Smart Secured Wireless ATM using Finger Print Recognition

Manjari Jain, Sagar, Saravanan K

Abstract*: *Automated Teller Machines (ATMs) have become an essential part of the individual's daily routine as it is utilized to change one's existing ATM Personal Identification Number (PIN), check one's amount balance and its most important function is to extract one's money. Nowadays, the culprits have the latest technologies at their disposal, which aids them, to easily hack into the secured systems of the banks and collect the confidential information of the clients such as their ATM PINs, Card Details, etc., To counter that, fingerprint sensing incorporated with One Time Passwords (OTPs) has been suggested, as it is globally accepted that the fingerprints of every person are unique and different, while OTPs don't hold its value like ATM PINs. This research is based on using Python Graphical User Interface (GUI) as the ATM screen. The innovation in this study exists in two ways. The first one is that OTPs will be sent via Python Graphical User Interface (GUI), on the client's registered email address also (along with the client's recorded phone number), so that OTPs can still be accessed in case of Subscriber Identity Modules (SIMs) lost. The second one is that including a Uniform Resource Allocator (URL: www.msbank.co.in) for online enrollments of the clients and producing Application Program Interfaces (APIs). The main idea is to first check the client's fingerprints and then to verify the OTPs from our Admin-Password Protected Mongo Database. The involved algorithm also maintains a check that the same email address cannot be utilized again for registration.

Keywords*: *APIs, Fingerprint, MongoDB Python GUI.

I. INTRODUCTION

In today's world, people are using computers to store huge data sets. Data is inexpensively transmitted through the whole wide world. We are using ATM for approximately more than 50 years since its inauguration. From its launch to its present date, ATM has created an environment of withdrawing money without any difficulties.

In the area of banking, the flexibility of ATM to be deployed in every location possible is considered to be of eminence because that gives the liberty to the clients to make transactions at their end. The card reader and keys act as input gadgets while the visual screen and cash dispenser act as output tools. The bank-owned host processor acts as a medium channel for numerous ATMs to collaborate with them on the common level. [2]. Authorized Banks generate distinguished ATM PINs for their clients. These ATM PINs are sent through a registered phone number. If someone knows the user's card details and saw the notification of PIN on a user's phone. Then, they have the full accessibility to the client's account and can be responsible for any illegalities caused. Criminals have contrived different strategies to take cash from ATMs. Since they can't simply remove cash from an ATM because of intensely made sure about the money compartment, they rather take card data of different clients. Taking ATM card data is a lot simpler than breaking into the ATM itself. Card skimming is one of these techniques hoodlums regularly use. Card skimmers are introduced on ATMs card per user space. They have an electronic circuit to peruse the data on an attractive piece of the card and this data is put away on card skimmer's memory. This data is later replicated by the lawbreakers in the wake of expelling the skimmer from the ATM. Card skimmers are intended to be an ideal fit over unique cards per user so clients can without much of a stretch fall prey to it. On the off chance that card spaces feel massive or free, there are chances that it is a skimmer gadget.

There are likewise phony key cushions accessible in obscurity web commercial centers over the web, which can be put over the first key cushion of the ATM, which logs all the client inputs. These logged inputs are then abused by crooks to take cash from the client account. Fraudsters can likewise introduce a little camera simply over the keypad of the ATM, which continues recording client inputs, which incorporate your ATM PIN too. Clients are regularly exhorted by their banks to shroud keypad with their other hand while entering the PIN. At times, the whole front of the ATM is supplanted with a phony front, which looks precisely like a genuine one. If there should be an occurrence of a phony ATM front, it turns out to be difficult to know whether the ATM has been undermined. Cash doesn't apportion out of the phony front and it likewise continues recording client inputs.

Various methods have come to neutralize this current situation, one of them is face recognition fails because due to aging in the human biological body, the various facial features grow out of proportion of the last image taken of the user. The user has to re-register his/her image periodically to sustain its productivity, which could be a tremendous effort for a bed-ridden patient or face-burnt victims.

On the other hand, the recognition of fingerprints is widely accepted because of its permanence and uniqueness. Here, the fingerprints are converted to templates so no misuse of the system is possible [1]. The biometric recognition happens in two stages: enrollment and recognition: identification and verification. [3] [4]

Revised Manuscript Received on May 20, 2020.
* Correspondence Authors

Manjari Jain*, Bachelor of Technology (Electronics and Communication Engineering), Vellore Institute of Technology, Vellore, Tamil Nadu, India. Email: manjari.jain2016@vitstudent.ac.in

Sagar, Bachelor of Technology (Electronics and Communication Engineering), Vellore Institute of Technology, Vellore, Tamil Nadu, India. Email: sagar.2016@vitstudent.ac.in

Saravanan K, Professor, School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. Email: kasisaravanan@vit.ac.in

Stage 1: Enrollment => The enrollment works in a way that first it encounters a fingerprint from the user, processes it to a digital image, purged the undesired features from it. Post-process the image and stored it in the database.

Stage 2: Identification => We used a fingerprint sensor for operating on a fingerprint, it forms the feature extraction from it, matched it with the N templates of a fingerprint from our database.

Stage 3: Verification => On the matching of the fingerprint with a particular fingerprint from our database, we verified it again by running the same fingerprint with the matched database again.

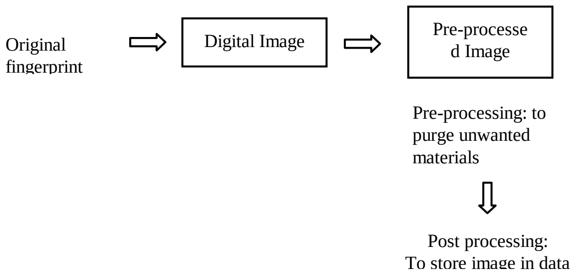

Original fingerprint
Digital Image
Pre-processed Image
Pre-processing: to purge unwanted materials
Post processing: To store image in data

Fig 1.1 Enrollment. [1]

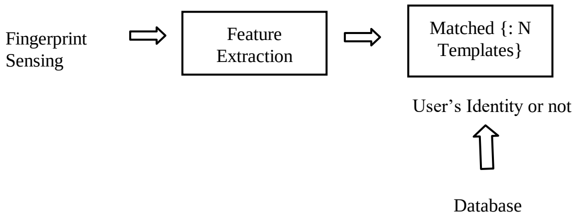


Fig 1.2 Identification. [1]

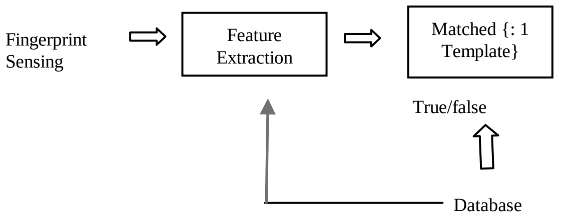


Fig 1.3 Verification. [1]

The usage of biometric attributes offers a plethora of satisfaction over conventional methods. Fingerprints don't tarnish over any period of time. Therefore, due to their uniqueness and indestructible nature, fingerprint recognition is accoladed as one of the best measures to ensure security.

On of top of the fingerprint recognition, three One Time Passwords will be sent to the matched fingerprint customer's registered Email ID customeruser@example.com along with the registered Phone Number 99XXXXXXXX. If he is able to enter the OTPs correctly on or before the third OTP is transferred, then, by all means, he is eligible to perform transactions. If he enters the amount to be withdrawn higher than the amount present in his bank account, then he has to start the process from the beginning. On completion of the transaction, he will receive a text message on phone as well as his email stating that the transaction was successfully on this Account No: 56XXXXXX with the remaining balance. On the other side, after the failure of the third OTP, he will receive an alert security breach email and will be asked to contact his nearest branch as soon as possible.

II. LITERATURE SYNOPSIS

Korea welcomed its first ATM in 1975. With the help provided by the Shinhan Bank, the locals were able to utilize the advantages of an ATM. [5].

According to [6], there was a webcam installed on the ATM which stores the live photo-age of any clients that walk by. This captured image is then contrasted with the remaining images from the database. The successful result of the contrast generates an arbitrary password that is delivered on the client's registered phone. Then the client is instructed to enter the same password on the ATM screen. If the user enters accurately then he/she can perform transaction operations. But this theory has two major flaws: 1) If the mobile phone is lost or stolen then it will become difficult to prevent theft from happening until unless immediate action is taken. 2) With aging, our facial expressions tend to change. Hence the original image captured at that time will be compared with the latest image of our faces which will lead to discrepancies.

The Palm Print Recognition and Confirmation System used by the ATM [7], the idea of using the PIN as a secure password are not highly suitable by the researchers. Therefore, to broaden the security, incepting the concept of palmprint authorization was introduced. The profound research was that a simulator imitates the current ATM functions. In concluding, they compared 89.43% of the cervical recognition program with a rejection rate of 10.57% [7]. Therefore, 53 out of 500 customers who visit the upgraded ATMs through this verification process might have difficulties. The rejection rate was elevated as high as ten percent.

The Graphical User Authentication introduced by Lalzirtira was to purge mistakes in the alphanumeric certification of ATMs. The work done by him suggested that a code that incorporates image is more straightforward. He came up with a password that would aid clients to memorize it easily in their minds [8]. The pass-code which includes images for providing authorization in the ATM system has its advantages in some levels but failed due to video recordings.

Another theory that was established was of dyno-passwords. Here the client is provided with a text message from the bank on their registered phone number containing the passcode. This new passcode will be entered through the ATM screen. The database server of the bank will again cross-examine it. Thus, implying to withdraw money from ATM, all one needs is the client's PIN, card, and SIM. Anyone in the social circle of the client can be easily equipped with this amount of confidential information. As a result of this, this theory opened the doors for hackers [9].

According to [10], other neural network-based research work has been pursued to match clients' fingerprints through the method of its patterns of ridges established. This theory was achievable only on binary images; On the other hand, this research states that once a group is traced, then it can be traced with utmost efficiency.

This theory fails on the grounds of unreachable neural networks [10].

[11] The bankers have to collect the client's fingerprints and their phone numbers when registering for the first time. As soon as the client locates his finger on the fingerprint sensor, he will receive an automated generated message of the four-numbered password on his GSM phone. The clients are requested to enter the same password. If it is validated, then the client can proceed towards the transaction. The only fatal flaw of this research is that once the client lost the hold on his SIM Card then he can no longer perform any actions despite being an authenticated user of the bank.

The process of authentication for fingerprints in an embedded environment follows two stages:

Minutia extraction and Minutia coordinating. Equipment programming co-plan answerable for coordinating two unique finger impression details sets and recommends the utilization of reconfigurable designs for the Automatic Fingerprint Authentication System. This paper clarifies the nitty-gritty execution of a unique finger impression calculation utilizing a Spartan-6 FPGA, as a proper versatile and minimal effort gadget. The chip runs with high precision, yet with less speed for applications which are utilizing the details based unique mark coordinating calculation. The estimation on Laptop may not be precise because of issues of continuous limitations not upheld by the Windows 7 Operating System. However, this assessment needs to stress the reaction time distinction as far as greatness requests. [16][18]

Here, we learned that the Fingerprint Authorization in an embedded environment incorporates a microchip with cumulated accuracy, but with decreased momentum for processes that are using the instructions based on distinctive patterns of mathematical calculation.

III. PRESENT ATM

A computerized technology that establishes the role of being a monetary medium between the clients and the bank to maintain the functionality of transactions without the presence of a third party. Some charge cards, be that as it may, may experience more difficulty. ATMs are highly feasible because it allows the clients to perform any required transaction without having the obligation to go to the bank.

The PIN stands for Personal Identification Number. It is a combination of four numbers, each one ranging from 0 to 9 amounts to a decade of PINs possible, which is preferably set by the clients. This PIN remains universal throughout the longevity of the bank account until unless it is not changed by the client. Since it is modicum in size, it can be swiftly memorized. The hacker has every technological tool at their disposal to guess the accurate PIN [12][13]. When the client enters the PIN on the ATM screen then it is cross-examined from the database of the bank organizations. The present ATM works in such a way that the person first enters the ATM. He/she inserts his/her ATM card into the machine. Then, they enter the ATM PIN for verifying that they are the owner of the ATM Card. After the verification, they select the type of Accounts from which they want to withdraw money. If they have sufficient balance in their account, the ATM dispenses the amount and informed them via a Text Message / Email about the transaction successful and remaining balance present in the amount.

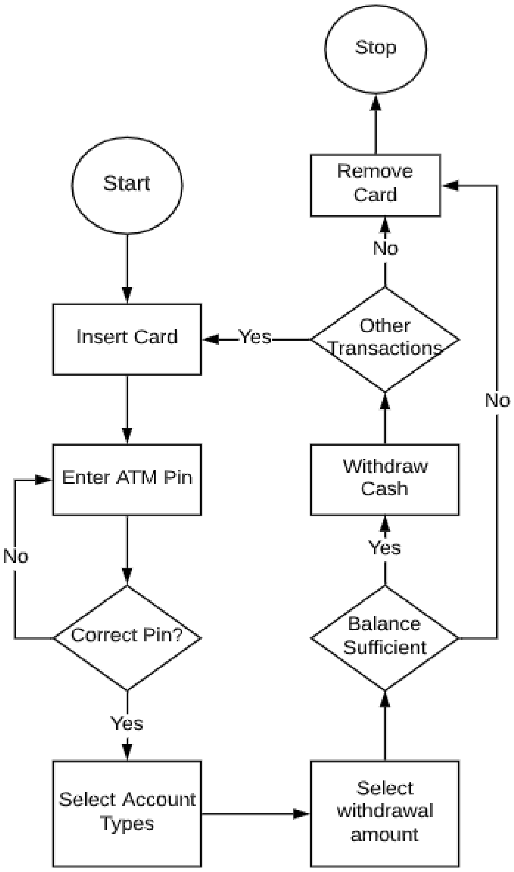


Fig 3.1 Present ATM Flowchart.

IV. METHODOLOGY

Our initiated methodology is to include fingerprint recognition along with the One Time Passwords. Hence, we are appending one more layer of secured and personal identification in the present system. Only after careful verification of the clients' fingerprints, they will proceed to their registered Email IDs as well as registered Phone Number to check for One Time Password from the bank. They will be given three chances to write their correct OTP in front of the ATM screen. If they enter it accurately, then they will be permitted to withdraw money on the contingency of having sufficient balance in their accounts. On the other hand, even after providing them with three One Time Passwords, they enter incorrectly then they will receive a mail from us stating of "Security Breach and Kindly Contact your nearest branch". We will be using APIs to send and receive data of the uniquely identified customer.

Hardware Required:

- Fingerprint Sensor Adafruit R307
- Arduino Uno
- Power Supply
- Connecting Wires

Software Required:

- Python
- Spyder
- Tkinter
- Mongo DB
- Visual Code (Node JS)

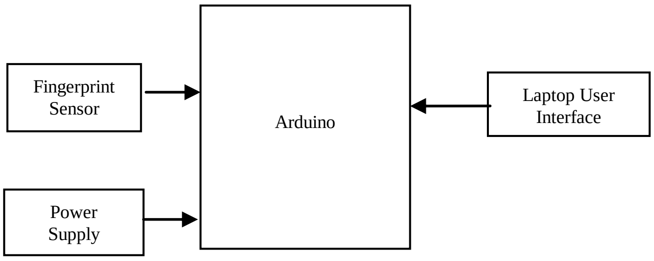


Fig 4.1 Block Diagram.

A. Fingerprint Recognition

The most widely accepted security measure to be installed in the ATM is of biometric fingerprint technology. It delivers a much more secure initiative than the existing ATM security. The quality of this technology to be elegantly aligned with our present lives is quite impressive as it is quite undemanding to install and to be operated at. Due to this, it is accoladed as one of the most successful authentication techniques. The fingerprints data are not stored in any database; thus, no misuse of the fingerprint is conceivable. [24]

The unique finger impression ID depends on two fundamental suppositions: - Invariance and Peculiarity Invariance. Invariance implies the finger impression qualities don't change along with life. Peculiarity: implies the unique mark is extraordinary and no two people have a similar example of a unique finger impression.

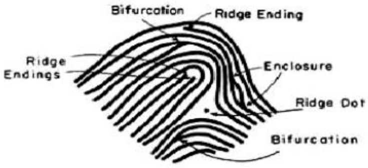


Fig 4.2 Features of a Fingerprint. [1]

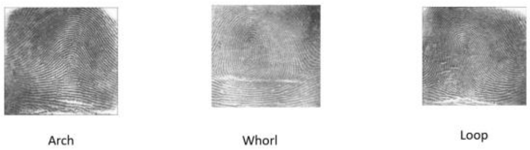


Fig 4.3 Types of Fingerprints.

Unique biometric impression: The unique pattern is the component example of the biometric authentication as follows: [2]

- *Step 1) Binarization:* It describes the changes from greyscale into binary picture by finalizing the esteem value. [2]
- *Step 2) Block Filter:* It is the method of diminishing the thickness of all ridgelines to a solitary pixel
- width to extricate minutiae viably. [2]
- *Step 3) Minutiae Extractruction:* Details are inferred following minutiae removal. [2]
- *Step 4) Minutiae Matching:* It is to compare the data of distinctive finger impressions. The layout of minutiae coordination is also employed. [2]
- *Step 5) Matching Score:* It is the relation to calculate the collaborating score of the original fingerprint & template data. [2]

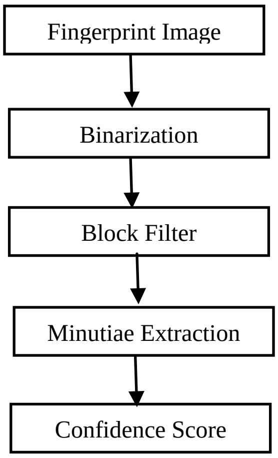
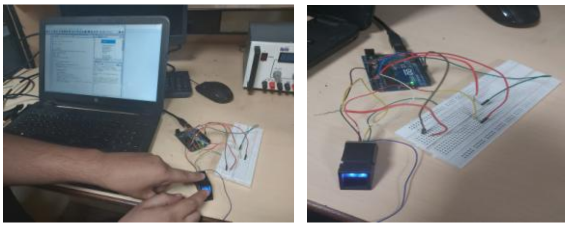


Fig 4.4 Fingerprint Authentication Process Diagram. [2]

B. Workflow



(a) *(b)*

Fig 4.5 Circuit Diagram

The framework is introduced to implement explicit assignments, such as validating python code, email correlation, Phone compatibility, etc. and subsequently each method reset to start regulations.

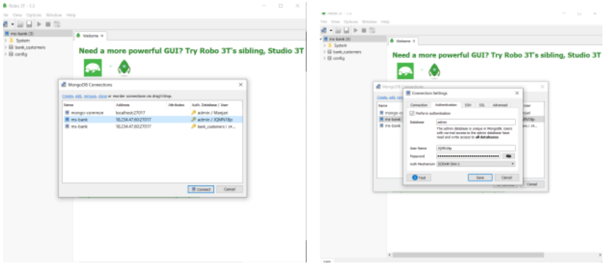
The purposed methodology is different from the current ATM system as it incorporates fingerprint sensing in it. It will begin such as the user enters the ATM:

[Step 1] It will be first labeled as to whether he/she is an existing customer or a new customer that wants to open their account in our bank. If he/she is an existing customer then they will be asked to directly proceed to the fingerprint authentication part of the process. Otherwise, he/she will be asked to register with us by submitting their frequently used Email Address and Phone Number along with his/her fingerprint in our database.

[Step 2] After that, both the existing and new customers will be acquired to give their fingerprints for verification of their existence in our database.

They are allowed to scan their fingerprints as long as they reach a satisfying confidence match from our database. If the fingerprint authentication fails, then they will be restricted to take part in the next steps.

Here are the images of our secured database:



Need a more powerful GUI? Try Robo 3T's sibling, Studio 3T

MongoDB Connections

Name	Address	Attributes	Auth. Database / User
mongo-common	localhost:27017		admin / Manjari
ms-bank	18.234.47.60:27017		admin / XQMN18p
ms-bank	18.234.47.60:27017		bank_customers / 14...

Connection Settings

☑ Perform authentication

Database: admin

User Name: XQMN18p

Password: ••••••••••••••••••••••••••••••

Auth Mechanism: SCRAM-SHA-1

(a) *(b)*

Fig 4.6. Password Protected DB

(It shows that only one who has the authenticated credentials like admin and password has the ability to access the database.)

Thus, this is to ensure that the fraudulent activities happening as the hacker can easily trace the confidential information such as Card Number, Personal Information Security, and the mobile number will diminish to such an extent that it creates a sense of safe and secure environment.

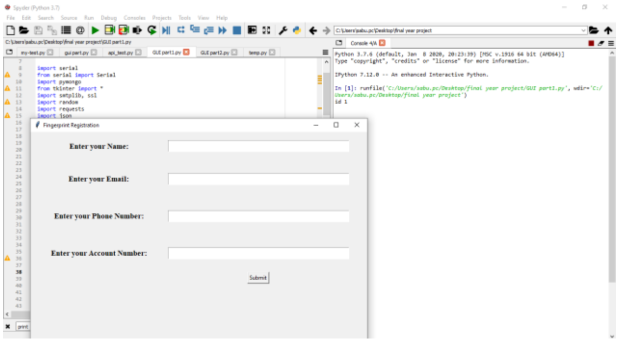
[Step 3] On the successful verification of the fingerprint, they will be asked to enter the first OTP send to their registered Email Address and Phone Number. If they enter it correctly, they will be asked to enter the amount they want to withdraw.

[Step 4] If the amount entered is less than the balance present in the bank account, they will successfully withdraw it. On the backend side, we will update the remaining balance in our database.

[Step 5] If they fail to enter their first OTP accurately, then a second OTP will be sent to their Email Address and Phone Number again with following the same consequences.

[Step 6] On the third OTP, they will have only this chance to enter it fairly. If they failed to do so, then from our side, a security breach mail and a text message will be sent to their registered Email Address and Phone Number and they will be locked out to proceed for the transaction of money. They have to start over with the whole process again.

We are using Python GUI Tkinter as the interface to take the input from the user. We are using APIs and Mongo DB to extract and deliver the data of customers on the requirement. We have deployed an online URL for registering using WIFI with us: www.msbank.co.in. This URL is used for generating Application Program Interfaces. They are used for storing the credential information of the clients in the MS Bank Storage. They are simultaneously updated with any changes performed in the Admin-Password Protected Database. They are also used to find information about the particular client in general.



Spyder (Python 3.7)

C:\Users\sabu.pc\Desktop\final year project\GUI part1.py

```
import serial
from serial import Serial
import pymongo
from tkinter import *
import smtplib, ssl
import random
import requests
import json
```

```
Python 3.7.6 (default, Jan  8 2020, 20:23:39) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.12.0 -- An enhanced Interactive Python.

In [1]: runfile('C:/Users/sabu.pc/Desktop/final year project/GUI part1.py', wdir='C:/Users/sabu.pc/Desktop/final year project')
id 1
```

Fingerprint Registration

Enter your Name:

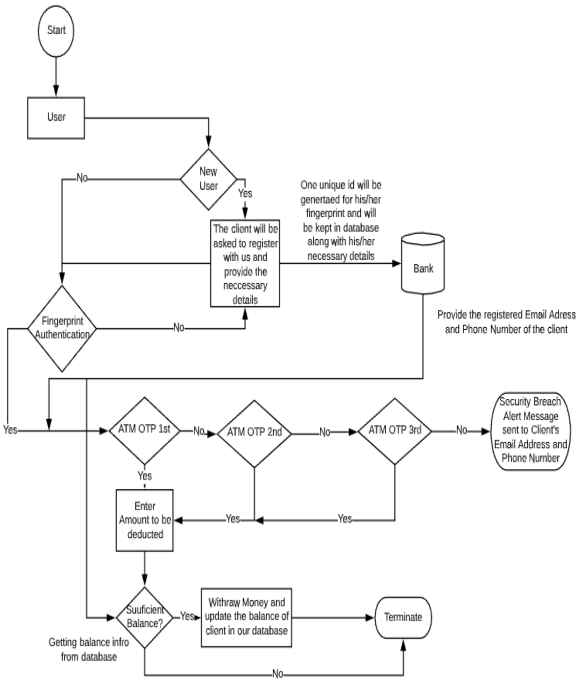
Enter your Email:

Enter your Phone Number:

Enter your Account Number:

Fig 4.7 Python GUI for entering data.

(It is the GUI for entering the details when the new client comes to the bank, it takes name, email, phone and account no as input.)



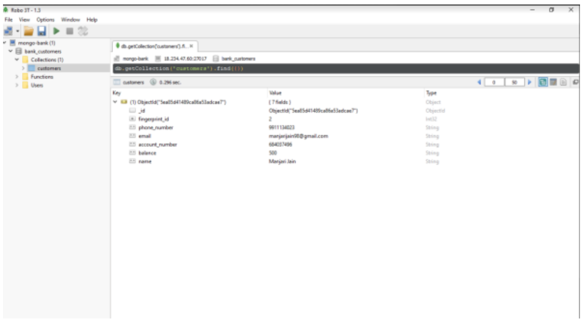
Start
User
New User
No
Yes
The client will be asked to register with us and provide the neccessary details
One unique id will be genertaed for his/her fingerprint and will be kept in database along with his/her necessary details
Bank
Provide the registered Email Adress and Phone Number of the client
Fingerprint Authentication
No
Yes
ATM OTP 1st
No
ATM OTP 2nd
No
ATM OTP 3rd
No
Security Breach Alert Message sent to Client's Email Address and Phone Number
Yes
Enter Amount to be deducted
Yes
Yes
Suuficient Balance?
Yes
Withraw Money and update the balance of client in our database
Terminate
Getting balance info from database
No

Fig 4.8 Proposed Methodology.

V. RESULT AND DISCUSSION

Here is the technical output of the research:

Database:



Robo 3T - 1.3

```
db.getCollection('customers').find({})
```

mongo-bank   18.234.47.60:27017   bank_customers

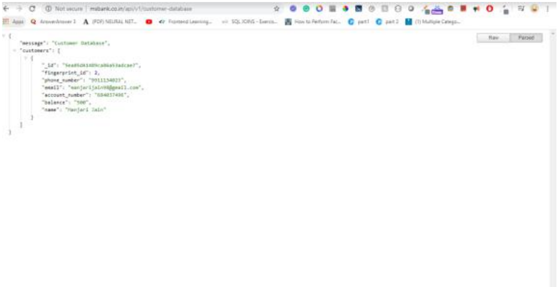
customers   0.296 sec.

Key	Value	Type
(1) ObjectId("5ea85d41489ca86a53adcae7")	{ 7 fields }	Object
_id	ObjectId("5ea85d41489ca86a53adcae7")	ObjectId
fingerprint_id	2	Int32
phone_number	9911134023	String
email	manjarijain98@gmail.com	String
account_number	684037496	String
balance	500	String
name	Manjari Jain	String

Fig 5.1 (a) Mongo DB

DOI: 10.35940/ijitee.H6165.069820

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

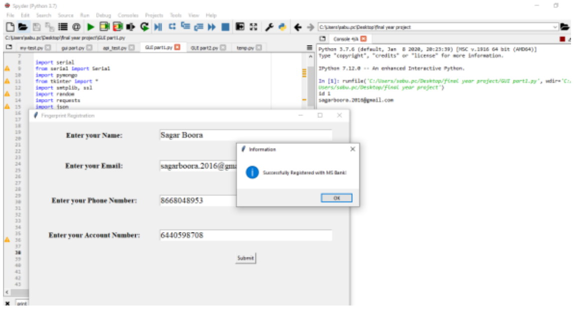


```
Not secure | msbank.co.in/api/v1/customer-database
{
    "message": "Customer Database",
    "customers": [
        {
            "_id": "5ea85d41489ca86a53adcae7",
            "fingerprint_id": 2,
            "phone_number": "9911134023",
            "email": "manjarijain98@gmail.com",
            "account_number": "684037496",
            "balance": "500",
            "name": "Manjari Jain"
        }
    ]
}
```

Fig 5.1 (b) APIs

Explanation: It shows our database of current customers registered in MS Bank.

Storing new entry:



```
import serial
from serial import Serial
import pymongo
from tkinter import *
import smtplib, ssl
import random
import requests
import json
```

```
Python 3.7.6 (default, Jan  8 2020, 20:23:39) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.12.0 -- An enhanced Interactive Python.

In [1]: runfile('C:/Users/sabu.pc/Desktop/final year project/GUI part1.py', wdir='C:/Users/sabu.pc/Desktop/final year project')
id 1
sagarboora.2016@gmail.com
```

Fingerprint Registration

Enter your Name: Sagar Boora

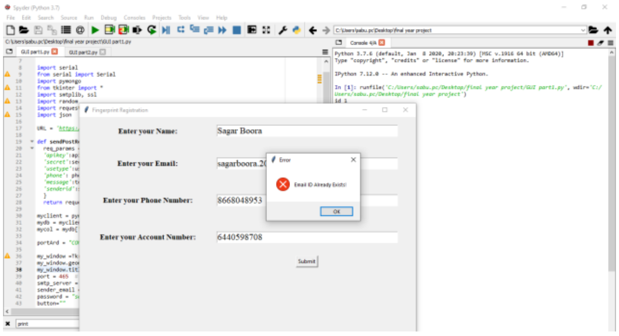
Enter your Email: sagarboora.2016@gm

Enter your Phone Number: 8668048953

Enter your Account Number: 6440598708

Information: Successfully Registered with MS Bank!

Fig 5.2 (a) Storing new data



```
import serial
from serial import Serial
import pymongo
from tkinter import *
import smtplib, ssl
import random
import reques
import json

URL = 'https:/

def sendPostR
    req_params
    'apikey':ap
    'secret':se
    'usetype':u
    'phone': ph
    'message':t
    'senderid':
    }
    return requ

myclient = py
mydb = myclie
mycol = mydb[

portArd = "CO

my_window =Tk
my_window.geo
my_window.tit
port = 465
smtp_server =
sender_email
password = "s
button=""
```

```
Python 3.7.6 (default, Jan  8 2020, 20:23:39) [MSC v.1916 64 bit (AMD64)]
Type "copyright", "credits" or "license" for more information.

IPython 7.12.0 -- An enhanced Interactive Python.

In [1]: runfile('C:/Users/sabu.pc/Desktop/final year project/GUI part1.py', wdir='C:/Users/sabu.pc/Desktop/final year project')
id 1
```

Fingerprint Registration

Enter your Name: Sagar Boora

Enter your Email: sagarboora.20

Enter your Phone Number: 8668048953

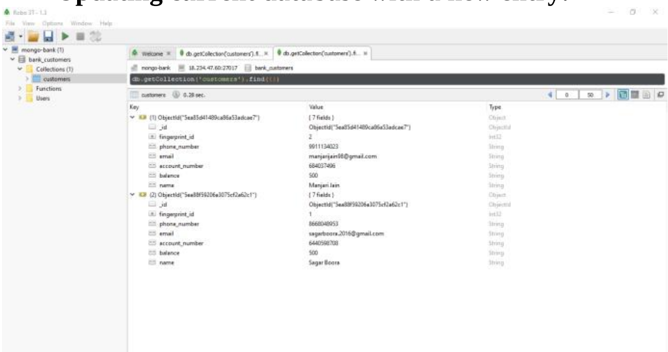
Enter your Account Number: 6440598708

Error: Email ID Already Exists!

Fig 5.2 (b) Warning for using the same email

Explanation: *(a):* The new user enters the bank, this GUI appears on the ATM Screen which stores his fingerprint and personal information such as Name, Email, Phone Number, and Account Number. After entering the details, a successful message pop up will appear. *(b):* It shows that the same email address cannot be used again as it already exists in our database.

Updating current database with a new entry:



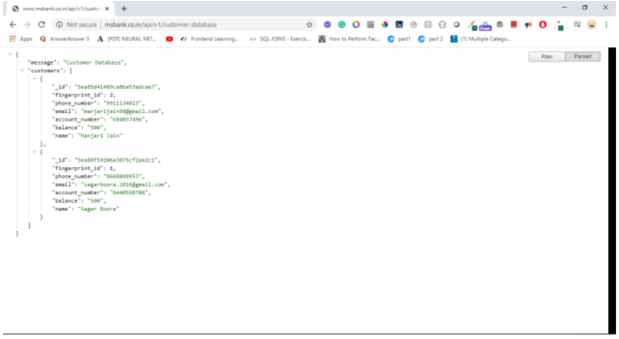
mongo-bank | 18.234.47.60:27017 | bank_customers

```
db.getCollection('customers').find({})
```

customers 0.28 sec.

Key	Value	Type
(1) ObjectId("5ea85d41489ca86a53adcae7")	{ 7 fields }	Object
_id	ObjectId("5ea85d41489ca86a53adcae7")	ObjectId
fingerprint_id	2	Int32
phone_number	9911134023	String
email	manjarijain98@gmail.com	String
account_number	684037496	String
balance	500	String
name	Manjari Jain	String
(2) ObjectId("5ea88f59206a3075cf2a62c1")	{ 7 fields }	Object
_id	ObjectId("5ea88f59206a3075cf2a62c1")	ObjectId
fingerprint_id	1	Int32
phone_number	8668048953	String
email	sagarboora.2016@gmail.com	String
account_number	6440598708	String
balance	500	String
name	Sagar Boora	String

Fig 5.3 (a) Mongo DB Updated

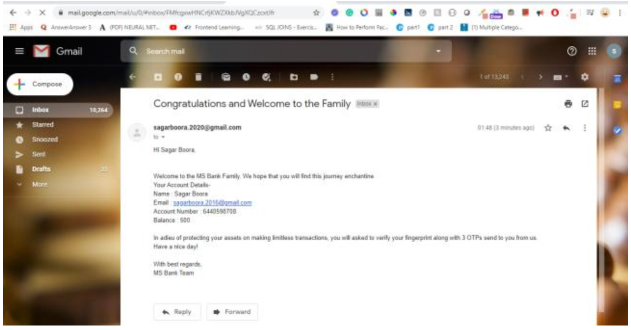


```
Not secure | msbank.co.in/api/v1/customer-database
{
    "message": "Customer Database",
    "customers": [
        {
            "_id": "5ea85d41489ca86a53adcae7",
            "fingerprint_id": 2,
            "phone_number": "9911134023",
            "email": "manjarijain98@gmail.com",
            "account_number": "684037496",
            "balance": "500",
            "name": "Manjari Jain"
        },
        {
            "_id": "5ea88f59206a3075cf2a62c1",
            "fingerprint_id": 1,
            "phone_number": "8668048953",
            "email": "sagarboora.2016@gmail.com",
            "account_number": "6440598708",
            "balance": "500",
            "name": "Sagar Boora"
        }
    ]
}
```

Fig 5.3 (b) APIs Updated

Explanation: *(a):* Mongo DB and *(b):* APIs are updated with the database of the new user. It shows the new data has been successfully stored in our database as well as APIs.

Confirmation Mail:



Congratulations and Welcome to the Family

sagarboora.2020@gmail.com
01:48 (3 minutes ago)

Hi Sagar Boora,

Welcome to the MS Bank Family. We hope that you will find this journey enchantine
Your Account Details-
Name : Sagar Boora
Email : sagarboora.2016@gmail.com
Account Number : 6440598708
Balance : 500

In adieu of protecting your assets on making limitless transactions, you will asked to verify your fingerprint along with 3 OTPs send to you from us.
Have a nice day!

With best regards,
MS Bank Team

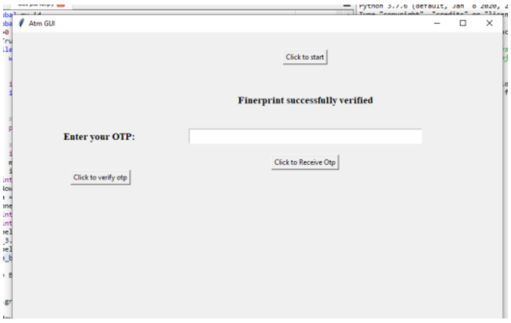
Fig 5.4 Confirmation Mail.

Explanation: After successful registration, MS Bank sent a confirmation mail to the new user along with his/her account details that he/she enters in figure 5.2 (a).

After successful fingerprint verification, two cases arise such as:

Case 1: Case of entering OTP correctly:

It represents that any registered customer, who enters the OTP matching from the text messages and emails, is allowed to make the transactions depending on the amount present in his/her bank account.



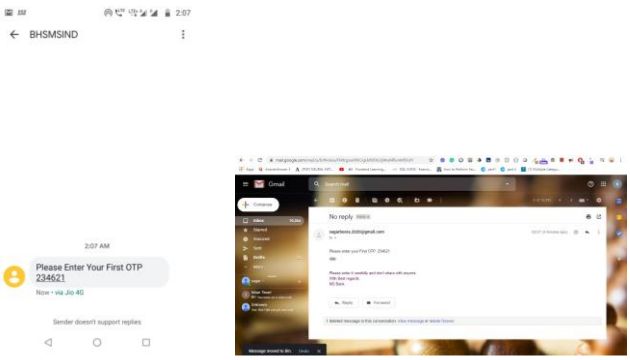
Atm GUI

Finerprint successfully verified

Enter your OTP:

Fig 5.5 Successful Fingerprint Verification.

Explanation: After successful fingerprint verification of the newly registered user, then a new GUI appears asking for the first OTP to be entered here.



2:07

BHSMSIND

2:07 AM

Please Enter Your First OTP
234621

Now • via Jio 4G

Sender doesn't support replies

Gmail

No reply

sagarboora.2020@gmail.com

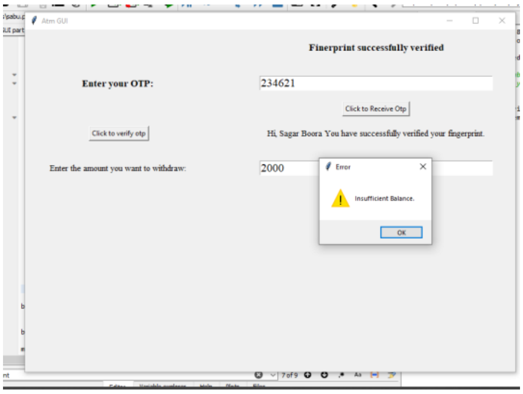
Please enter your First OTP: 234621

Please enter it carefully and don't share with anyone.
With Best regards,
MS Bank

Reply Forward

Fig 5.6 (a) C1: First OTP on Phone and (b) C1: First OTP on Email

Explanation: The same first OTP was sent on the new user's registered Phone Number *(a)* and Email Address *(b)*. This OTP is required to be entered by the new user after his/her successful fingerprint authentication



Atm GUI

Finerprint successfully verified

Enter your OTP: 234621

Click to Receive Otp

Click to verify otp

Hi, Sagar Boora You have successfully verified your fingerprint.

Enter the amount you want to withdraw: 2000

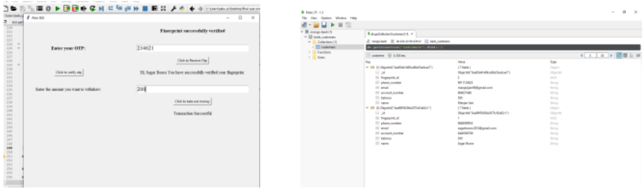
Error

Insufficient Balance.

OK

Fig 5.7 Correct OTP with insufficient balance

Explanation: When the customer enters the correct OTP but put the insufficient amount to be dispensed then it shows a warning of having "Insufficient Balance". This GUI reflects that the client doesn't have the authority to withdraw the amount when the money present in his/her account is less than the amount entered.



Finerprint successfully verified

Enter your OTP: 234621

Click to Receive Otp

Click to verify otp

Hi, Sagar Boora You have successfully verified your fingerprint.

Enter the amount you want to withdraw: 200

Click to take out money

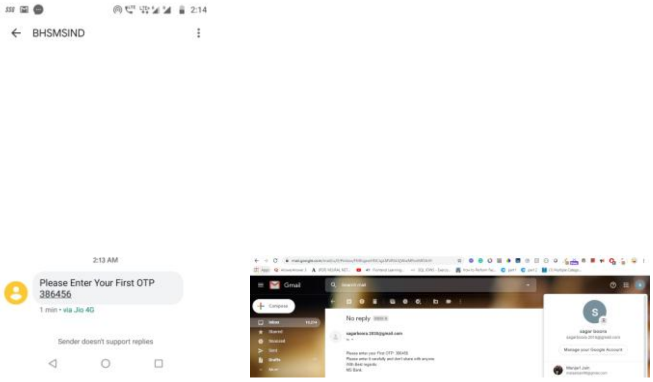
Transaction Successful

Fig 5.8 (a) Correct OTP with sufficient balance. (b) Remaining balance updated in Mongo DB

Explanation: *(a):* when the customer enters significant amount (less than the money present in his/her account) then it is allowed to be dispersed and *(b):* we update the remaing amount in our database.

Case 2: Case of entering OTP incorrectly:

This is the case where any registered customer fails to enter the OTP accurately for the third time. Due to this, they will receive a "Security alert, kindly contact your nearest branch as soon as possible" Email.



2:14

BHSMSIND

2:13 AM

Please Enter Your First OTP
386456

1 min • via Jio 4G

Sender doesn't support replies

Gmail

No reply

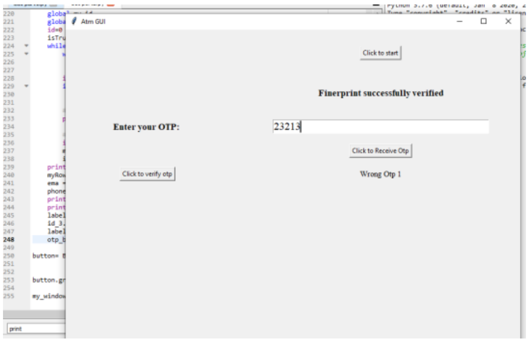
sagarboora.2020@gmail.com

Please enter your First OTP: 386456

Please enter it carefully and don't share with anyone.
With Best regards,
MS Bank

Fig 5.9 (a) C2: First OTP on Phone and (b) C2: First OTP on Email

Explanation: The same first OTP was sent on the client's registered Phone Number *(a)* and Email Address *(b)*. This OTP is required to be entered by the client after his/her successful fingerprint authentication



Atm GUI

Click to start

Finerprint successfully verified

Enter your OTP: 23213

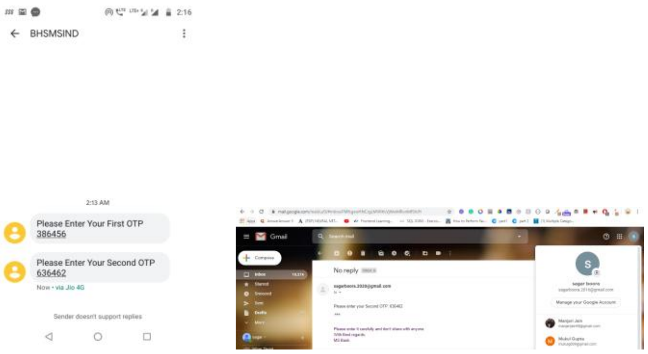
Click to Receive Otp

Click to verify otp

Wrong Otp 1

Fig 5.10 C2: First OTP Wrong.

Explanation: The customer enters the first OTP wrong. When the customer enters the first OTP which doesn't match the one send to the registered Email and Phone No, then the GUI prints a warning stating that "Wrong otp 1". After this customer has to click "Click to Receive OTP" in to receive the second OTP.



2:16

BHSMSIND

2:13 AM

Please Enter Your First OTP
386456

Please Enter Your Second OTP
636462

Now • via Jio 4G

Sender doesn't support replies

Gmail

No reply

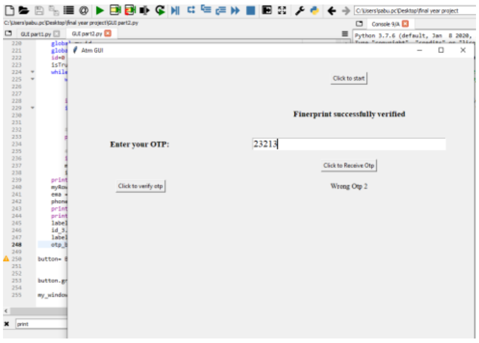
sagarboora.2020@gmail.com

Please enter your Second OTP: 636462

Please enter it carefully and don't share with anyone.
With Best regards,
MS Bank

Fig 5.11 (a) C2: Second OTP on Phone and (b) C2: Second OTP on Email

Explanation: The same second OTP was sent on the client's registered Phone Number *(a)* and Email Address *(b)*. This OTP is required to be entered by the client.



Atm GUI

Click to start

Finerprint successfully verified

Enter your OTP: 23213

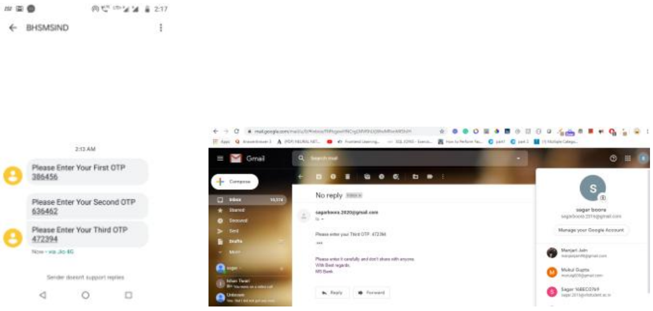
Click to Receive Otp

Click to verify otp

Wrong Otp 2

Fig 5.12 C2: Second OTP Wrong.

Explanation: The customer enters the second OTP wrong. When the customer enters the second OTP which doesn't match the one send to the registered Email and Phone No, then the GUI prints a warning stating that "Wrong otp 2". After this customer has to click "Click to Receive OTP" in to receive the third OTP.



BHSMSIND

2:13 AM

Please Enter Your First OTP 386456

Please Enter Your Second OTP 636462

Please Enter Your Third OTP 472394

No reply

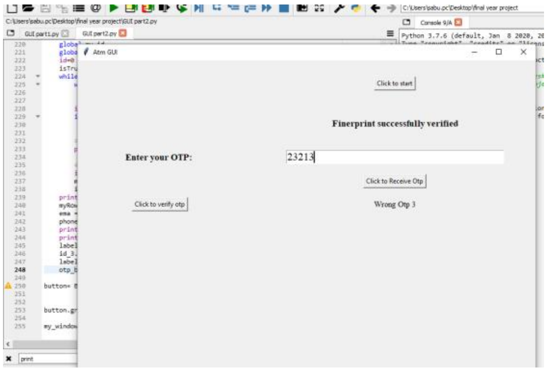
sagarboora.2020@gmail.com

Please enter your Third OTP : 472394

Please enter it carefully and don't share with anyone.
With Best regards,
MS Bank

Fig 5.13 (a) C2: Third OTP on Phone and (b) C2: Third OTP on Email

Explanation: The same third OTP was sent on the client's registered Phone Number *(a)* and Email Address *(b)*. This OTP is required to be entered by the client.



Atm GUI

Click to start

Finerprint successfully verified

Enter your OTP: 23213

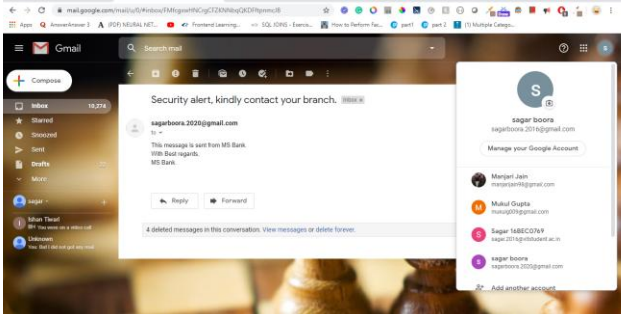
Click to Receive Otp

Click to verify otp

Wrong Otp 3

Fig 5.14. C2: Third OTP Wrong.

Explanation: The customer enters the third OTP wrong. When the customer enters the second OTP which doesn't match the one send to the registered Email and Phone No, then the GUI prints a warning stating that "Wrong otp 3". After this, the customer is not allowed to make a transaction and has to start the process again to withdraw money. Along with this restriction, he/she receives an alert email from our side.



Security alert, kindly contact your branch.

sagarboora.2020@gmail.com

This message is sent from MS Bank.
With Best regards,
MS Bank

4 deleted messages in this conversation. View messages or delete forever.

Fig 5.15 Security Alert Message.

Explanation: Security Theft Alert Message to the customer's registered Email Address after he/she failed at the third time to enter the OTP accurately.

VI. CONCLUSION

There are some discrepancies in the past research for improving the ATM security using fingerprint authentication as being discussed in the Literature Synopsis. Thus, there was a necessity to improvise the scope of ATM safety with a better and cost-effective solution. The answer is to incorporate fingerprints as well but the direction of sending OTPs varies from the previous studies, as OTPs are conveyed out in two ways: client's registered email address and phone number. The methodology works such that it provides the alternative to the new client to register with the bank using Python GUI (ATM Screen). For the registered clients, the ATM Fingerprint Sensor first acknowledges that the biometric is authenticated. After that, an OTP is forwarded to the contact details of the client. If the client fails to enter the first one correctly, he/she is left with 2 more possibilities to enter it accurately. On the account of third OTP failure, the client (or suspected hacker) is blocked from making any transactions and a Security Theft Alert mail is also dispatched. A URL www.msbank.co.in is also utilized for the online registrations of clients as well as constructing APIs to safely store the data of our new and enrolled clients. As a result, in case of WIFI absence, the client can use his/her mobile OTP, or in case of SIM lost, the customer can retrieve that same OTP from his/her logged email address. In conclusion, the results obtained from the research proved that this theory is attainable.

REFERENCES

1. Kavitha Hooda, International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016, "ATM Security", pp-1.
2. Mithun Dutta, Kangkhita Keam Psyche and Shamima Yasmin, American Journal of Engineering Research (AJER), Volume 6, Issue 8, August 2017, "ATM Transaction Security Using Fingerprint Recognition", pp-41-45.
3. Zhao F., Tang, X., The Journal of the Patter Recognition Society, Volume 40, Issue 4, April 2007, "Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction", pp-1270-1281.
4. F. A. Afsar, M. Arif and M. Hussain, National Conference on Emerging Technologies, 2004, "Fingerprint Identification and Verification System using Minutiae Matching", pp-141-146.
5. Hmadri nath maoulick, Joyjit Patra, Arun Kanti Manna, International Journal of Engineering Inventions, Volume 3, Issue 1, August 2013, "Computer Assisted and Contour Detection in Medial Image Using Fuzzy Logic", pp-1-7.

6. Frimpong Twum, Kofi Nti, Michael Asante, International Journal of Science and Engineering Applications, Volume 5, Issue 3, May 2016, “Improving Security Levels in Automatic Teller Machines (ATM) Using Multifactor Authentication, pp-503.
7. Sanjay S. G., International Journal of Engineering and Computer Science, 2014, “ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation System”, pp-5332-5335.
8. Lalzirtira, National Institute of Technology Rourkela M. Tech Thesis, 2013, “Graphical User Authentication, India”.
9. Anand D. A., Dinesh G. and Naveen H. D., International Journal of Communication and Computer Technologies (IJCCT), 2013, “A Reliable ATM Protocol and Comparative Analysis on Various Parameters with other ATM Protocols”, pp-192-197.
10. Saropourian, B., ICCSIT, 2009, 2nd IEEE International Conference, 2009, “A new approach of finger-print recognition based on neural network”, pp-158-161.
11. Ratha, N., Connel, J. & Bolle, R., IBM Systems Journal, Volume 40, No. 3, 2001, “Enhancing Security and Privacy in Biometrics-based Authentication Systems”, pp-614-634.
12. Sowmya Ravikumar, Sandhya Vaidyanathan, B. Thamotharan, S. Ramakrishan, International Journal of Engineering and Technology, Volume 5, No. 3, 2013, “A new business model for ATM transactions security using fingerprint recognition”.
13. Petrlic, Ronald and Christoph Sorge, IET Information Security, Volume 8, Issue 2, 2013, “Establishing user trust in automated teller machine integrity”, pp-132-139.
14. Myo, N., International Conference on Education Technology and Computer, 2009, “Fingerprint Identification based on the Model of the Outer Layers of Polygon Subtraction”, pp-201-204.
15. Journal for Research, Volume 2, Issue 12, February 2017.
16. Ms. Archana S. Shinde and Prof. Varsha Bendre, 2015 International Conference on Computing Communication Control and Automation, 2015, “An Embedded Fingerprint Authentication System”, pp-45.
17. Jun Zhou, Guangda Sua, Chun hongJiang, Neurocomputing, 70, 2007, “A face and fingerprint identity authentication based on multi-route detection”, pp-922-931.
18. Yuliang He, Jie Tian, Xiping Luo, Tanghui Zhang, Pattern Recognition, Letters 24, 2003, “Image enhancement and minutiae matching in fingerprint verification”, pp-1349-1360.
19. Wei Wang Jianwei Li, Feifei Huang, Hailiang Feng, Pattern Recognition, Letters 29, 2008, “Design and implementation of Log-Gabor filter in fingerprint image enhancement”, pp-301-308.
20. Lin Hong, Wan Yifei, Anil Jain, IEEE Transaction on patter Analysis and Machine intelligence, Volume 20, Issue 8, 1998, “Fingerprint image enhancement: algorithm and performance evaluation”, pp-777-789.
21. Der Chin Chen, Biometric Systems, Design and Applications, 2011, “Portable Biometric System of High Sensitivity Absorption Detection”.
22. Subra Mazumdar, Venkata Dhulipala, San Diego, “Biometric Security Using Finger Print Recognition”.
23. S.M. Shamsheer Daula, Dr. K.E. Sreenivasa Murthy, International Journal of Advanced and Innovative Research, Volume 1, Issue 2, July 2012, “An Embedded ATM Security Design Using ARM Processor with Fingerprint recognition and GSM”.
24. Steve Furber, ARM System-on-Chip Architecture, Second Edition, 2000, ISBN 0-201-67519-6.
25. Anil K. Jain, Jianjiang Feng, Karthik Nandakumar, IEEE Computer Society 2010, 0018-962/10, “Fingerprint Matching”, pp-36-44.

AUTHORS PROFILE

Manjari Jain will be receiving her B. Tech (Electronics and Communication Engineering) from VIT Vellore, in 2020. She maintains the CGPA of 9.13. She was awarded a scholarship from VIT, for her excellent academic performance. She performed many research projects in Communication and Signal Processing, during her B. Tech. She has the experience of creating URLs and APIs using Node Js technology. The deployment of the website was supervised by her.

Sagar is pursuing his B. Tech (Electronics and Communication) degree from VIT. He was also a member of Team Celerity, where he participated in ESVC 2018 (Asia’s Largest Electric Solar Vehicle Championship) and secured Rank 4 globally. VIT appreciates his talents by accommodating him with the "Achiever" award. He had worked on Python, GUI, Arduino, Fingerprint Sensor & Mongo DB.

Saravanan K received MTech Degree in Electronics and Communication Engineering from Pondicherry Engineering College and Ph.D. from Anna University, Chennai. He is currently working as a Professor in the Department of Communication Engineering, VIT, Vellore. He published 12 papers in various National and International journals. His research interests are Wireless. Networks, Network Security, Device to Device communication, and 5G.