A

Major Project

On

SMART ATM PIN RECOVERY SYSTEM USING FINGERPRINT IDENTIFICATION

Submitted to

Jawaharlal Nehru Technological University, Hyderabad

In Partial fulfillment of the requirements for the award of Degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

by

S.SRUTHI	**(187R1A05N6)**
D.HEMA PRASAD	**(187R1A05K1)**
G.DEEPAK JOY	**(197R5A0522)**

Under the esteemed guidance of

MR. SRINU VANDHANAPU
(Assistant Professor)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CMR TECHNICAL CAMPUS

UGC AUTONOMOUS

(Accredited by NAAC, NBA, Permanently Affiliated to JNTUH, Approved by AICTE, New Delhi)
Recognized Under Section 2(f) & 12(B) of the UGCAct.1956, Kandlakoya
(V), Medchal Road, Hyderabad-501401.

2018-22

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project entitled **“Smart ATM Pin Recovery System Using Fingerprint Identification”** being submitted by **S.Sruthi (187R1A05N6), D.Hema Prasad (187R1A05K1) & G.Deepak Joy (197R5A0522)** in partial fulfillment of the requirements for the award of the degree of B.Tech in Computer Science and Engineering to the Jawaharlal Nehru Technological University Hyderabad, is a record of bonafide work carried out by them under our guidance and supervision during the year 2021-22.

The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

Mr. Srinu Vandhanapu
Assistant Professor
INTERNAL GUIDE

Dr. A. Raji Reddy
DIRECTOR

Dr. K. Srujan Raju
HoD

EXTERNAL EXAMINER

Submitted for viva voice Examination held on _________________

ACKNOWLEDGEMENT

Apart from the efforts of us, the success of any project depends largely on the encouragement and guidelines of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project.

We take this opportunity to express my profound gratitude and deep regard to my guide **Mr. Srinu Vandhanapu,** Assistant Professor for his exemplary guidance, monitoring and constant encouragement throughout the project work.The blessing, help and guidance given by him shall carry us a long way in the journey of life on which we are about to embark. We also take this opportunity to express a deep sense of gratitude to the Project Review Committee (PRC) **Dr. M. Uday Kiran, Mr. J. Narasimha Rao, Dr. T. S. Mastan Rao, Mrs. G. Latha, Mr. A. Kiran Kumar,** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Srujan Raju,** Head, Department of Computer Science and Engineering for providing encouragement and support for completing this project successfully.

We are obliged to **Dr. A. Raji Reddy,** Director for being cooperative throughout the course of this project. We also express our sincere gratitude to Sri. **Ch. Gopal Reddy,** Chairman for providing excellent infrastructure and a nice atmosphere throughout the course of this project.

The guidance and support received from all the members of **CMR Technical Campus** who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

S.SRUTHI	**(187R1A05N6)**
D.HEMAPRASAD	**(187R1A05K1)**
G.DEEPAK JOY	**(197R5A0522)**

ABSTRACT

ATM (Automated Teller Machine) is an electronic telecommunication device that is used to perform a financial transaction without the need for a human clerk or bank teller. ATMs extend traditional banking hours by dispensing cash and making other transactions available 24 hours a day. In ATMs, the user is identified by inserting an ATM card, and authentication is provided by the customer entering a PIN. The PIN provided to the customer is compared with the recorded reference PIN in the bank server. In the existing system, the user has to insert the card and the PIN. If the PIN is correct, the system allows for the transaction. Otherwise, the system asks for the PIN again and it allows a maximum of three times to enter it. After 3 trials the ATM card will get blocked. To reactivate the card, users need to visit the bank and do the bank formalities, which is a tedious and time-consuming job. Biometrics is the science of establishing the identity of an individual based on the physical, chemical behavioral attributes of a person. The fingerprint is a pattern of ridges and valleys on the surface of a fingertip. It is used for biometric identification. Fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual. To reactivate that ATM card in the ATM center itself we are using fingerprint biometric.

LIST OF FIGURES

LIST OF SCREENSHOTS

TABLE OF CONTENTS

1.INTRODUCTION

1.INTRODUCTION

1.1 PROJECT SCOPE

The aim of our Project is to design a Smart ATM System with pin recovery and security using Fingerprint identification for users which mainly focuses on rural parts as well as all over the country. Our System has the capability to reduce the time consumption for new pin generation along with high security.It even reduces the burden for a user to go and visit the bank to unlock his/her ATM card.

1.2 PROJECT PURPOSE

The ATM security system provides a mechanism for recovery of ATM PIN by using fingerprint identification. The system is able to send an alert message to the ATM card owner for entering the wrong PIN.The developed system is able to authenticate the user based on fingerprint identification. An OTP is also sent to the owner of the card for creation of a new PIN.

1.3 PROJECT FEATURES

To help overcome the time consumption in reactivating the pin.The main reason for introducing the Biometric system is to increase the overall security.To avoid the user visiting the bank and fulfilling some of the formalities in order to unblock his/her card.

2.SYSTEM ANALYSIS

2.SYSTEM ANALYSIS

SYSTEM ANALYSIS

System Analysis is the important phase in the system development process.The System is studied to the minute details and analyzed.The system analyst plays an important role of an interrogator and dwells deep into the working of the present system. In analysis, a detailed study of these operations performed by the system and their relationships within and outside the system is done.A key question considered here is,“what must be done to solve the problem?”The system is viewed as a whole and the inputs to the system are identified. Once analysis is completed the analyst has a firm understanding of what is to be done.

2.1 PROBLEM DEFINITION

The proposed methodology is based on identification of fingerprints of the ATM user.The user inserts the ATM card and enters PIN to perform transactions.If the user enters the invalid PIN three times, an alert message will be displayed as a pop-up on the ATM machine.The pop-up window displays the message “You have entered the wrong PIN;please give your registered fingerprint to create a new PIN”.User provides the finger impression for authentication. If fingerprint matches then the bank server will provide flexibility for the user to create his/her new PIN on the ATM machine itself. After that user will get a message that you have successfully got a new PIN. Now users can continue transactions with this new PIN as earlier.

2.2 EXISTING SYSTEM

In the existing system, the user has to insert the card and the PIN number. If the PIN is correct, the system allows for the transaction. Otherwise, the system asks for the PIN again and it allows a maximum of three times to enter it. After 3 trials the ATM card will get blocked. To reactivate the card user needs to visit the bank and do the bank formalities, which is a tedious and time consuming job.

2.2.1 LIMITATIONS OF EXISTING SYSTEM

- The user needs to visit the bank and do the formalities to reactivate the ATM card.
- If the user fails to provide the correct pin after three attempts the card will be blocked.
- Lack of availability and continuity of services.
- The system cannot reactivate the card.
- The ATM system does not contain the biometric system.

2.3 PROPOSED SYSTEM

The proposed ATM security system provides a mechanism for recovery of ATM PIN by using fingerprint identification. The developed system is able to authenticate the user based on fingerprint identification. The system is able to send an alert message to the ATM card owner for entering the wrong PIN. The alert message is also sent to the owner of the card upon successful creation of a new PIN. From the tests carried out we have been able to prove that the biometric identification for ATM transactions can be practically implemented in a real time environment. The developed system provides ATM users with the facility to change the PIN in the ATM machine itself.

2.3.1 ADVANTAGES OF THE PROPOSED SYSTEM

- The main reason for introducing the Biometric system is to increase the overall security.
- To avoid the user visiting the bank.
- To reactivate the ATM pin anytime and anywhere of the ATM center.
- Less time consuming.
- The system is suitable for emergency situations.

2.4 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and the business proposal is put forth with a very general plan for the project and some cost estimates.During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the user.

Three key considerations involved in the feasibility analysis are

- Economic Feasibility
- Technical Feasibility
- Social Feasibility

2.4.1 ECONOMIC FEASIBILITY

The developing system must be justified by cost and benefit. Criteria to ensure that effort is concentrated on a project, which will give best, return at the earliest. One of the factors, which affect the development of a new system, is the cost it would require.

The following are some of the important financial questions asked during preliminary investigation:

- The costs conduct a full system investigation.
- The cost of the hardware and software.
- The benefits in the form of reduced costs or fewer costly errors.

Since the system is developed as part of project work, there is no manual cost to spend for the proposed system. Also all the resources are already available, it gives an indication that the system is economically possible for development.

2.4.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources.The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

2.4.3 BEHAVIORAL FEASIBILITY

This includes the following questions:

- Is there sufficient support for the users?
- Will the proposed system cause harm?

The project would be beneficial because it satisfies the objectives when developed and installed.All behavioral aspects are considered carefully and conclude that the project is behaviorally feasible.

2.5 HARDWARE & SOFTWARE REQUIREMENTS

2.5.1 HARDWARE REQUIREMENTS:

Hardware interfaces specify the logical characteristics of each interface between the software product and the hardware components of the system.The following are some hardware requirements.

● Processor	:	Intel core i5,64 bit
● Input Devices	:	Fingerprint scanner along with a cable,NODEMCU ESP32,RFID-Reader Module,GSM Module,Buzzer
● RAM	:	4GB and Above.

2.5.2 SOFTWARE REQUIREMENTS:

Software Requirements specifies the logical characteristics of each interface and software components of the system.The following are some software requirements.

● Operating System	:	Windows 7 and Above
● Language	:	Python IDLE 3.10.1 version
● Software	:	Arduino 1.8.19 version
● Database	:	Json.txt

3.ARCHITECTURE

3.ARCHITECTURE

3.1 PROJECT ARCHITECTURE

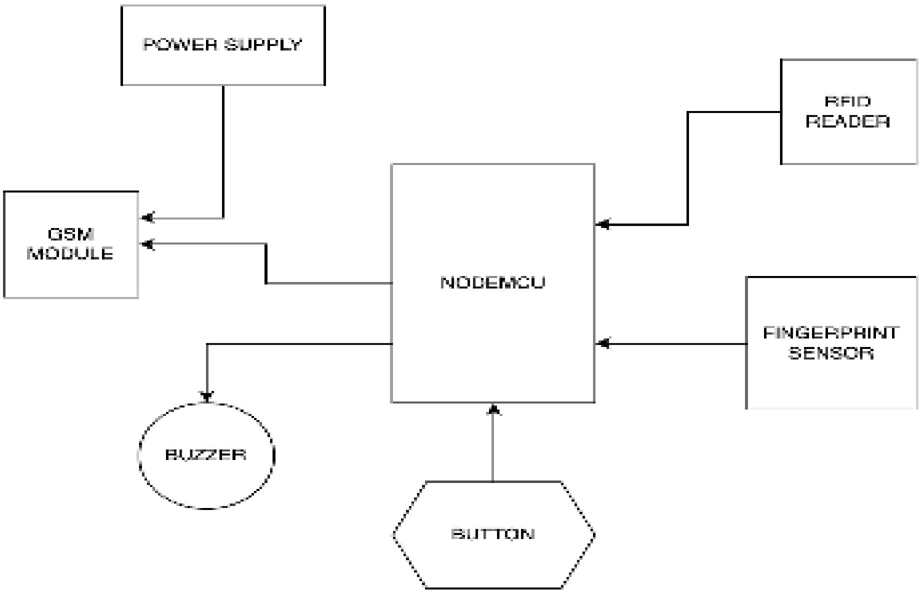


Fig 3.1 Project Architecture

3.2 DESCRIPTION

NODEMCU ESP32 : ESP32 is a series of low-cost, low-power system on chip microcontrollers with integrated Wi-Fi and dual-mode Bluetooth.

RFID Reader : The module can support I2C, SPI and UART and normally is shipped with a RFID card and key fob. It is commonly used in attendance systems and other person/object identification applications.

Fingerprint Sensor : There are many kinds of fingerprint modules.They are optical, capacitive, piezoresistive, ultrasonic, piezoelectric, RF, thermal, etc. An optical fingerprint sensor is used in this system. This sensor reads the fingerprint pattern. The scan image is converted as a template and saved in memory.

Buzzer : Buzzer is a small yet efficient component to add sound features to our project/system. It is very small and compact 2-pin structure hence can be easily used on breadboard, Perf Board and even on PCBs which makes this a widely used component in most electronic applications.

GSM Module : A GSM module is a chip or circuit that will be used to establish communication between a mobile device or a computing machine and a GSM.GSM module is a hardware device that uses GSM mobile telephone technology to provide a data link to a remote network.

Button : The user can assign actions to a button press and release, and assign a separate action when the button is held down.

3.3 USE CASE DIAGRAM

In the use case diagram we have basically one actor i.e, the user. The user has the rights to import Package, upload dataset, train system and predict result.

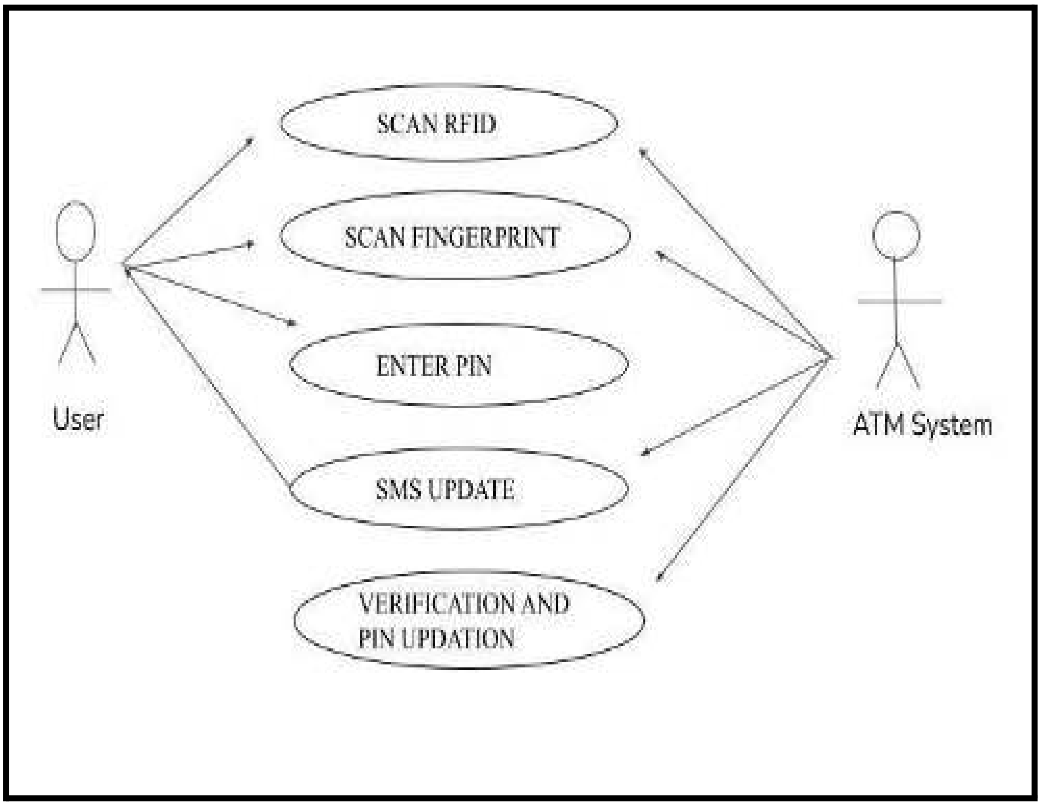


Figure 3.3: Use Case Diagram

3.4 CLASS DIAGRAM

Class Diagram is a collection of classes and objects.

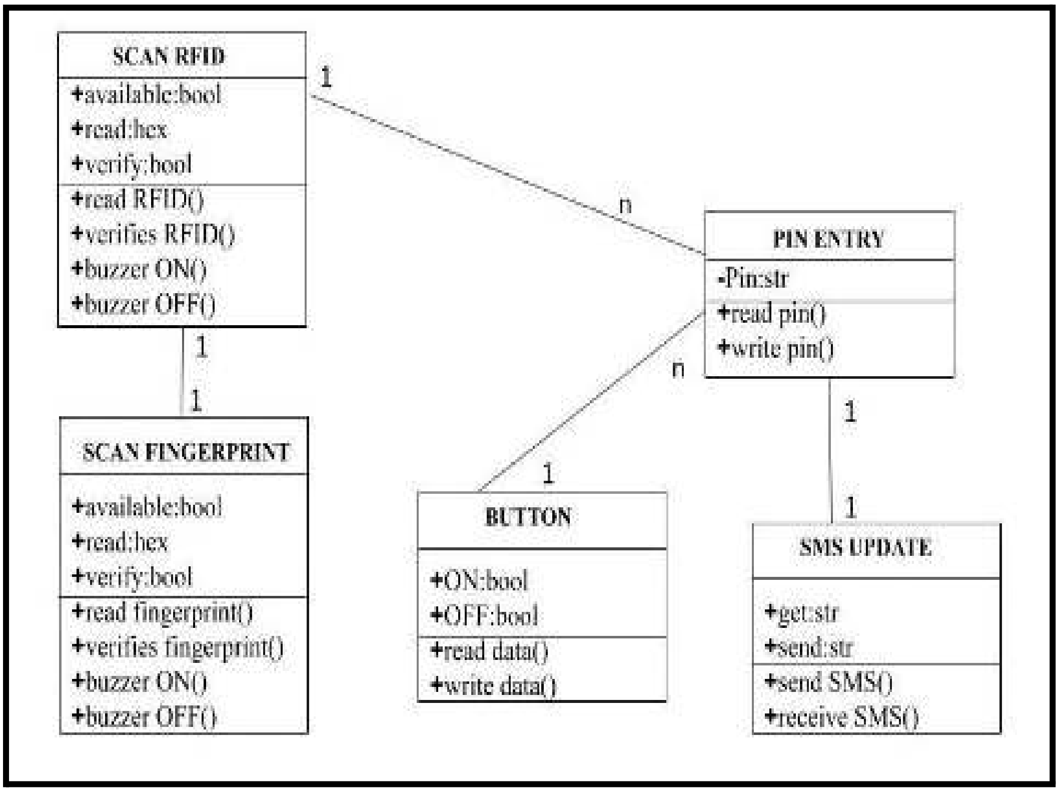


Figure 3.4: Class Diagram

3.5 SEQUENCE DIAGRAM

The sequence diagram shows the sequence in which different tasks are being carried out by the actors.

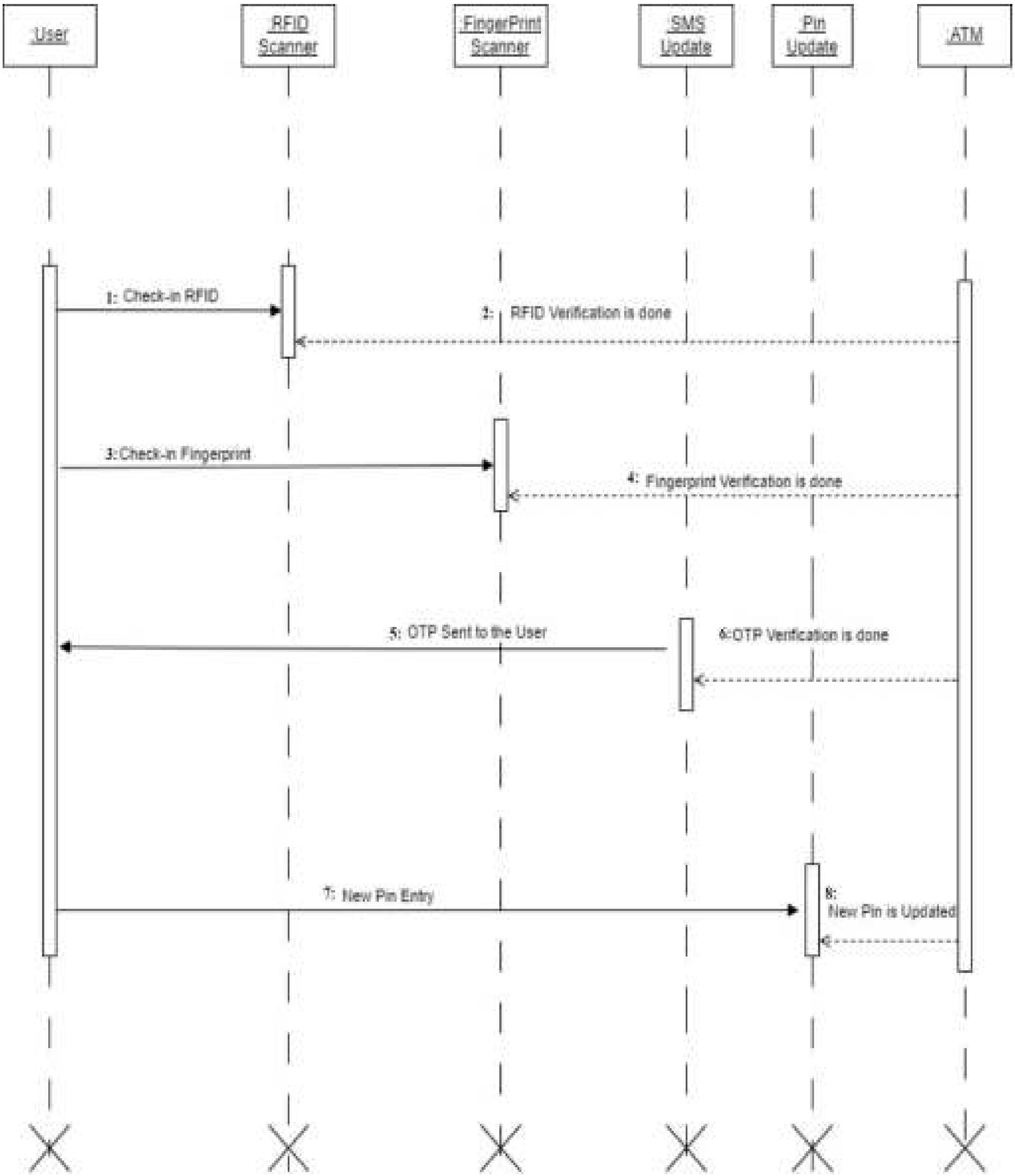


Figure 3.5: Sequence Diagram

3.6 ACTIVITY DIAGRAM

It describes the flow of activity states.

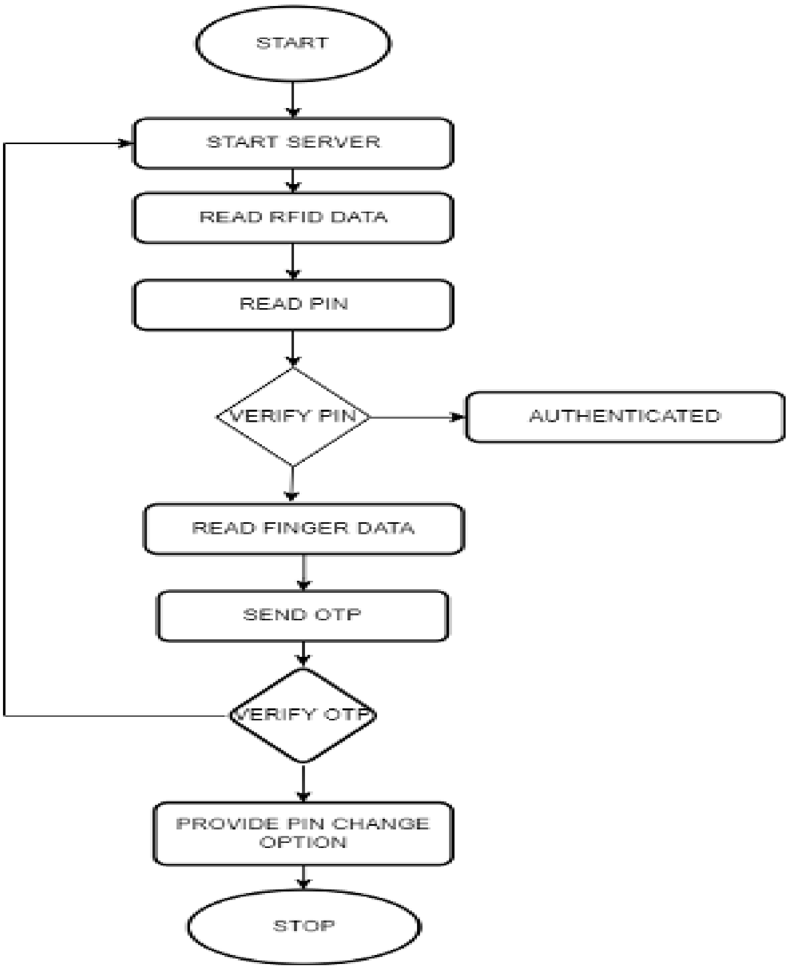


Figure 3.6: Activity Diagram

4.IMPLEMENTATION

4. IMPLEMENTATION

4.1 SAMPLE CODE

```
from flask import Flask,render_template,request
import random
import serial
import threading
import json
import time
st = 0
otpValue = 0
id = 0
com = 0
ser = 0
pin_count = 0
f = open("db.json")
dct = json.load(f)
print(dct)
f.close()
for i in range(0,256):
    try:
        ser = serial.Serial('COM'+str(i),9600,timeout=2)
        print('COM'+str(i))
        com = 'COM'+str(i)
    except :
        pass
        #print("Connect the device")
print(com)
def getCard():
    global ser
    ser.write(b"getcardid")
    r = 0
    while 1:
        r = ser.readline()
        try:
            if len(r) > 0 :
                r = r.decode('utf-8')
                print(r)
                if 'CardId :' in r:
                    r = r.split("CardId :")[1].split(",")[0]
                    print(r)
```

```
break
except:
print("Error card")
pass
return r
def getindex():
   global ser
   ser.write(b"getfingerindex")
   r = 0
   while 1:
      r = ser.readline()
      try:
         if len(r) > 0:
            r = int(r.decode('utf-8').split(":")[1])
            print(r)
            break
      except:
         print("Error card")
         pass
   return r
def getsendSMS(otpnum,mobile):
   global ser
   otpnum =
f"otp:{otpnum},mobile:{mobile};".encode("utf-8")#otp:1234,mobile:7095797212;
   #otp:1234,mobile:1234567890;
   print("sending : ",otpnum)
   ser.write(otpnum)
   r = 0
   while 1:
      r = ser.readline()
      if len(r) > 0 :
         print(r)
         break
   return r.decode('utf-8')
def load(pinValue):
   global id
   print(id)
   f = open("db.json")
   dct = json.load(f)
   dct[id]["pin"] = pinValue
   print(dct)
   f.close()
   with open('db.json', 'w') as json_file:
      json.dump(dct, json_file)
```

```
def get_w():
global ser
    global st
    global otpValue
    global id
    global dct
    while 1:
        if st ==1:
id = getCard()
 print(dct)
  if(id in dct.keys()):
                st = 2
        continue
         st = 2
         index = getindex()
         print(index, dct[id])
         if dct[id]["index"] == index:
         print("Authenticated")
         st = 3
         otpValue = random.randint(1000,9999)
          print("OTP : ",otpValue)
          getsendSMS(otpValue)
                else:st = 0
        elif st == 3:
            index = getindex()
            print(index, dct[id])
            if dct[id]["index"] == index:
                print("Authenticated")
                st = 4
                otpValue = random.randint(1000,9999)
                print("OTP : ",otpValue)
                getsendSMS(otpValue,dct[id]["mobile"])
            else:st = 5
        else:pass
app = Flask(__name__)
@app.route('/',methods=["get","post"])
def home():
    global st
    if request.method=="GET":
        st = 1
        return render_template('home.html')
    if request.method=="POST":
            return {"data":st}
@app.route('/check',methods=["get","post"])
```

```
def checkFinger():
global st
if request.method=="GET":
        st = 3
        return render_template('check.html')
    if request.method=="POST":
            return {"data":st}
@app.route('/checkpin',methods=["get","post"])
def checkpin():
    global st
    global dct
    global id
    global pin_count
if request.method=="GET":
        pin_count = 0
        return render_template('checkPin.html')
  if request.method=="POST":
        if st == 2:
pin_count +=1
    print(dct[id]['pin'],int(request.data.decode("utf-8")))
            if(dct[id]['pin'] == request.data.decode("utf-8")):return {"data":4}
            if pin_count ==4:return {"data":5}
            return {"data":pin_count}
        return {"data":0}
@app.route('/otp',methods=["get","post"])
def otp():
    global st
    global otpValue
    if request.method=="GET":
        st = 0
        return render_template('otpcheck.html')
    if request.method=="POST":
        try:
            otp = int(request.data.decode("utf-8"))
            print('Got OTP :',otp)
            print("Generated OTP :",otpValue)
            if otp == otpValue:return {"data":1}
            else :return {"data":0}
        except Exception as e:
            print(e)
            return {"data":0}
    return ""
@app.route('/change',methods=["get","post"])
def change():
 global dct
    global random_value
    if request.method=="GET":
        return render_template('change.html')
    if request.method=="POST":
        try:
            pin = request.data.decode("utf-8")
            print('Got pin :',pin)
            pin = pin.split(",")[0]
            load(pin)
            f = open("db.json")
            dct = json.load(f)
            print(dct)
            f.close()
       except Exception as e:
print(e)
    return ""
kwargs = {'host': '0.0.0.0', 'port': 8080, 'threaded': True, 'use_reloader': False, 'debug': True}
if __name__ == '__main__':
    threading.Thread(target=get_w).start()
    threading.Thread(target=app.run, daemon=True, kwargs=kwargs).start()
```

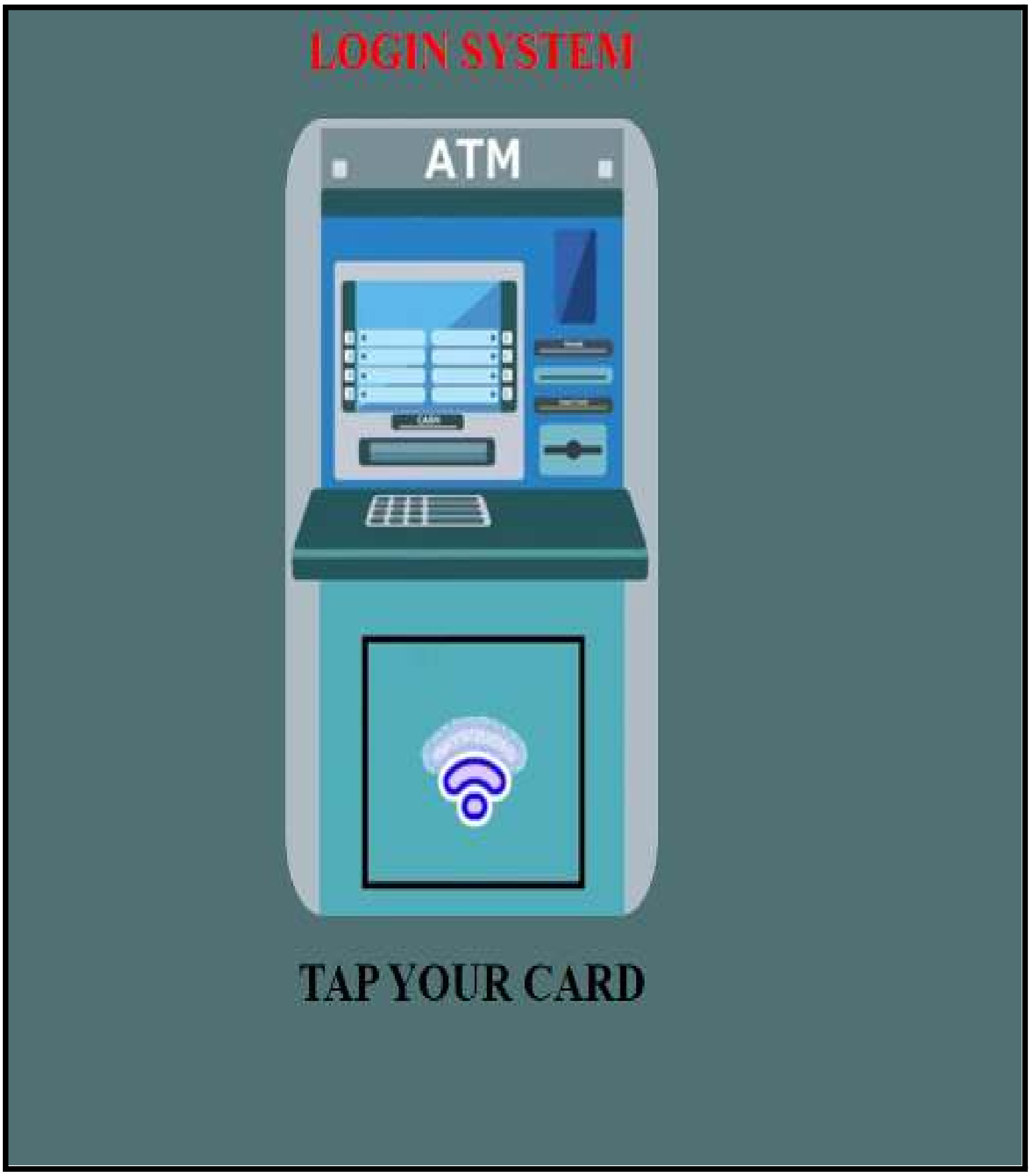
Source code Drive link :
https://docs.google.com/document/d/1rX3WpEADg8UeXcwhnRYbCFLKI0IKh96aVALMEX4dKPE/edit?usp=sharing

5.RESULTS

5.1 SCREENSHOTS

5.1.1 HOME PAGE RESULT

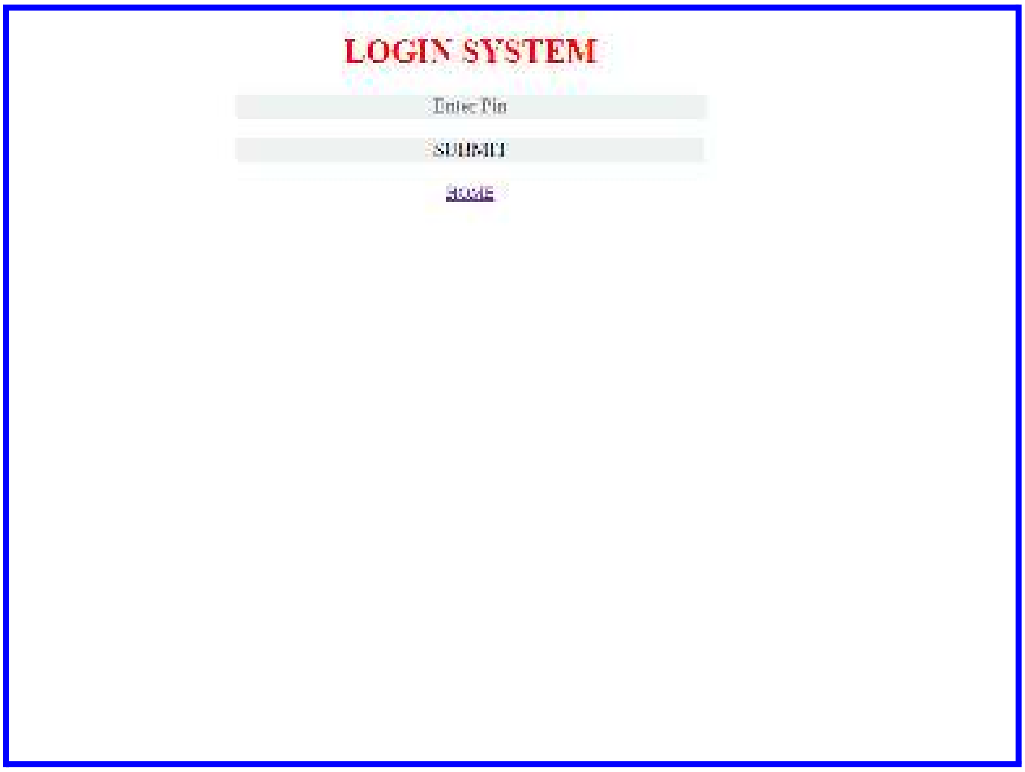
The Homepage displays an ATM machine wherein the user can scan his/her card.



Screenshot 5.1.1: Home Page Result

5.1.2 PIN ENTRY

The Login Page is where the user enters his/her pin number in the system to perform transactions.



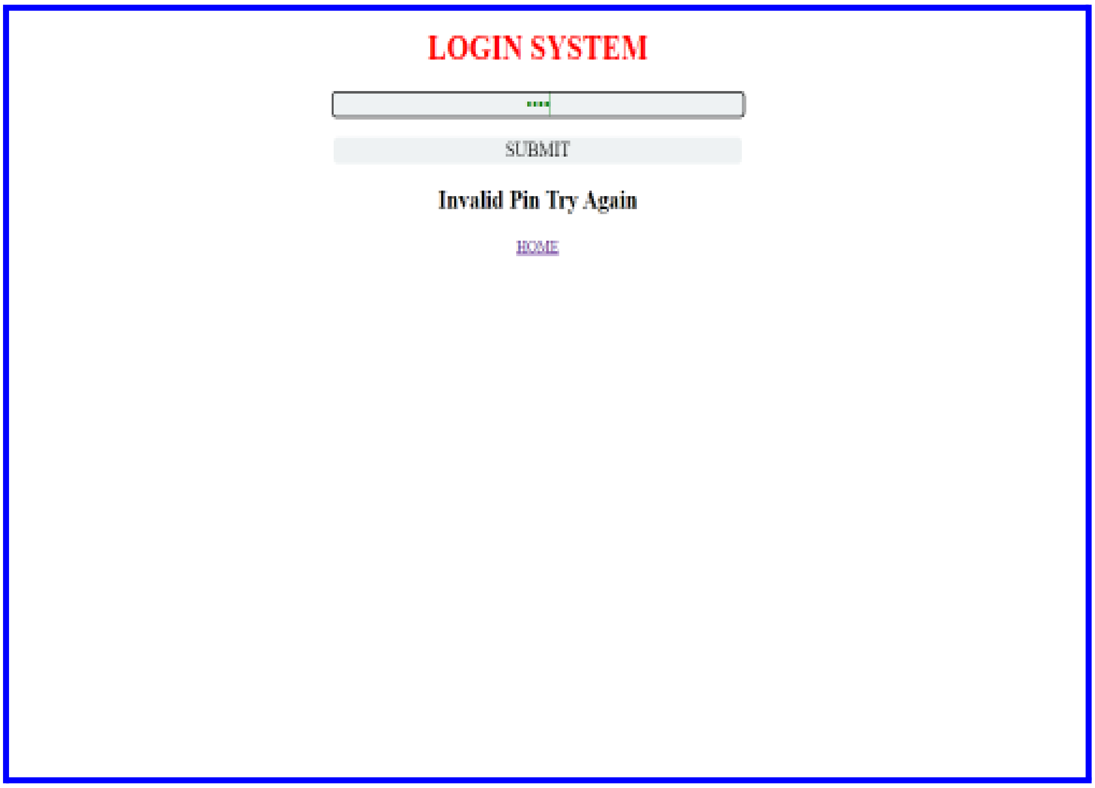
LOGIN SYSTEM

Enter Pin

Screenshot 5.1.2: PIN Entry Result

5.1.3 INVALID PIN ENTRY

The Page where the user enters a wrong/invalid pin number in the system.

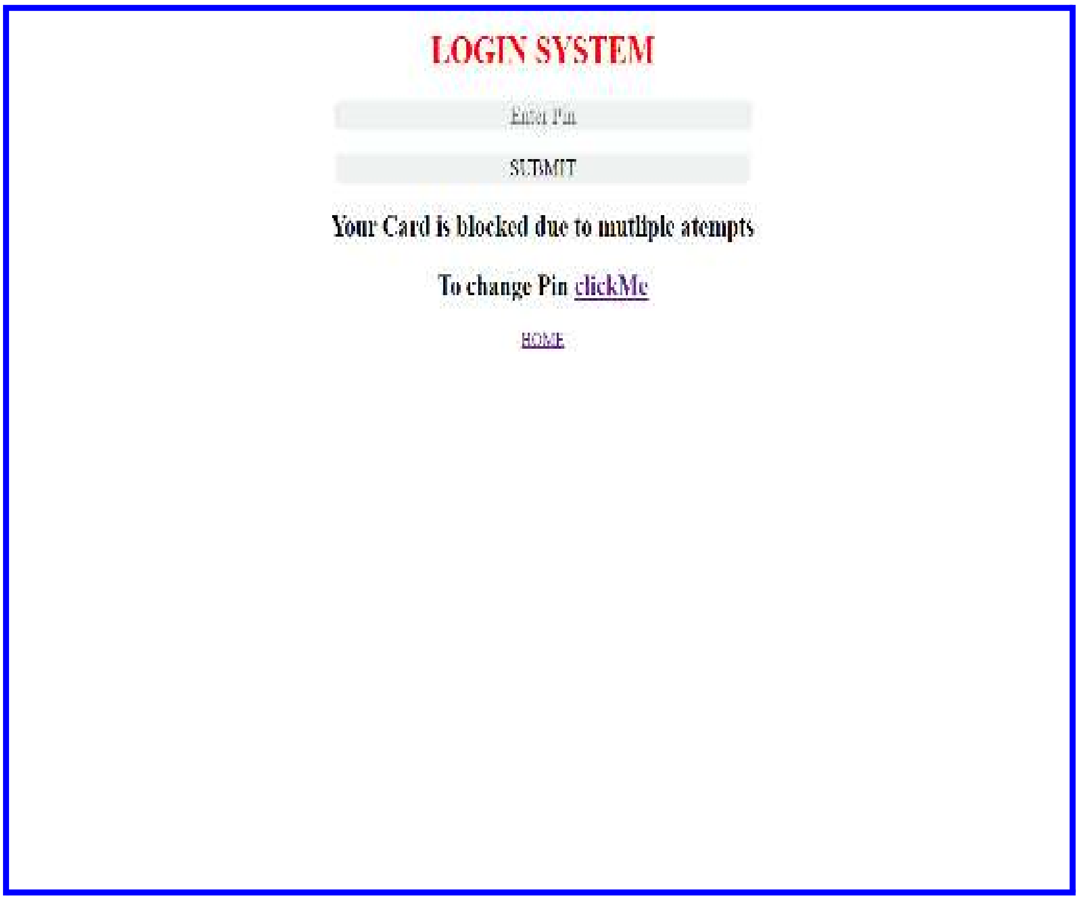


Invalid Pin Try Again

Screenshot 5.1.3: Invalid PIN Entry Result

5.1.4 PIN CHANGE

This page shows that the user's his/her card is blocked for entering the pin number more than three times.



LOGIN SYSTEM

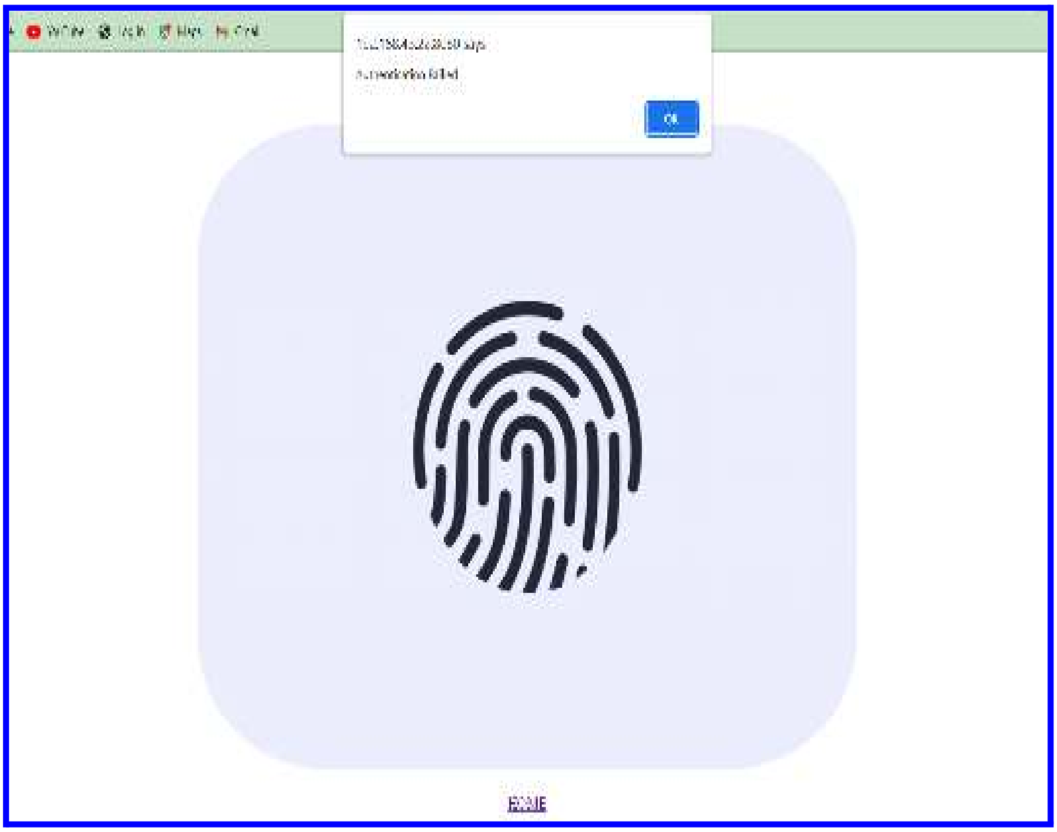
Your Card is blocked due to mutliple atempts

To change Pin clickMe

Screenshot 5.1.4: Pin Change Result

5.1.5 FINGERPRINT AUTHENTICATION RESULT

Here in the page the user scans his/her finger for verification.If his/her finger matches with the data present in the card then the authentication is completed and moves to the next step otherwise the authentication is failed.

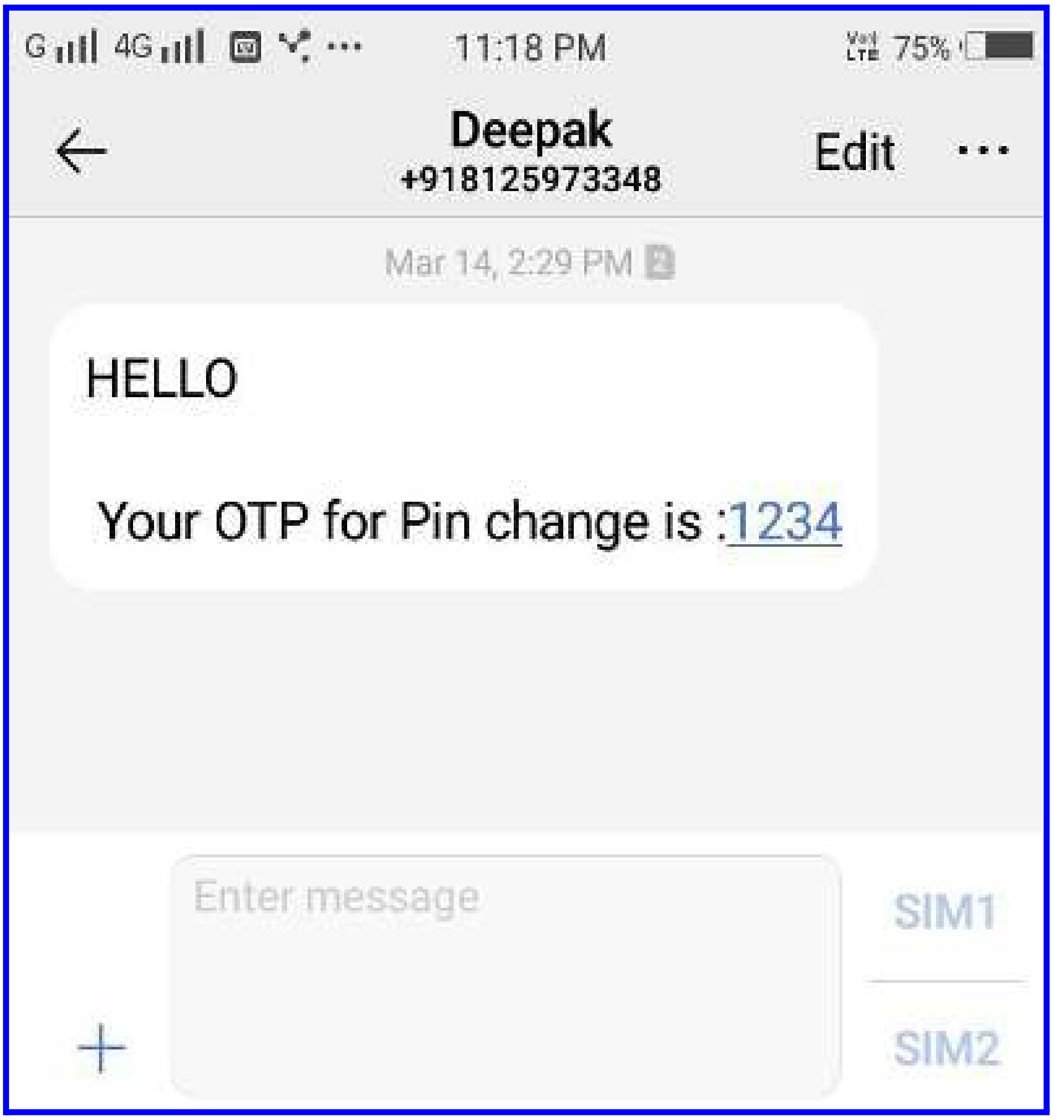


Authentication failed

Screenshot 5.1.5: Fingerprint Authentication Result

5.1.6 OTP MESSAGE RESULT

This is the message sent to the user’s registered mobile number from the system.



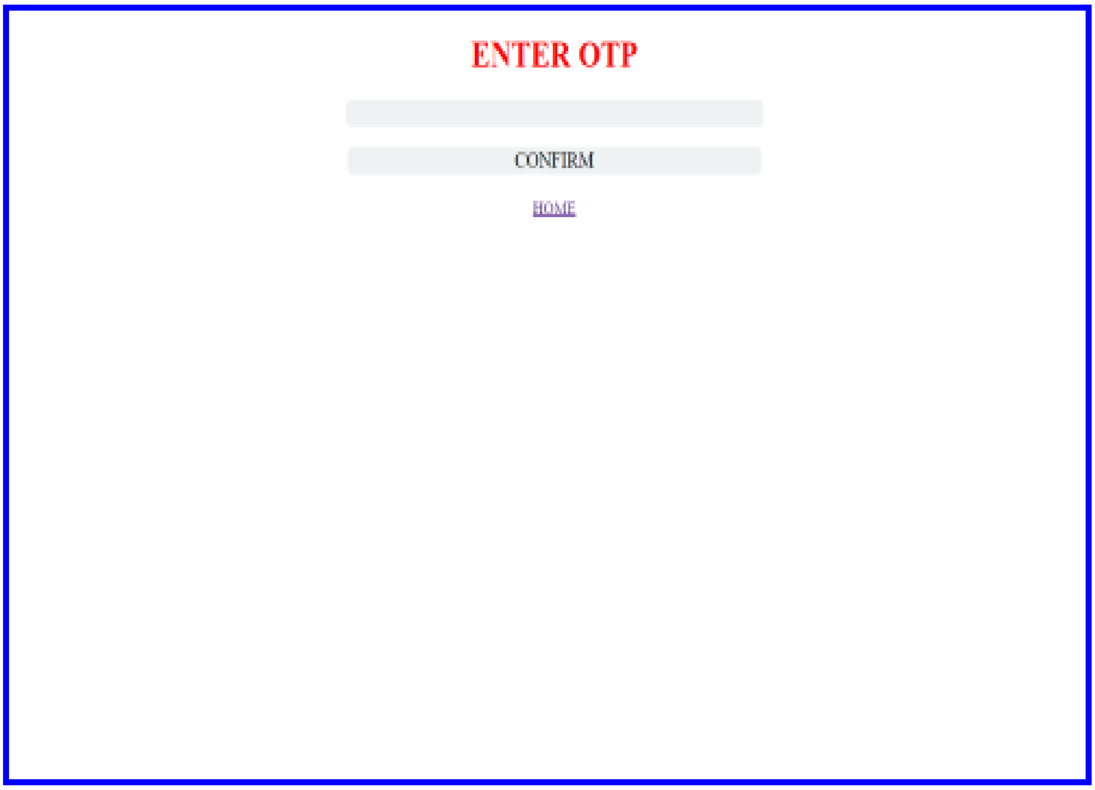
HELLO

Your OTP for Pin change is :1234

Screenshot 5.1.6: OTP Message Result

5.1.7 OTP VERIFICATION

The system sends an OTP to the user's registered mobile number.Here in this page the user enters the OTP that he received from the system.After the OTP verification is completed it moves to the next page.

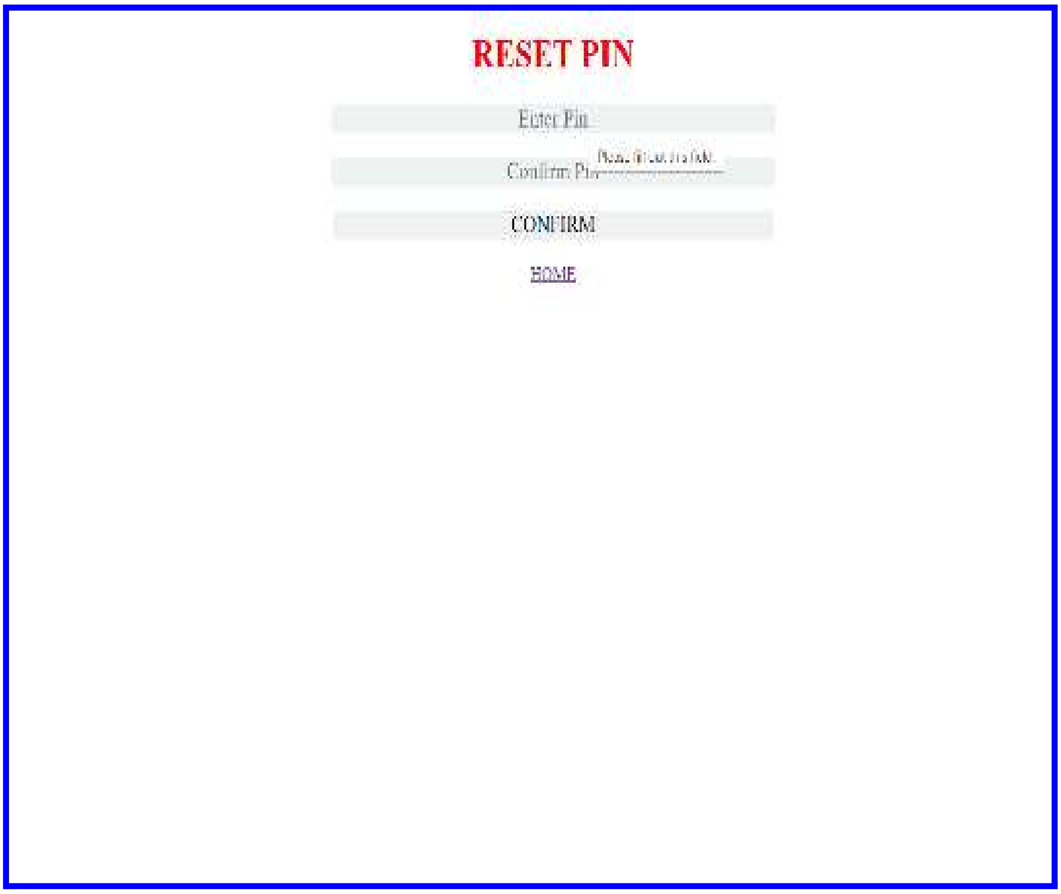


ENTER OTP

Screenshot 5.1.7: OTP Verification Result

5.1.8 RESET PIN RESULT

This is where the user can reset his/her pin number.The ATM System will update this pin number to his/her card.From then the user can continue his/her transactions

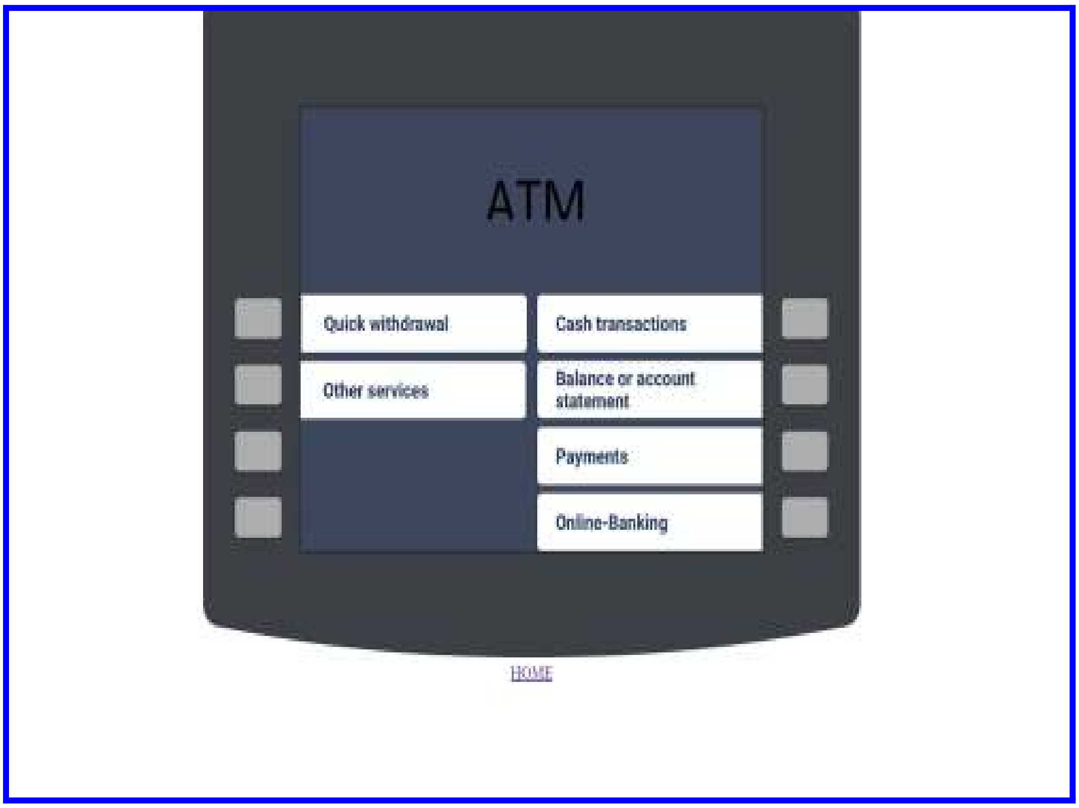


Please fill out this field.

Screenshot 5.1.8: Reset Pin Result

5.1.9: TRANSACTION PAGE RESULT

The Page where the user can perform his/her transactions in the system.



Screenshot 5.1.9: Transaction Page Result

6.TESTING

6. TESTING

6.1 INTRODUCTION TO TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product.It provides a way to check the functionality of components, subassemblies, assemblies and/or a finished product.It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner.There are various types of test.Each test type addresses a specific testing requirement.

6.2 TYPES OF TESTING

6.2.1 UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs.All decision branches and internal code flow should be validated.It is the testing of individual software units of the application.It is done after the completion of an individual unit before integration.This is a structural testing,that relies on knowledge of its construction and is invasive.Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration.Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

6.2.2 INTEGRATION TESTING

Integration tests are designed to test integrated software components to determine if they actually run as one program.Testing is event driven and is more concerned with the basic outcome of screens or fields.Integration tests demonstrate that although the components were individually satisfaction,as shown by successfully unit testing,the combination of components is correct and consistent.Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

6.2.3 FUNCTIONAL TESTING

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases.In addition, systematic coverage pertaining to identifying Business process flows; data fields, predefined processes.

6.3 TEST CASES

6.3.1 PIN RECOVERY

Test case ID	Test case name	Purpose	Test Case	Output
1	System reads the pin	Use it for detection	The pin value does match with the card.	Moves to transaction page
2	System reads the pin	Use it for detection	The pin value does not match with the card.	Moves to fingerprint page

6.3.2 PIN SECURITY

Test case ID	Test case name	Purpose	Input	Output
1	System reads the fingerprint	Use it for security	The fingerprint matches with the card	Moves to OTP verification page
2	Server reads the OTP	Use it for security	The OTP verification is done	Moves to new pin generation page
3	System reads new pin	Use it for security	The new pin and confirm pin must be same	New pin is generated

7.CONCLUSION

7.CONCLUSION & FUTURE SCOPE

7.1 PROJECT CONCLUSION

The proposed ATM security system provides a mechanism for recovery of ATM PIN by using fingerprint identification. The developed system is able to authenticate the user based on fingerprint identification. The system is able to send an alert message to the ATM card owner for entering the wrong PIN. The alert message is also sent to the owner of the card upon successful creation of a new PIN. From the tests carried out we have been able to prove that the biometric identification for ATM transactions can be practically implemented in a real time environment. The developed system provides ATM users with the facility to change the PIN in the ATM machine itself.

7.2 FUTURE SCOPE

This system can be directly connected to the ATM systems in realtime to make it easier for the user.In the future we can even replace fingerprints with the pin to improve security and reduce card fraud detection.Even the ATM system can be made into Wi-Fi Enabled.

8.BIBLIOGRAPHY

8.BIBLIOGRAPHY

8.1 REFERENCES

1. Alhassan M.E,Ganiyur S.O,Muhammad-Bello B.L," An enhanced ATM security system using second level authentication",International journal of computer application(0975-8887),vol 111-no 5,feb 2015.

2. A.Gera,N.sethi, "A revived survey of various credit card fraud detection techniques," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 780 – 791, April 2014.

3. G. Stanley, "Card-less financial transaction," Apr. 21 2014, US Patent App. 14/257,588.

4. Fingershield ATM – ATM Security System using Fingerprint Authentication, Christiawan; Bayu Aji Sahar; Azel Fayyad Rahardian; Elvayandri Muchtar 2018 International Symposium on Electronics and Smart Devices (ISESD).

5. Securing ATM pins and passwords using Fingerprint based Fuzzy Vault System, Sweedle Machado; Prajyoti D'silva; Snehal D'mello; Supriya Solaskar; Priya Chaudhari 2018 Fourth International Conference on Computing Communication Control and Automation.

6.A.K. Ojha, "ATM Security using Fingerprint Recognition", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5, No. 6, pp. 170- 175, 2015.

7. R. Banu Priya, P. Kavitha, T. Ashok, N. Logesh Kumar and M. Chandrasekar, "Smart ATM Access and Security System using RFID and GSM Technology", International Journal of Scientific Research and Education, Vol. 2, No. 5, pp. 446- 453, 2013. 0 10 20 30 40 50 60 Successful Attempts Biometrics ISSN: 2395-1680 (ONLINE) ICTACT JOURNAL ON MICROELECTRONICS, JULY 2018, VOLUME: 04, ISSUE: 02 575

8. G. Eason, B. Noble and I.N. Sneddon, "On Certain Integrals of Lipschitz-Hankel Type Involving Products of Bessel Functions", Philosophical Transactions of the Royal Society A, Vol. A247, pp. 529-551, 1955.

9. G. Sambasiva Rao, C. Naga Raju, L.S.S. Reddy and E.V. Prasad, "A Novel Fingerprints Identification System Based on the Edge Detection", International Journal of Computer Science and Network Security, Vol. 8, No. 12, pp. 394-397, 2008.

10. M.R. Girgis, A.A. Sewisy and R. F. Mansour, "Employing Generic Algorithms for Precise Fingerprint Matching based on Line Extraction", Graphics, Vision and Image Processing Journal, Vol. 7, No. 1, pp. 51-59, 2007.

11. Duresuoquian Miao, Qingshi Tang and Wenjie Fu, “Fingerprint Minutiae Extraction Based on Principal Curves”, Pattern Recognition Letters, Vol. 28, pp. 2184- 2189, 2007.

12. Pranali Ravikant Hatwar and Ravikant B Hatwar, “BioSignal based Biometrics Practices”, International Journal of Creative Research Thoughts, Vol. 1, No. 4, pp. 1-9, 2013.

13. Edmund Spinella, “Biometric Scanning Technologies: Finger, Facial and Retinal Scanning”, Available at: https://www.sans.org/readingroom/whitepapers/authentication/biometric-scanningtechnologies-finger-facial-retinal-scanning-1177.

14. J. Swann, “Teaching Ethics: It's the Right Thing to Do”, Available at: https://www.informs.org/ORMSToday/Archived-Issues/2004/orms-6-04/Teaching-EthicsIt-s-the-Right-Thing-to-Do.

15. O.W. Fatai, J.B. Awotunde and O.E. Matluko, “A Novel System of Fingerprint Recognition Approach for Immigration Control”, IOSR Journal of Computer Engineering, Vol. 16, No. 3, pp. 39-42, 2014.

16. N. Selvaraj and G. Sekar, “A Method to Improve the Security Level of ATM Banking Systems using AES Algorithm”, International Journal of Computer Applications, Vol. 3, No. 6, pp. 5-9, 2010.

17. T.C. Glaessner, T. Kellermann and V. McNevin, “Electronic Security: Risk Mitigation in Financial Transactions: Public Policy Issues”, Working Paper, World Bank Publications, pp. 3-5, 2002.

18. W.W.N. Wan, C.L. Luk and C.C. Chow, “Customers Adoption of Banking Channels”, International Journal of Bank Marketing, Vol. 23, No. 3, pp. 255-272, 2005. [14] B. Richard and M. Alemayehu, “Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons”, Journal of Internet Banking and Commerce, Vol. 11, No. 2, pp. 1-6, 2006.

19. N.K. Ratha, J.H. Connell and R.M. Bolle, “Enhancing Security and Privacy in Biometrics-based Authentication Systems”, IBM Systems Journal, Vol. 40, No. 3, pp. 614-634, 2001.

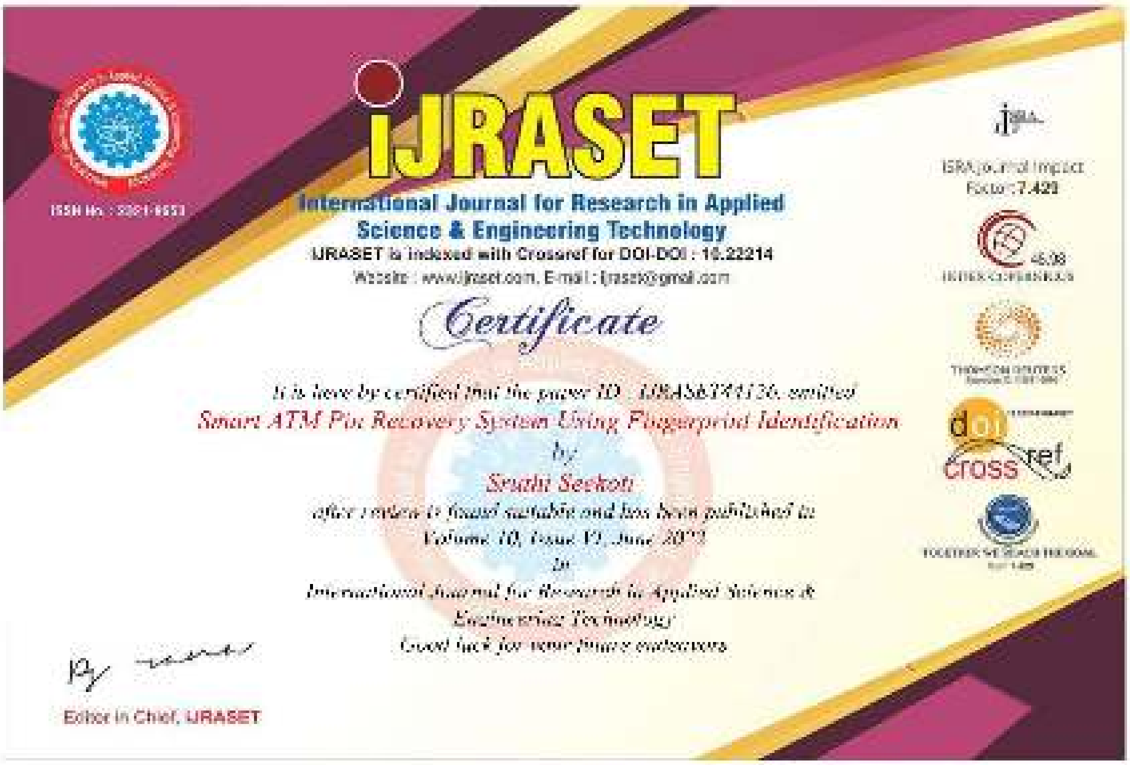
20.J. Yang, N. Xiong, A.V. Vasilakos, Z. Fang, D. Park, X. Xu, S. Yoon, S. Xie and Y. Yang, “A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications”, IEEE Systems Journal, Vol. 5, No. 4, pp. 574-583, 2011.

8.2 WEBSITES

1. www.seminarsonly.com
2. www.geeksforgeeks.org

8.3 GITHUB LINK

https://github.com/sruthisree1830/Smart-ATM-Pin-Recovery-System-Using-FingerPrint-Identification-I.git



ISSN No. : 2321-9653

iJRASET

International Journal for Research in Applied Science & Engineering Technology

IJRASET is indexed with Crossref for DOI-DOI : 10.22214

Website : www.ijraset.com, E-mail : ijraset@gmail.com

ISRA Journal Impact Factor: 7.429

45.98 INDEX COPERNICUS

THOMSON REUTERS

doi crossref

TOGETHER WE REACH THE GOAL

Certificate

It is here by certified that the paper ID : IJRASET44126, entitled

Smart ATM Pin Recovery System Using Fingerprint Identification

by

Sruthi Seekoti

after review is found suitable and has been published in

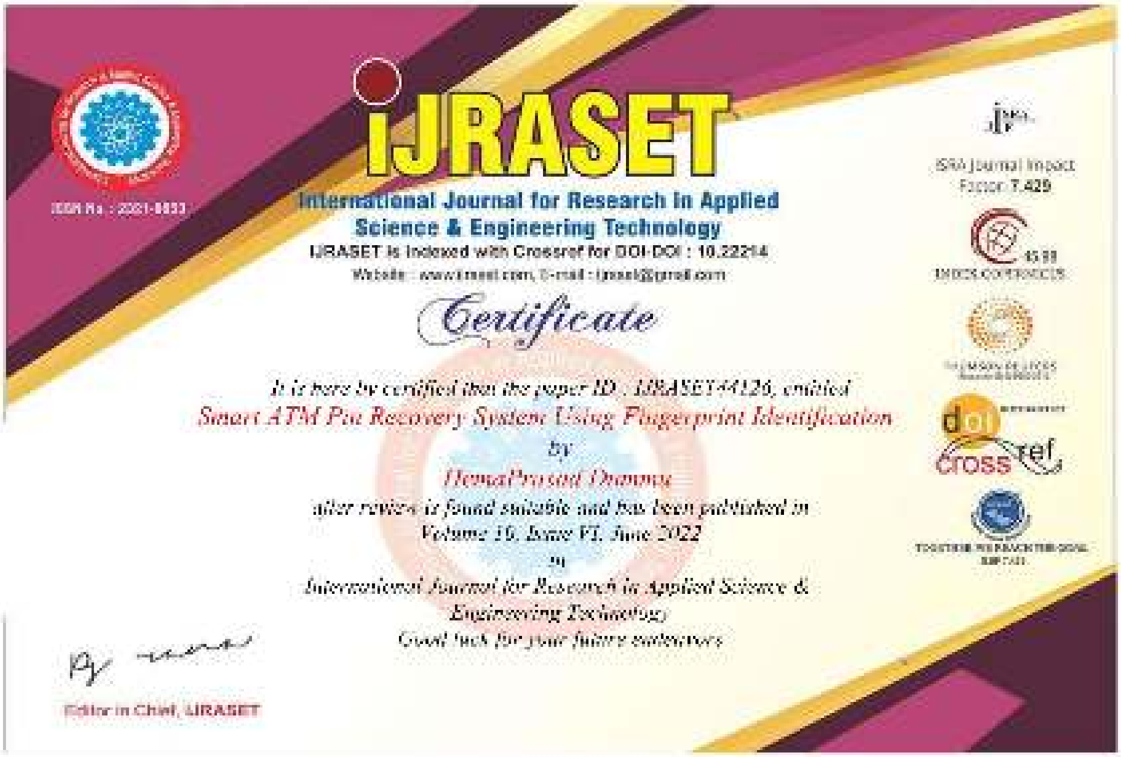
Volume 10, Issue VI, June 2022

in

International Journal for Research in Applied Science & Engineering Technology

Good luck for your future endeavors

Editor in Chief, IJRASET



ISSN No. : 2321-9653

iJRASET

International Journal for Research in Applied Science & Engineering Technology

IJRASET is indexed with Crossref for DOI-DOI : 10.22214

Website : www.ijraset.com, E-mail : ijraset@gmail.com

ISRA Journal Impact Factor: 7.429

45.98 INDEX COPERNICUS

THOMSON REUTERS

doi crossref

TOGETHER WE REACH THE GOAL

Certificate

It is here by certified that the paper ID : IJRASET44126, entitled

Smart ATM Pin Recovery System Using Fingerprint Identification

by

HemaPrasad Dummu

after review is found suitable and has been published in

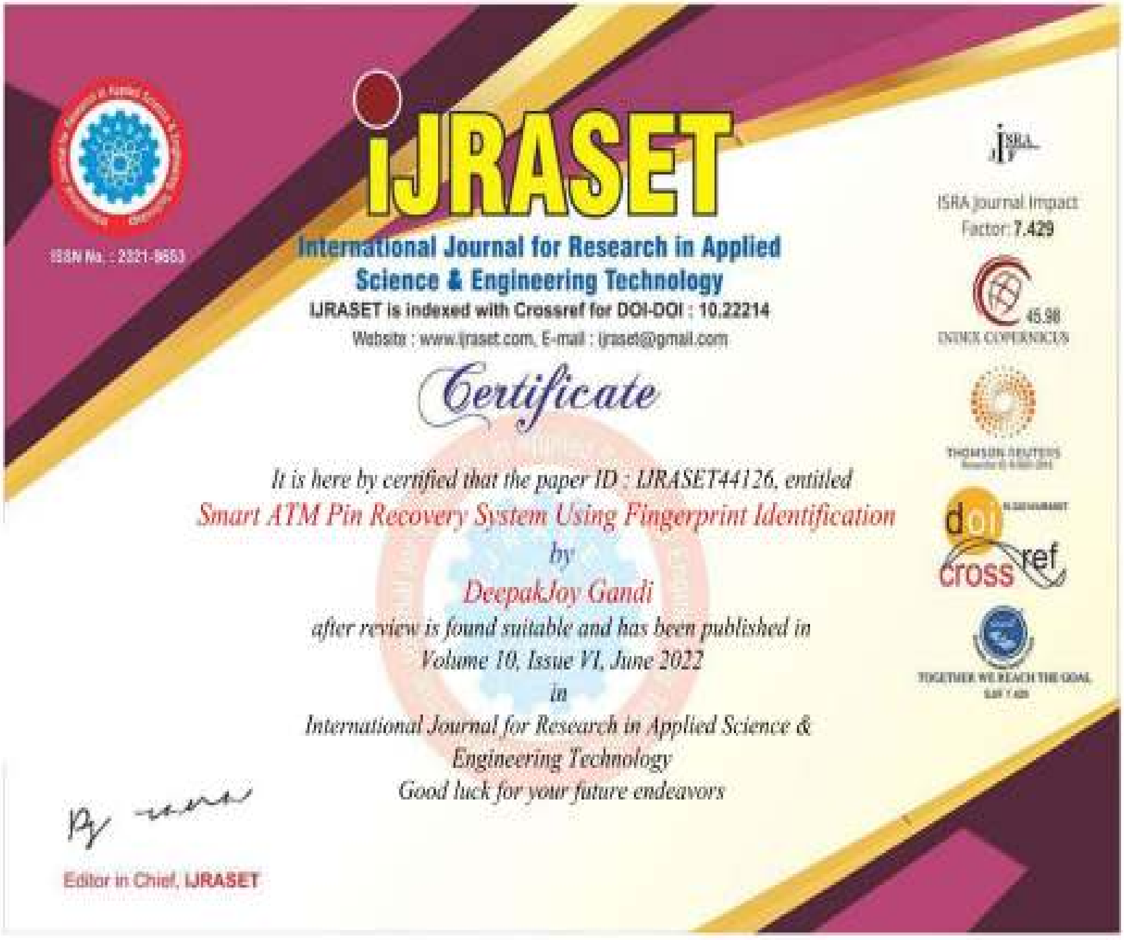
Volume 10, Issue VI, June 2022

in

International Journal for Research in Applied Science & Engineering Technology

Good luck for your future endeavors

Editor in Chief, IJRASET



ISSN No. : 2321-9653

iJRASET

International Journal for Research in Applied Science & Engineering Technology

IJRASET is indexed with Crossref for DOI-DOI : 10.22214

Website : www.ijraset.com, E-mail : ijraset@gmail.com

ISRA Journal Impact Factor: 7.429

45.98 INDEX COPERNICUS

THOMSON REUTERS

TOGETHER WE REACH THE GOAL

Certificate

It is here by certified that the paper ID : IJRASET44126, entitled

Smart ATM Pin Recovery System Using Fingerprint Identification

by

DeepakJoy Gandi

after review is found suitable and has been published in

Volume 10, Issue VI, June 2022

in

International Journal for Research in Applied Science & Engineering Technology

Good luck for your future endeavors

Editor in Chief, IJRASET