Analysis (LDA) for facial recognition.[6] For PCA good dataset is required for matching. Facial features (mouth, eyes, nose, etc.) along with geometric relationships between them are used. GSM module is utilized when the user is recognized and

OTP has to be sent to the user's mobile phone. At this stage a user simply needs to look into the camera installed on ATM. If the user is recognized, then OTP is sent to user's mobile phone.

We will be using the Haar Cascade which is an object detection algorithm to detect objects in video and images. In our system we will use it for facial recognition from a live feed. For this we will have to incorporate the "haarcascade frontal-face default.xml" into our project. Initially the webcam will capture the input video feed of say 640 X 480 pixels, the cascades which are just xml files applies the algorithm after converting the video into frames. It then returns the X and Y coordinates that help in forming a rectangle using `cv2.rectangle()` function around the face of the user. These coordinates can then be used to crop or scale out the face from the image for further processing. For real-time images, the input images will be pre-processed before being passed to the model. This including conversion of images to grayscale and resizing the images.

### 2.3 Online credit card system Based on Kerberos Authentication

In our project we have tried to integrate Kerberos authentication protocol for secure and encrypted transactions. The basic idea about Kerberos is well explained in the paper written by "Kim, J.E." titled "A Secure on-line credit card transaction method based on Kerberos Authentication protocol." [4] Kerberos which is an authentication protocol for client/server applications to increase security.

It is a back-end technology which excels at Single Sign On (SSO) i.e., if you provide your identity once to Kerberos, it will pass your TGT (Ticket Granting Ticket) to other services or machines as a proof of your identity.

## 3 IMPLEMENTATION METHODOLOGY

This section explains in brief the algorithms, methods, Libraries and Frameworks used in our system. We have tried to integrate Face and fingerprint recognition with GSM modem via Kerberos authentication protocol using voice commands. Taking in account the current scenario where the world is striving to fight against the Nobel coronavirus and maintain social distancing, we thought of using voice commands in our system. For this purpose, we have used HTML's Speechrecognition API and developed in JavaScript.

Our project is divided into two modules:

### 3.1 First module

So before entering the PIN which is the only process followed by the existing traditional ATM Systems, in our system the user will have to first undergo Two-Factor Authentication which includes Face Recognition & Fingerprint Recognition in the same sequence as listed here and navigation through the system is using voice commands.

The user has to first register before logging in. Before authentication, the user will first have to login using the Login ID and password which during the entry of a new user will be hashed and stored in the database using the password function.

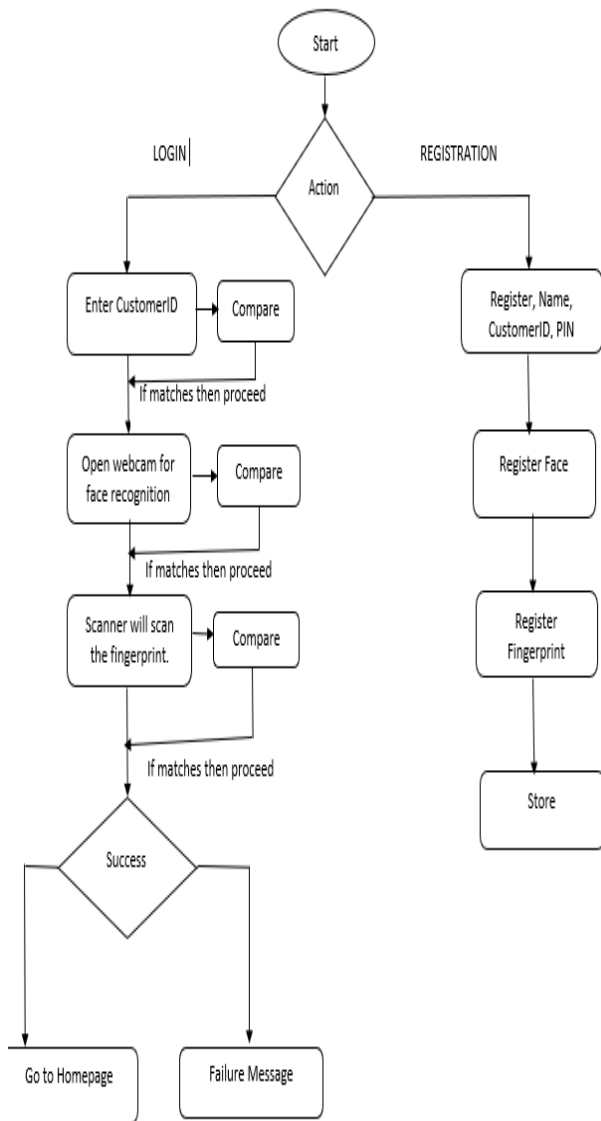


Fig (1): Login and Registration

**OpenCV:**

We have used opencv which is an open-source computer vision and machine learning software

library. It has C++, C, and Python interfaces running on Windows, Linux, Android and Mac.

(OpenCV comes with a trainer as well as a detector. OpenCV already contains many pre-

trained classifiers for face, eyes, smile, etc.) Opencv provides three builtin face recognizers Eigenfaces, Fisherfaces and local binary patterns histogram.

**3.1.1 Face Recognition:**

In the 1<sup>st</sup> Level which is Face Recognition the person’s face will be captured which will identify the person as valid comparing the entry with the input data.

**Haar Cascade Algorithm used for Face Detection:**

Haar Cascade classifier is a machine learning algorithm in which a lot of positive and negative images are used to train the classifier. It essentially has few features like the haar feature selection, creating integral images and cascading classifiers.

The first step is to create the haar features, as edge features, line features and center surround feature. A haar feature considers adjacent rectangular regions at the specified location in a direction window. It sums up the pixel intensities in each region and then calculates the difference between these sums. Integral images are used to make this process faster, most of the images collected are irrelevant, so its job is to identify which ones are relevant and it does this by superimposing the positive images over a set of negative ones. In the next step, haar features are used to detect theoretical fits so we have the eyes, nose and the mouth so essentially this stage of the algorithm is going to be used in face detection and feature extraction in which you are trying to identify how a face looks different from say your hand and you are going to know what a face has like it has two eyes, one nose, one mouth so things like that.

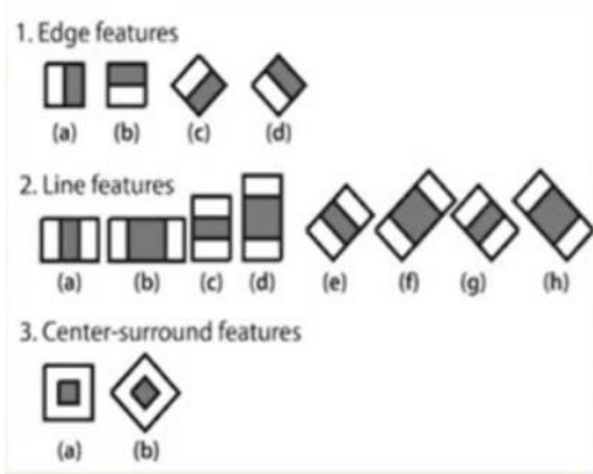


Fig (2): Haar Features

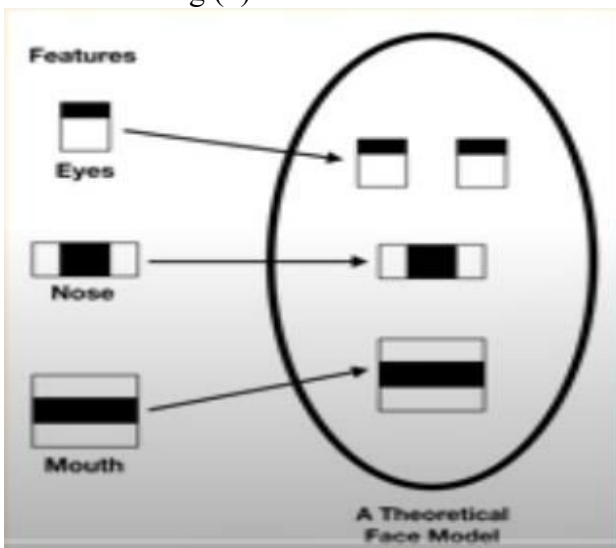


Fig (3): Haar features used to detect theoretical fits (Eyes, nose, and mouth)



Fig (4): Image obtained after Face detection using Haar Classifier

### Face Recognition:

Next, we move to local binary patterns histogram recognizer this is used in the face recognition part. So, once we have identified a face and we know what a face looks like then we are going to pin point whom this face belongs to. (Now lbph works at looking at every single point of the image). Some pixels are generated from each local point, there is a central pixel which we compare with its neighbouring pixels. If the neighboring pixel values are lower than the central pixel then it's written as 0 and if the neighboring pixel values are greater than or equal to the central pixel then it's written as 1. Therefore, we can make a binary pattern of

each individual matrix, (hence the name local binary patterns) These binary patterns are converted into decimal patterns which are plotted on histograms. (Hence each image is going to generate a lot decimal numbers which are plotted on histograms.)

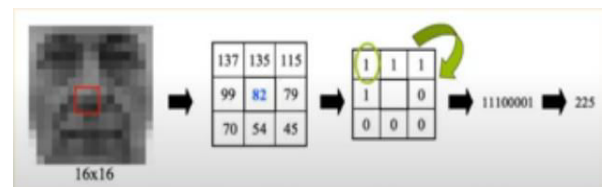


Fig (5): Pixels generated from each local point

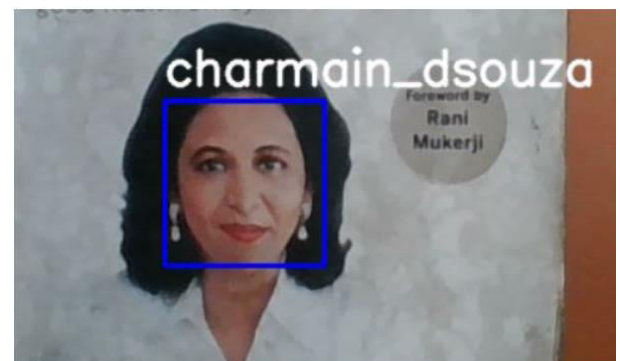


Fig (6): Image obtained after Face recognition using Local Binary Patterns Histogram

### Local Binary Patterns Recognizer used for



### Preprocessing of Images:

- 50 training images generated by the algorithm using "haarcascade\_frontalface\_default.xml" from haar cascades, so 50 histograms are generated in total.
- Read the image
- It reduces the RGB images to grayscale with 8 bit per pixels, and it crops the images to 98x98 pixel values
- Removal of Noise using fastNLMeans-Denoising, which gives a lower confidence than gaussian blur, and then convert image into image array
- During testing, the algorithm again creates a histogram from the test image and it compares that with the training histograms to try to get a match.



Fig (8): Image before pre-processing



Fig (9): Image obtained after pre-processing

Pre-processing Flowchart:

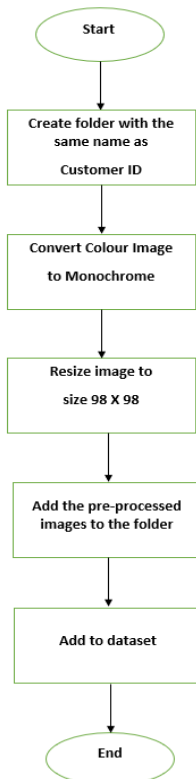


Fig (7): Preprocessing of Images

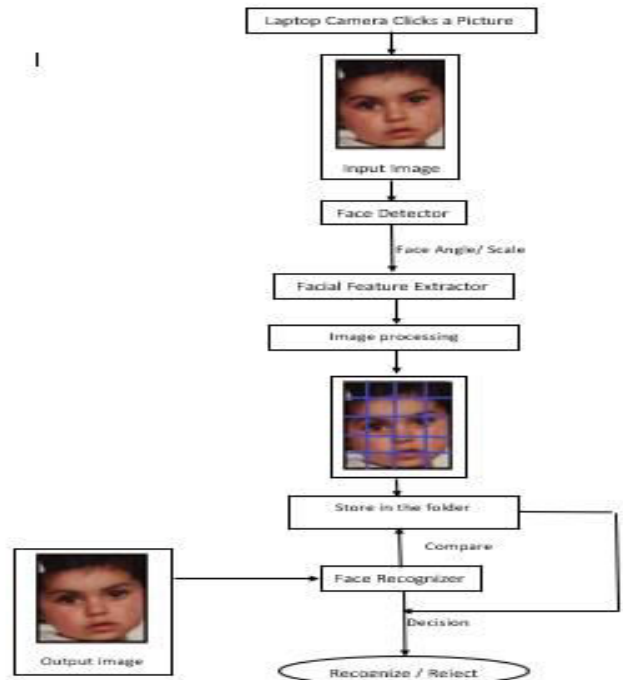


Fig (10): Flowchart for face recognition

**Flask Framework:**

Flask Framework is used to run python scripts on the web for Face/Fingerprint Recognition. Jinja2 is a modern-day templating language for Python developers. It was made after Django’s template. It is used to create HTML, XML or other markup formats that are returned to the user via an HTTP request.

**3.1.2 Fingerprint Recognition:**

Moving to the 2<sup>nd</sup> Level which is Fingerprint Recognition, with the help of a scanner (Generic R307 Optical Fingerprint Reader Module Sensor) the fingerprint of the user will be fed to the system. After matching it with the database, the user will be identified as valid.

After a fingerprint image is obtained by the fingerprint sensor or reader (Generic R307 Optical Fingerprint Reader Module Sensor), this fingerprint must be interpreted. It must be processed in such a way that read-outs can be efficiently compared and matched against each other.

After that the user will have to select a particular action to perform using voice commands and then enter the PIN, which is stored in the database in the encrypted form

Fingerprint Recognition is a technique used to match and identify unique finger prints that might need to be stored and then accessed in a database.

Generic R307 Optical Fingerprint Reader Module Sensor performs preprocessing of the images with a built-in feature. Two important steps required for Recognition are mentioned below:

**1. Enroll Fingerprint.**

The first step is to import the fingerprint package from the python library. The sensor is then tested for initialization with the appropriate

baud rate and it is checked for its password. The template count where the fingerprint can be stored is acquired.

The fingerprint is now detected and converted into machine-readable characters by employing image processing and stored in char buffer 1. With the help, if-else loop conditions the acquired fingerprint is checked for a match with the existing print. If there is any match, the template count of that particular fingerprint should be shown.

Again, the fingerprint is detected and stored in char buffer 2. The same process is repeated. If a new fingerprint is detected it is stored in another variable called PositionNumber. An exception is thrown in case of any discrepancy

**2. Search Fingerprint**

It is used to search our fingerprint from the data which has been stored.

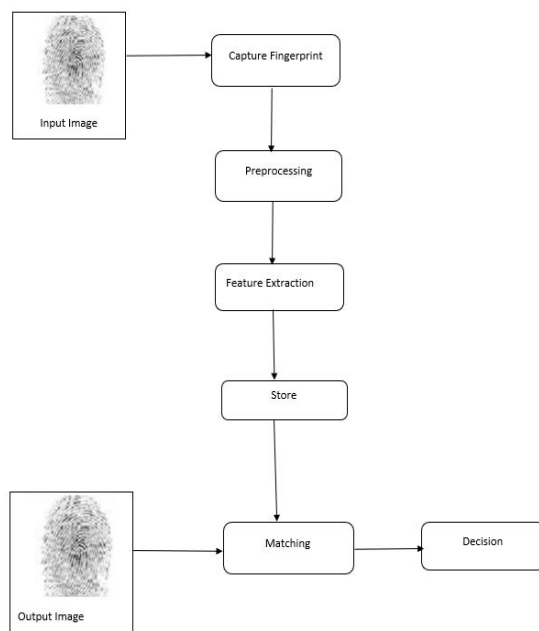


Fig (11): Flowchart for fingerprint Recognition

If the user fails to pass the any of the above authentication levels, then he will be identified as an unauthorized user by the system & the actual user will be notified on his registered mobile number using GSM Modem by a message stating that their ATM account is been accessed by an unauthorized user.

In worst case scenario, if an authorized person is unable to access his/her account using Biometrics due to some issues, then there's an alternative to it which is a voice automated codeword.

Voice automated codeword will be assigned to every valid user having an ATM account. This codeword will be unique for every user and can be used only in case of an exception.

### 3.1.3 Voice Commands:

Taking in account the current scenario where the world is striving to fight against coronavirus and maintain social distancing, we thought of using voice commands in our system using webkitSpeechRecognition.

JavaScript Web Speech API (also known as webkitSpeechRecognition)

webkitSpeechRecognition handles both the recording and transcribing of speech.

### 3.1.4 SMTP Protocol

We have used the SMTP (Simple Mail transfer Protocol) Library in python for sending alert mails to the user. A simple SMTP client session object is created which is used to send emails to any valid email address on the internet. Port used for email is 465. Mailing alerts is one by SMTP instance object called sendmail ()

### 3.1.5 Kerberos Authentication Protocol

The transactions (withdraw and deposit) are carried through Kerberos for ensuring security over transmission line.

For communication we've used Kerberos

which is an authentication protocol for client/server applications to increase security.

It is a back-end technology which excels at Single Sign On (SSO) i.e. if you provide your identity once to Kerberos, it will pass your TGT (Ticket Granting Ticket) to other services or machines as a proof of your identity.

Kerberos uses Key Distribution Centre (KDC) as Third Party to authenticate the client before it can directly request File Server for services.

There are 2 servers located on the Key Distribution Centre (KDC) named as the Authentication Server (AS) and the Ticket Granting Server (TGS) which help Kerberos in this process.

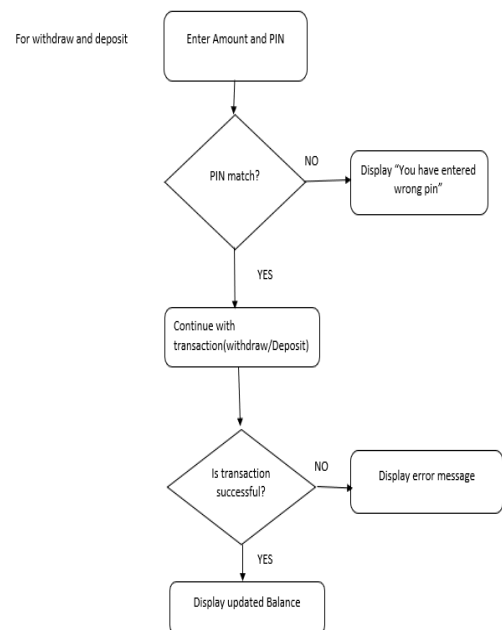


Fig (12): Flowchart Of withdraw/deposit

## 3.2 Second module

In 2013, before Safety Net was built, internal systems at a bank in the United Arab Emirates were compromised, and the cash-withdrawal limits on 12 pre-paid MasterCard debit card accounts were raised by hackers.



The hackers had created fake cards using the stolen account numbers and withdrew cash from ATMs in a number of different countries. According to the post, 300 machines were hit in 26 countries over about 11 hours and more than \$40 million in cash was stolen, including \$5 million in the first four minutes.[3]

We have tried to identify such type of an attack in our system. An anomalous transaction deviating from the baseline behaviour for a particular customer such as large ATM cash withdrawals or transactions made in different geographical regions, the system might decline it and notify the user.

If the user kept trying to complete the transaction, the system will shut down the account temporarily.

### 3.3 Hardware required

#### 3.3.1 RASPBERRY PI 3B+ / 3B PLUS MOTHERBOARD

The Raspberry Pi 3B+ is a cost effective, small in size computer that plugs into a computer monitor or TV. It uses a standard keyboard and mouse. It is a type of compact computer which enables processing to be carried like a normal computer.



Fig (13): Raspberry PI

#### 3.3.2 Easy Electronics SIM900A GSM Modem with SMA Antenna (GSM Module)

The GSM/GPRS Modem-RS232 is assembled with Dual Band GSM/GPRS engine-SIM900A; works on frequencies 900/ 1800 MHz. It provides options for connecting Mic and Speaker directly to GSM MODEM-RS232 for calls. It is compatible with ARDUINO, RASPBERRY PI, ARM, AVR, PIC, 8051, etc. Serial port is also available which helps to directly connect to the computer.

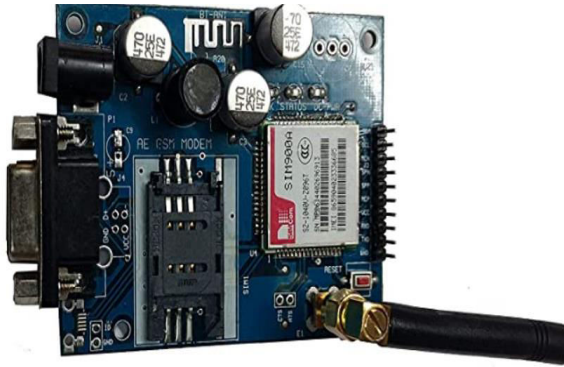


Fig (14): GSM Modem

#### 4 IMPLEMENTATION AND RESULTS:

This part explains in brief the part of the system already implemented.

##### 4.1 REGISTRATION

1. Register the customers basic details like Name, customerID, PIN, base amount, location.
2. Register face (Perform image processing on the captured image and store in a folder)
3. Register Fingerprint

### 3.3.3 Generic R307 Optical Fingerprint Reader Module Sensor

We are using Generic R307 Optical Fingerprint Reader Module Sensor for our project which provides High speed, Fingerprint identification, High accuracy. The fingerprint reader provides secondary development; can be used with wide range of end products.

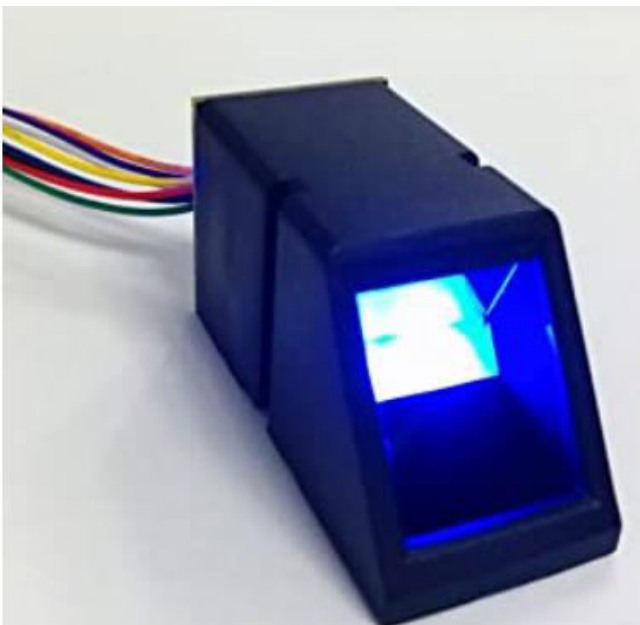
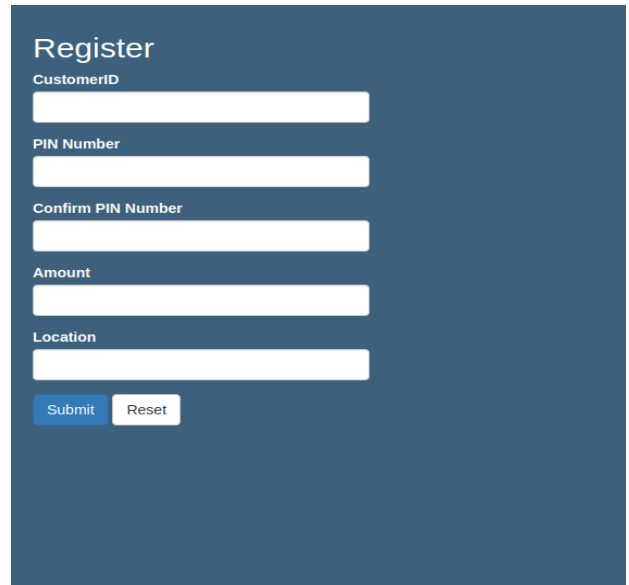


Fig (15): Fingerprint Sensor



STARTING WEB CAM FOR IMAGE REGISTRATION  
Please remain still and look into the camera.

Please wait for your FINGERPRINT REGISTRATION

Fig (16): Registration of the user

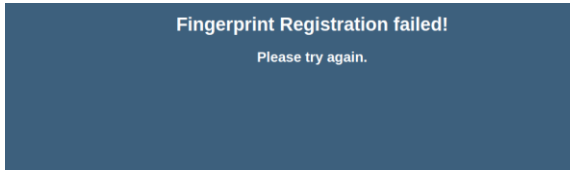


Fig (17): Registration failed

- For the registration of the face, a screen appears, where a message is shown "Starting webcam for image registration, please remain still and look into the camera" Each captured frame is saved in a folder, as the same name of the Customer ID, a total of 50 images are captured, pre-processing is performed
- After registering the face, a screen appears to register the fingerprint, with a message "Please wait for fingerprint registration". If the fingerprint of the user already exists, a message is displayed that the fingerprint already exists, and the registration stops. The sensor asks for fingerprint twice, first time when it asks for the fingerprint the sensor checks for the fingerprint in the memory and if it exists, a message displayed that the fingerprint already exists; the sensor asks for the fingerprint again if the fingerprint is unique it is stored in the sensor's memory. If the sensor cannot read the fingerprint properly, that is when the fingerprint registration fails

#### 4.2 LOGIN

1. Enter CustomerID. Check if the CustomerID exists in database. If exists, proceed forward.
2. Open the webcam for face recognition. The webcam will capture an image of the customer. Based on the CustomerID entered in the first step it will check the folder with the same name as the CustomerID, if image stored inside the folder matches then move forward. If

the recognition fails and the face is not recognized within 15 secs, then access denied screen is shown, and an alert mail is sent to the registered email address

3. After that a screen appears for Fingerprint The customer places his/her finger on then scanner, for Login. After successful login the Customer redirected to the Deposit/Withdraw page. If the recognition fails, access denied screen is shown, and an alert mail is sent to the registered email address

4. After all the authentication steps have been performed and passed the customer will be directed to the home page

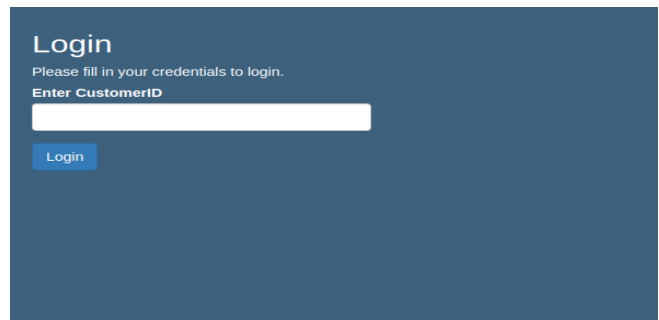


Fig (18): Login for registered user

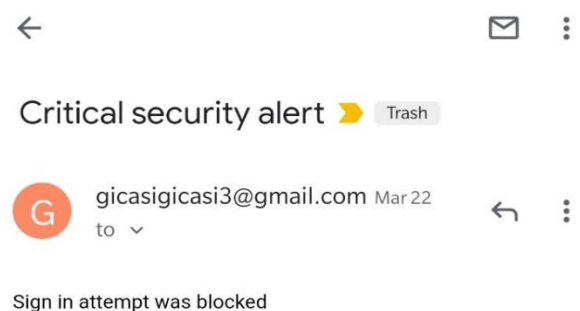


Fig (19): Alert Email if Face/Fingerprint Recognition fails

#### 4.3 TRANSACTION

1. For withdraw and deposit, first enter the amount and PIN, if the pin matches, the

system will allow the transaction to be completed otherwise it will display an error message that says “You have entered the wrong PIN “. It'll then take you back to the same page (withdraw or deposit page).

2. If withdraw or deposit is successful, it'll take you to the balance page which will show you the updated balance.
3. If while withdrawing you try to withdraw more than the current balance an error message will be displayed saying "Insufficient funds".
4. The balance page displays the current balance.

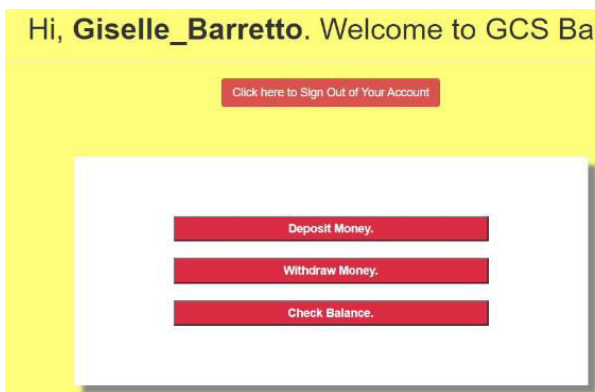


Fig (20): Homepage of the system

#### In the database we have two tables:

1. Users table: This table contains all the user details including CustomerID, Password which is encrypted, amount as well as the current balance at that time.
2. Transaction table: This table contains the transaction history



Fig (21): Deposit



Fig (22): Withdraw

For the machine learning part, if the customer tries to withdraw an unusual amount, a message will be sent to the customer notifying him/her of the unusual activity.

#### 4.4 FACE RECOGNITION

##### Face Recognition happens in three phases:

- Face detection and data gathering  
The Haar Cascade Classifier is used to detect faces or objects. Haar Cascade is a ML approach where a cascade function is trained with lot of positive and negative images, based on training it is then used to detect objects in other images. OpenCV comes with a set of pretrained classifiers for nose, face, eyes etc.

Each captured frame is stored in a folder with the same name as the CustomerID, 50 images are captured which are preprocessed further

- Training of the Recognizer  
The recognizer finds all the images in the dataset, transforms the images into arrays, and then passes the images and their respective CustomerID into the Recognizer for training. After that, the model creates a .yml file containing the corresponding histogram their labels (Supervised Learning) for further Recognition purposes
- Face Recognition

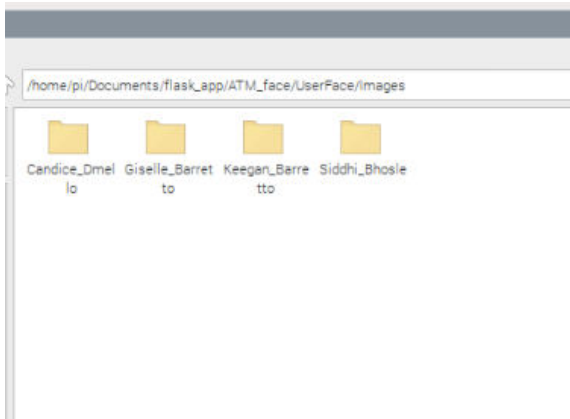


Fig (23): Folders created with names as CustomerID

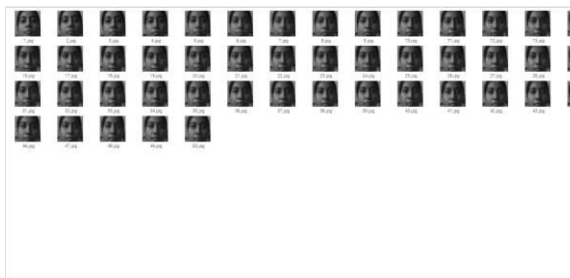


Fig (24): Images inside a folder

#### 4.5 FINGERPRINT RECOGNITION

The sensor will first scan the user’s fingerprint. If the Fingerprint is present in the database, then “Fingerprint already exists”

message is given on the screen. If the Fingerprint is not present in the database, then it’s stored in the sensor’s memory. If the Fingerprint is not read properly by the sensor “Failed to Register/Recognize Fingerprint” message is shown on the screen

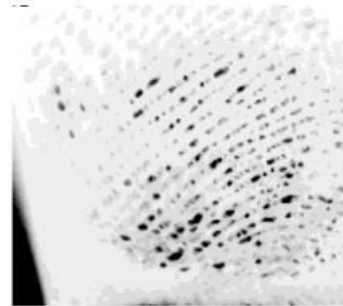


Fig (25): Image of a fingerprint stored in the sensor

#### 4.6 VOICE COMMANDS

The user can also use voice commands, if they want to move to the next page. The user can use the keyword “Login” to be directed to the Login page of the system. The user can use the keyword “Register” to be directed to the Register page of the system

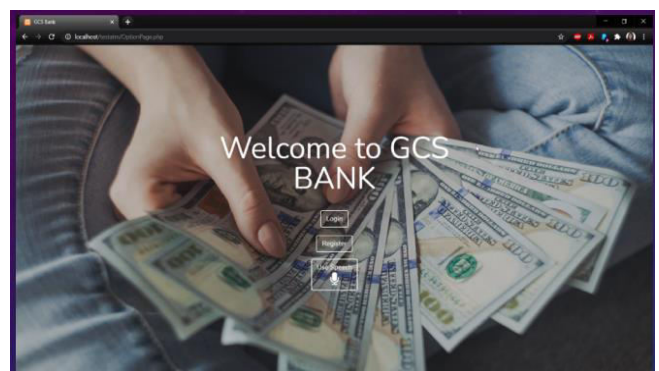


Fig (26): Voice Commands



## 5 CONCLUSION:

The main concept behind this project is to build a system which makes transactions reliable and secure. As we know ATM Card is misemployed in many ways which is a major threat to the society. Therefore, we have implemented multimode biometric to enhance the security of the ATM system. Security system using biometrics has transformed the way people generally regard security. We will further strengthen the security of the system by employing Machine Learning in our ATM system so that if the user displays a behavior diverging from its normal behavior, the system will notify the user and freeze the account for a certain period of time.

## 6 FUTURE SCOPE:

In the future we can add the following points to enhance the security as well as adaptability of the system. Also, if the person who cannot speak wants to perform transaction, he/she can do specific actions which the webcam can identify and AI will respond. We can use security questions as well for worst cases if the person is not authenticated using the biometrics. That is when the account is made some specific question is to be chosen by him as well as answered by him. The person after answering that question will be given the access. Moreover, the machine can be operated by blind persons

## 7 ACKNOWLEDGEMENT:

We would like to express our sincere and heartfelt gratitude to our teacher Prof. Dr. Saurabh Patil who gave us the golden opportunity to do this wonderful project on the topic ATM Transaction Using Biometrics, who also helped us in doing a lot of Research and we learned about so many new things. We are thankful to him for sharing with us

his knowledge and assisting us throughout this project.

## 8 REFERENCES:

- [1] *HISTORY*. (1969, SEPTEMBER 02). Retrieved from <https://www.history.com/this-day-in-history/first-atm-opens-for-business#:~:text=On%20September%20%2C%201969%2C%20America's,in%20Rockville%20Centre%2C%20New%20York>
- [2] *Investopedia*. (2020, April 20). Retrieved from Investopedia: <https://www.investopedia.com/terms/a/atm.asp>
- [3] emerj. (2019, November 22). *Artificial Intelligence for ATMs – 6 Current Applications*. Retrieved from emerj-The AI Research and advisory company: <https://emerj.com/ai-sector-overviews/artificial-intelligence-for-atms-6-current-applications/>
- [4] Kim, J. E. (2010). *A Secure on-line credit card transaction method based on*. Las Vegas.
- [5] Dutta, M., Psyche, K.K. and Yasmin, S., 2017. ATM transaction security using fingerprint recognition. *Am J Eng Res (AJER)*, 6(8), pp.2320-0847.
- [6] Karovaliya, M., Karedia, S., Oza, S. and Kalbande, D.R., 2015. Enhanced security for ATM machine with OTP and facial recognition features. *Procedia Computer Science*, 45, pp.390-396.

