GALGOTIAS COLLEGE OF ENGINEERING AND TECHNOLOGY
Department of Information Technology
ODD Semester, 2021-22

Galgotias College of Engineering & Technology

Department of Information Technology

Program Name: B. Tech (IT)
Semester: III
Session: 2021-22/ODD
Subject Name: Mini Project Lab
Subject Code: KCS-354

Faculty Name: MR. NILOTPAL PATHAK

GALGOTIAS COLLEGE OF ENGINEERING AND TECHNOLOGY
Department of Information Technology
ODD Semester, 2021-22

FORMAT FOR SYNOPSIS OF PROPOSED RESEARCH

S.No.	Content	Page No.
1	Title of Proposed Research	
2	Brief Introduction	
3	Brief Review of the Previous Work	
4	Identification of Potential Research Problem	
5	Methodology of the Research Work and major tools required	
6	List of References	

GALGOTIAS COLLEGE OF ENGINEERING AND TECHNOLOGY
Department of Information Technology
ODD Semester, 2021-22

Mini Project Topic

IOT BASED – ATM SECURITY SYSTEM USING FINGERPRINT

SUBMITTED BY: NILESH GUPTA
(2000970130069)
RITIK VISHWAKARMA
(2000970130093)

ABSTRACT

There is a drastic increase in the frauds related to the Automated Teller Machine (ATM) and it has actuated the development of advanced authentication mechanisms that can enhance the security of the ATM. Earlier, the traditional methods like ID card verification were used but due to advancement in the field of banking, technology has been involved in the identification and verification. Current trend of Cybercrime facilitate the need for an enhanced fingerprint application on ATM machine with unique code mechanism. The mechanism enable unassigned fingerprint authentication of customers with quick code and secret code. The project enhances the security authentication of customers using ATM. A core controller using fingerprint recognition system of ATmega128p in-system programmable flash is explored.

An R307 fingerprint module is used to capture fingerprints with DSP processor and optical sensor for verification and Secret-Codes respectively. Upon system testing of capable reduction of ATM fraud using C program, the new method of authentication is presented. Keyword-Automated Teller Machine (ATM) , ATmega128p, Language C program, R307 Fingerprint Module.

INTRODUCTION

Earlier, “barter system” was used for the exchange of goods and merchandise due to the lack of monetary instruments.

But, the society in the modern days has replaced the barter system by using the different monetary instruments as the unit of exchange. Hence, the money is now used for various denominations as the sole purchasing power. Now, this era has brought “plastic money” in the form of credit cards, debit cards, etc. into the existence which has now replaced the paper and metal based currency. This has introduced the Automated Teller Machine (ATM) and its use is increasing day by day all over the world.

Now-a-days, in the self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. ATM (Automatic Teller Machine) which provide the customers with the easily accessible bank note trading is quite common. However, the financial crime cases are rising repeatedly in recent years, many criminals tamper with the ATM terminal and rob the user's credit card and password illegally. Once user's bank atm card is lost and the password is stolen, the criminal will withdraw all the cash with in the shortest time, which will lead to enormous financial losses to customer. How to carry on the valid identity of the customer becomes the main focus in present financial circle. Traditional ATM systems authenticate basically by using the credit card and the password, this method has some defects. Using the credit card and password cannot verify the user's identity exactly. In recent years, the algorithm that the fingerprint

recognition consistently updated and give four digit unique code through the controller which has offered new verification method for us, the original password authentication method joined with the biometric identification method verify the clients' identity much better and achieve the purpose that using of the ATM machines improves the safety effectively.

In this paper, a design on Enhanced ATM security system is presented. As the fingerprint of any person is the most unique identity so the fingerprint module is used for the identification purpose. After the verification of fingerprints, the user can proceed for the transaction but if it is not verified for three attempts, the GSM module will send the warning message to the bank customer as well as to the nearest police station.

This design helps in protecting the user accounts from the unauthorized access. Even if the password is guessed, cracked or stolen, the perpetrator will not be able to access the account without having the verification codes which is obtained by the user only when the fingerprint verification is passed.

DESIGN CONSIDERATION AND SPECIFICATION

The embedded ATM client verification system is based on fingerprint recognition which is designed to improve on the performance of the existing ATM
system. The ATmega128p chip in Arduino microcontroller is used as the core of
this embedded system which is associated with the technologies of fingerprint recognition, unique code mechanism and current high speed network communication. The primary features of the developed system are:

1: Fingerprint recognition: The masters' fingerprint information was used as the standards of detection. It must certify the feature of the human fingerprint
before using ATM system.

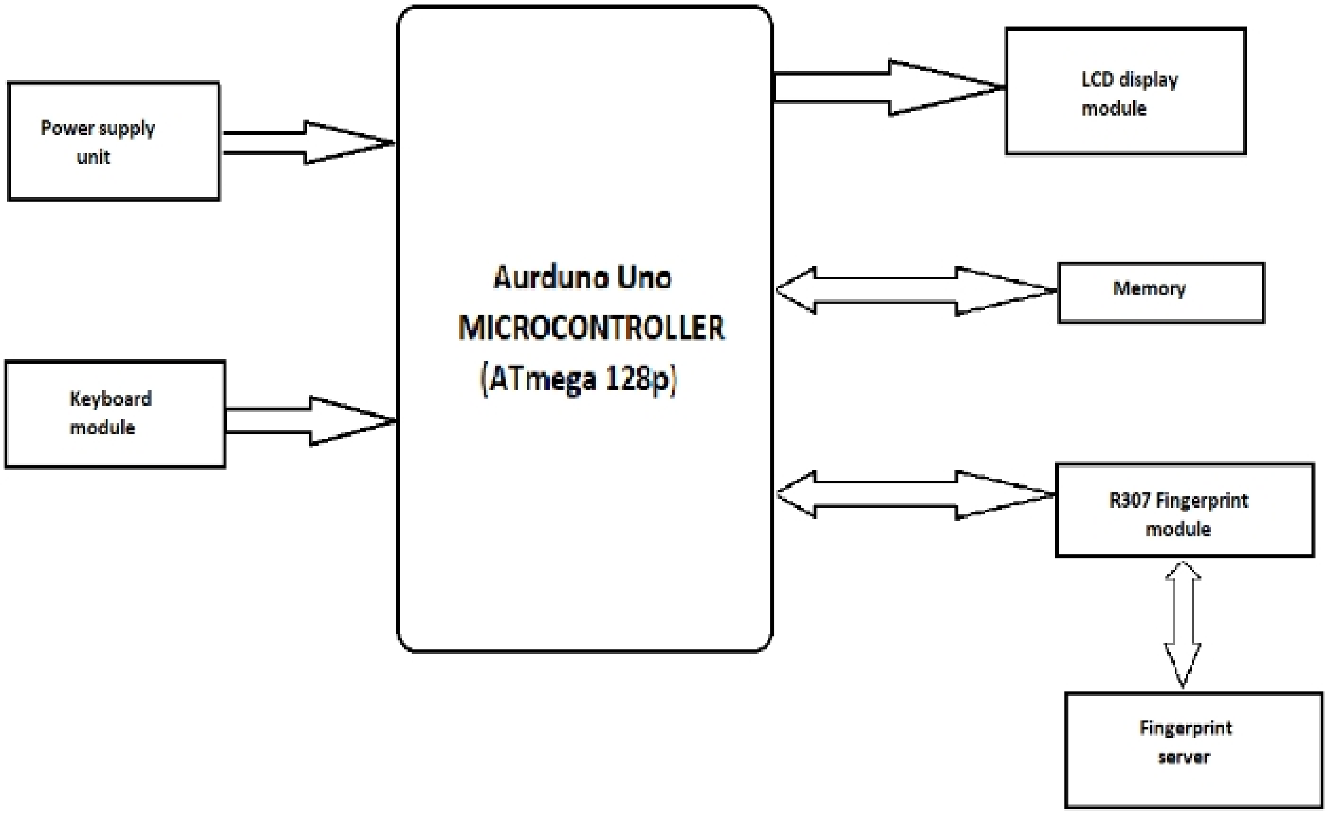
2. Remote verification: System that can compare current client's fingerprint information with remote fingerprint data server.

3. Password: There is customer’s secret code (i.e. S-Code) generated upon registration of fingerprint in the bank.

In an exception of fingerprint verification error of a genuine user, the system demands the customer secret code. In order not to deny a genuine customers access into his/her account, the system is capable to
quickly generate a unique 4-digit access code (i.e. Q-Code) on a condition that the customer supplied a correct secret code. This 4-digit access code will be
sent as OTP (One Time Password) message code to mobile phone of the authorized customer.

4. Two discriminate analysis systems: Unimodal Biometric and Two-tier Security. Two-tier security is used to provide two levels of security. In unimodal system, if the fingerprint system fails (this situation
happens very rarely) then, two level security units will take over and further queries will be required from such a user.

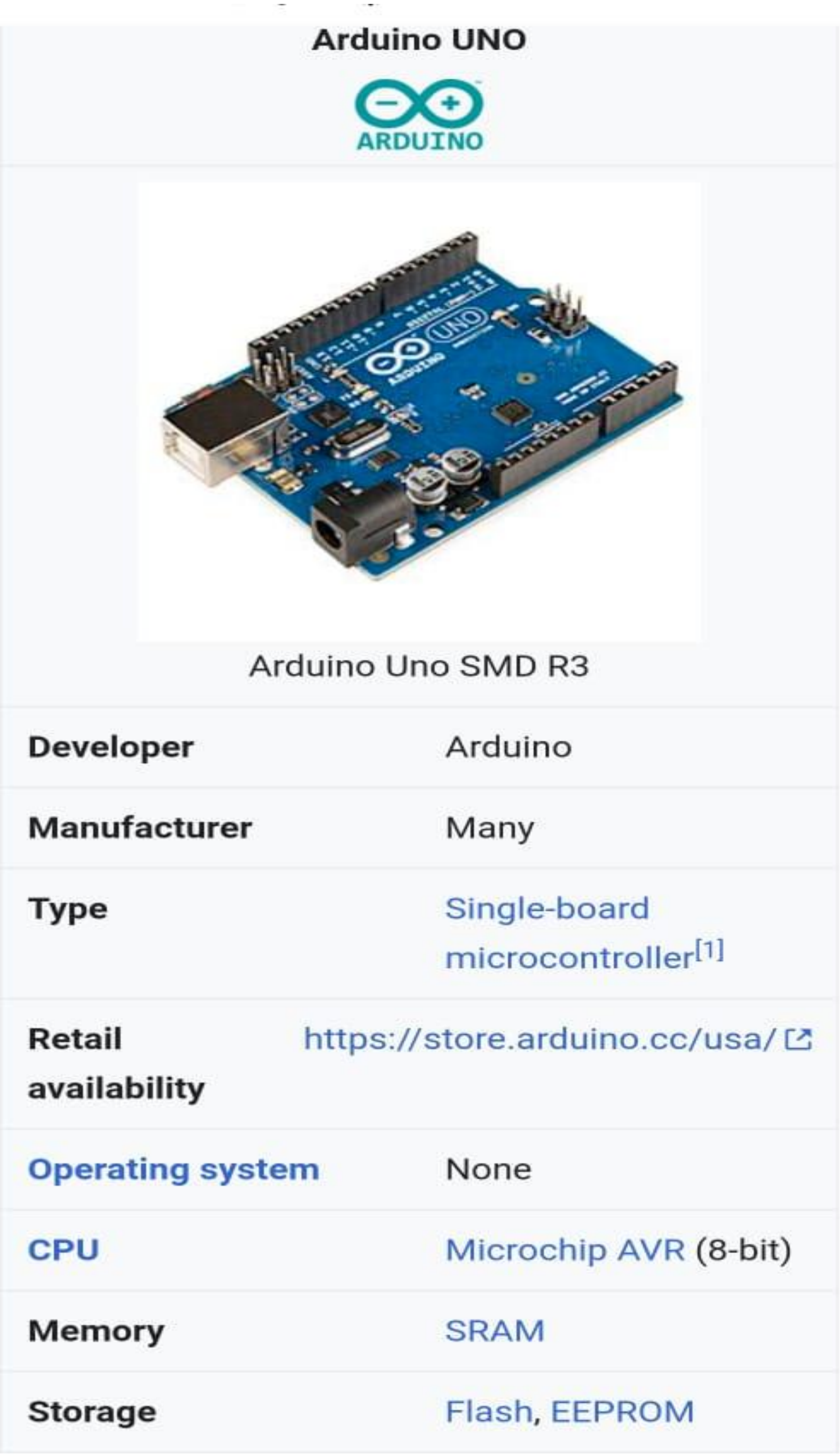
DIAGRAM OF THE PROJECT



MAJOR TOOLS REQUIRED :

- AURDINO MICROCONTROLLER
- FINGERPRINT R307
- JUMPER WIRE
- BREADBOARD
- LCD PANEL
- A2V DATA CABEL
- KEYPAD
- POWER SUPPLY – ADAPTER (12V , 2A)

Microcontroller (Arduino UNO ATMEGA128p)



Arduino UNO

Arduino Uno SMD R3

Developer	Arduino
Manufacturer	Many
Type	Single-board microcontroller[1]
Retail availability	https://store.arduino.cc/usa/
Operating system	None
CPU	Microchip AVR (8-bit)
Memory	SRAM
Storage	Flash, EEPROM

Microcontroller (Arduino UNO ATMEGA128p)

The Arduino Uno is an open-source microcontroller board based on the Microchip ATmega328P microcontroller and developed by Arduino.cc. The board is equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits. The board has 14 digital I/O pins (six capable of PWM output), 6 analog I/O pins, and is programmable with the Arduino IDE (Integrated Development Environment), via a type B USB cable. It can be powered by the USB cable or by an external 9-volt battery, though it accepts voltages between 7 and 20 volts. It is similar to the Arduino Nano and Leonardo.

The word "uno" means "one" in Italian and was chosen to mark the initial release of Arduino Software. The Uno board is the first in a series of USB-based Arduino boards; it and version 1.0 of the Arduino IDE were the reference versions of Arduino, which have now evolved to newer releases. The ATmega328 on the board comes preprogrammed with a bootloader that allows uploading new code to it without the use of an external hardware programmer.

While the Uno communicates using the original STK500 protocol, it differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it uses the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter.

R307 Fingerprint Module

R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other functions.

FEATURES:

• Perfect function: independent fingerprint collection, fingerprint registration, fingerprint comparison (1: 1) and fingerprint search (1: N) function.

• Small size: small size, no external DSP chip algorithm, has been integrated, easy to install, less fault.

• Ultra-low power consumption: low power consumption of the product as a whole, suitable for low-power requirements of the occasion.

• Anti-static ability: a strong anti-static ability, anti-static index reached 15KV above.

• Application development is simple: developers can provide control instructions, self fingerprint application product development, without the need for professional knowledge of fingerprinting.

- Adjustable security level: suitable for different applications, security levels can be set by the user to adjust.

- Finger touch sensing signal output, low effective, sensing circuit standby current is very low, less than 5uA.

Interface 4×3 & 4×4 Membrane Keypad with Arduino

Matrix keypads are the kind of keypads you see on cell phones, calculators, microwaves ovens, door locks, etc. They’re practically everywhere.

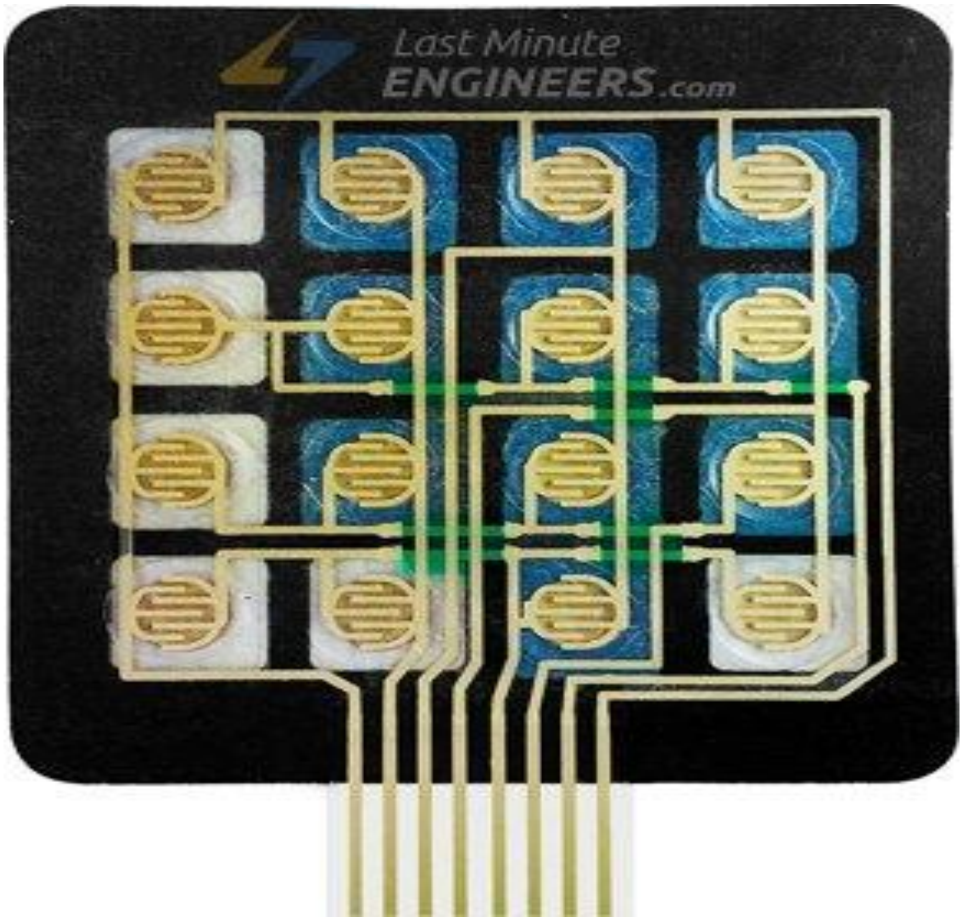
However, in DIY electronics, they are a great way to let users interact with your project and are often needed to navigate menus, punch in passwords and control robots.

Membrane keypads are made of a thin, flexible membrane material. They do come in may sizes 4×3, 4×4, 4×1 etc. Regardless of their size, they all work in the same way.

One of the great thing about them is that they come with an adhesive backing so you can attach it to nearly anything. You just have to peel the paper backing off.

Let’s take 4×4 keypad as an example. It has total 16 keys. Beneath each key is a special membrane switch.

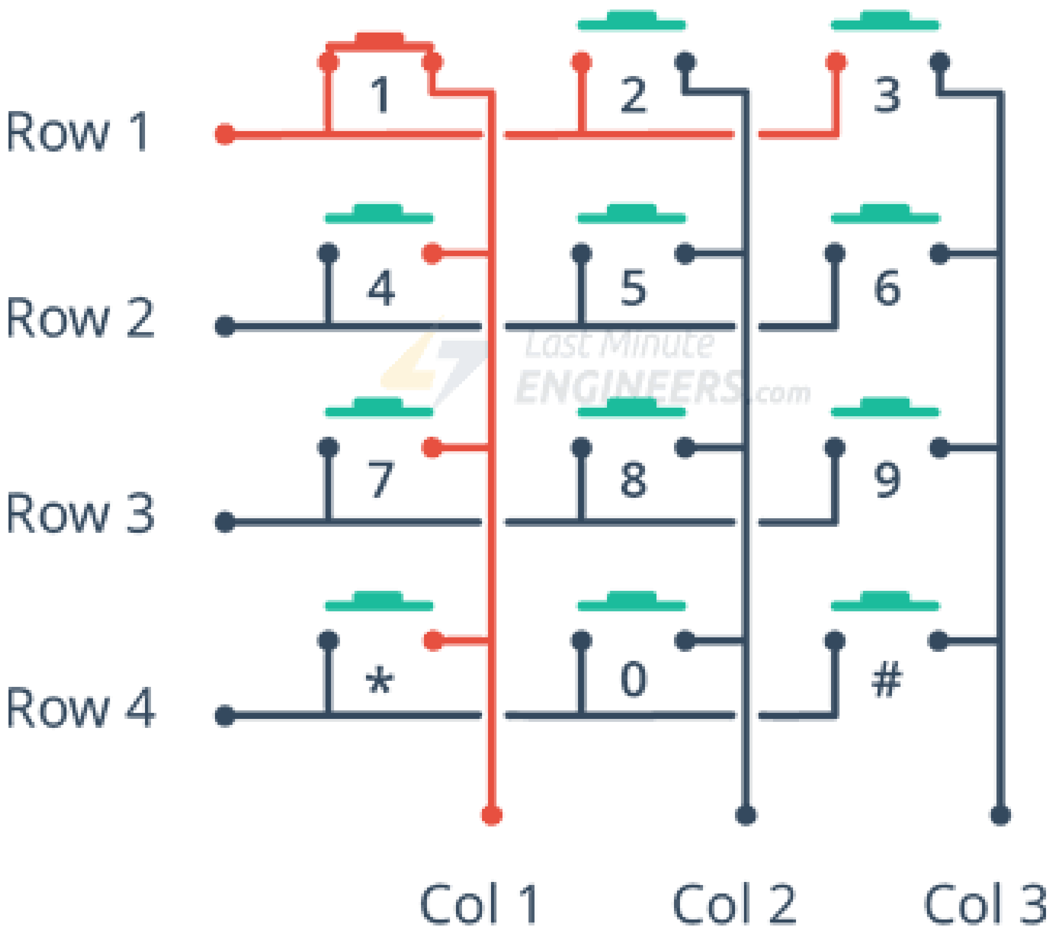
All these membrane switches are connected to each other with conductive trace underneath the pad forming a matrix of 4×4 grid.



If you had used 16 individual push buttons, you would have required 17 input pins (one for each key and a ground pin) in order to make them work. However, with matrix arrangement, you only need 8 microcontroller pins (4-columns and 4-rows) to scan through the pad.

How keypad works & How to scan them?

The working principle is very simple. Pressing a button shorts one of the row lines to one of the column lines, allowing current to flow between them. For example, when key ‘4’ is pressed, column 1 and row 2 are shorted.



A microcontroller can scan these lines for a button-pressed state. To do this, it follows below procedure.

1. Microcontroller sets all the column and row lines to input.
2. Then, it picks a row and sets it HIGH.

3. After that, it checks the column lines one at a time.
4. If the column connection stays LOW, the button on the row has not been pressed.
5. If it goes HIGH, the microcontroller knows which row was set HIGH, and which column was detected HIGH when checked.
6. Finally, it knows which button was pressed that corresponds to detected row & column.

LCD DISPLAY (16X2)

In LCD 16×2, the term LCD stands for Liquid Crystal Display that uses a plane panel display technology, used in screens of computer monitors & TVs, smartphones, tablets, mobile devices, etc. Both the displays like LCD & CRTs look the same but their operation is different. Instead of electrons diffraction at a glass display, a liquid crystal display has a backlight that provides light to each pixel that is arranged in a rectangular network.

Every pixel includes a blue, red, green sub-pixel that can be switched ON/OFF. Once all these pixels are deactivated, then it will appear black and when all the sub-pixels are activated then it will appear white. By changing the levels of each light, different color combinations are achievable. This article discusses an overview of LCD 16X2 & its working with applications.

An electronic device that is used to display data and the message is known as LCD 16×2. As the name suggests, it includes 16 Columns & 2 Rows so it can display 32 characters (16×2=32) in total & every character will be made with 5×8 (40) Pixel Dots. So the total pixels within this LCD can be calculated as 32 x 40 otherwise 1280 pixels.

16 X2 displays mostly depend on multi-segment LEDs. There are different types of displays available in the market with different combinations such as 8×2, 8×1, 16×1, and 10×2, however, the LCD 16×2 is broadly used in devices, DIY circuits, electronic projects due to less cost, programmable friendly & simple to access.

Specifications of LCD 16X2

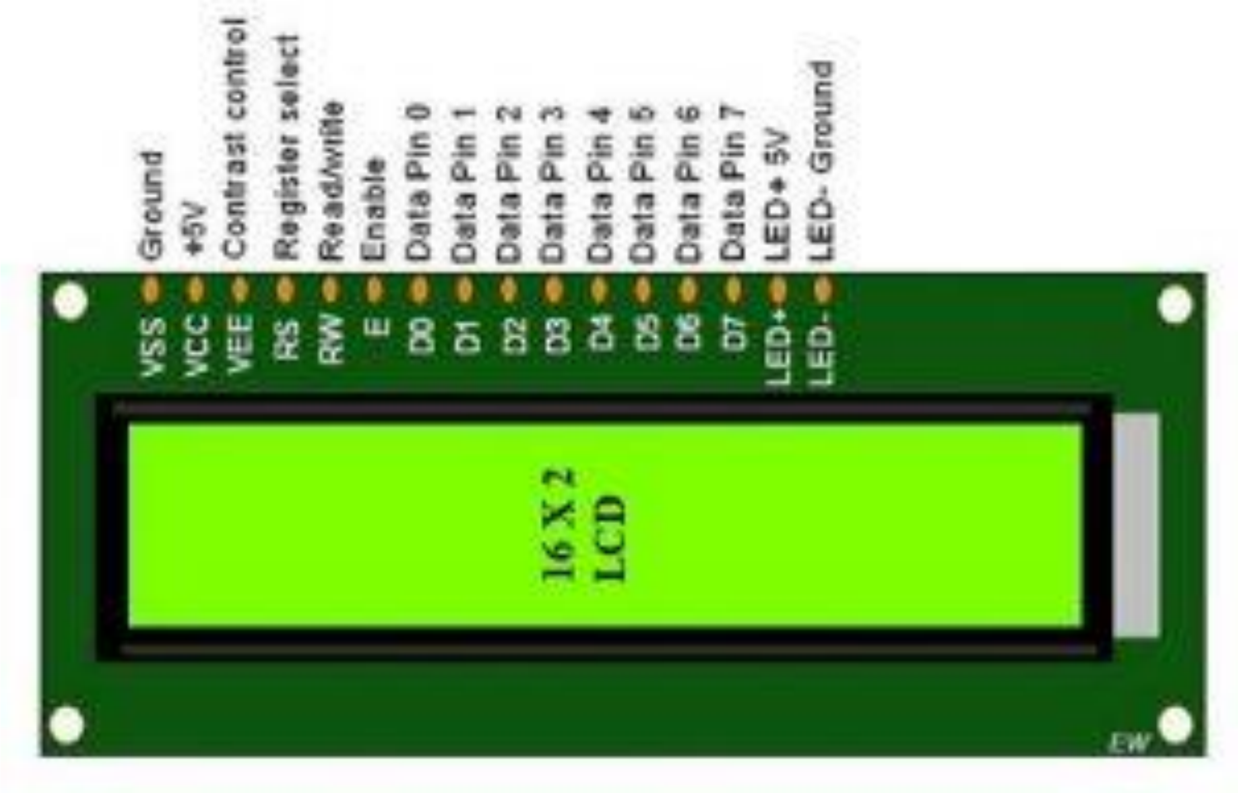
The **specifications of LCD 16X2** are discussed below.

- The operating voltage of this display ranges from 4.7V to 5.3V
- The display bezel is 72 x 25mm
- The operating current is 1mA without a backlight

- PCB size of the module is 80L x 36W x 10H mm
- HD47780 controller
- LED color for backlight is green or blue
- Number of columns – 16
- Number of rows – 2
- Number of LCD pins – 16
- Characters – 32
- It works in 4-bit and 8-bit modes
- Pixel box of each character is 5×8 pixel
- Font size of character is 0.125Width x 0.200height

LCD 16X2 Pin Configuration

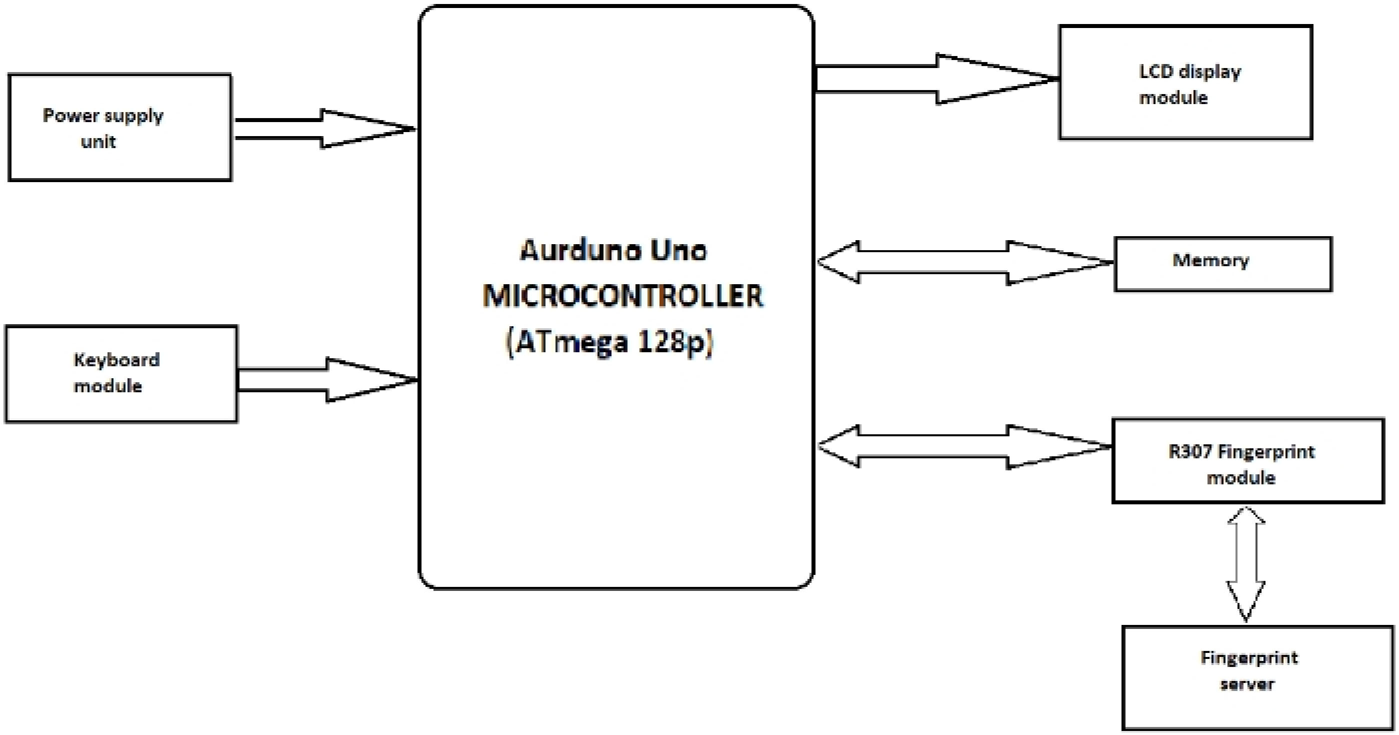
The **pin configuration of LCD 16 X 2** is discussed below so that LCD 16×2 connection can be done easily with external devices.



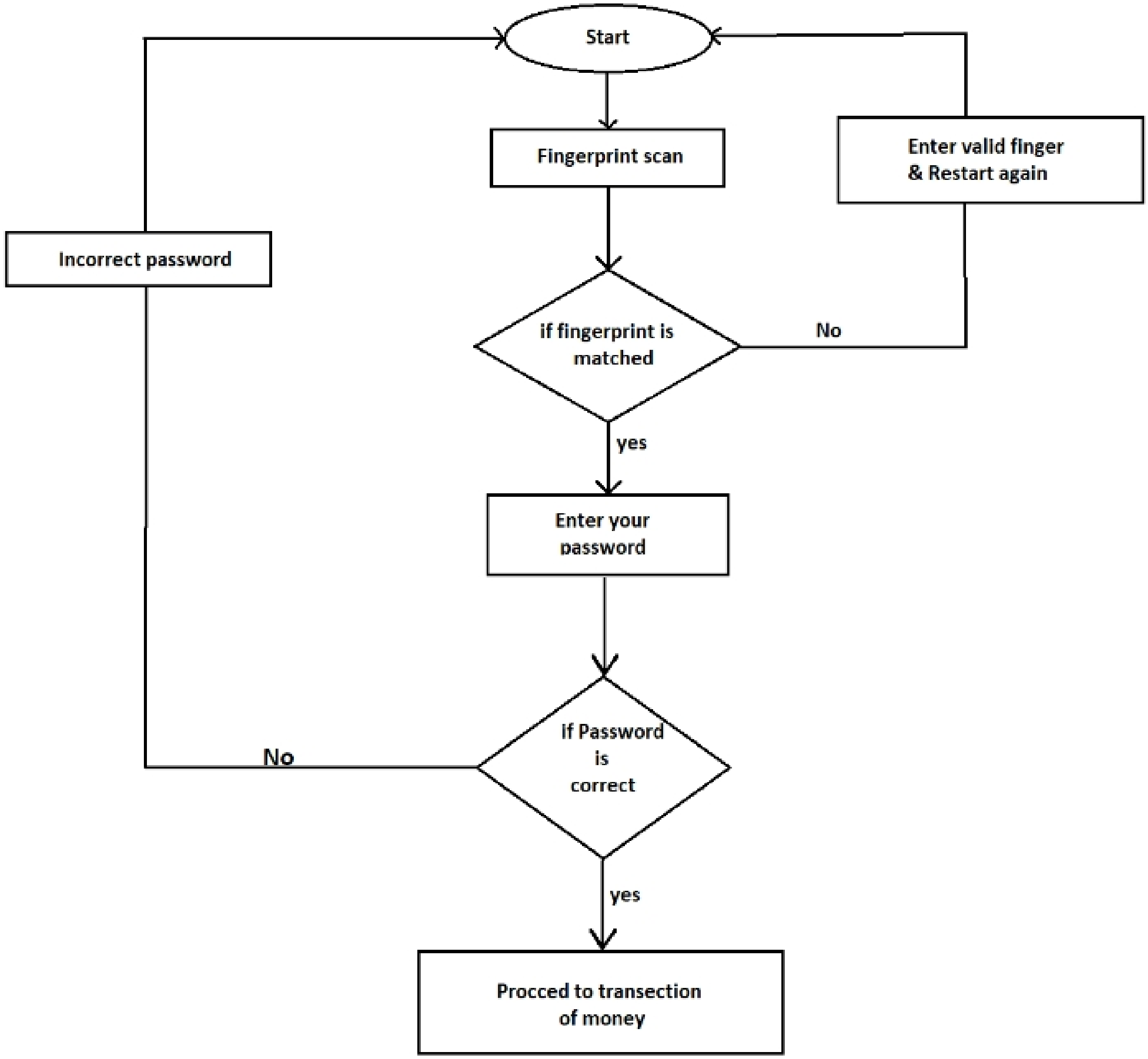
16X2 LCD Pin Diagram

- Pin1 (Ground): This pin connects the ground terminal.
- Pin2 (+5 Volt): This pin provides a +5V supply to the LCD
- Pin3 (VE): This pin selects the contrast of the LCD.
- Pin4 (Register Select): This pin is used to connect a data pin of an MCU & gets either 1 or 0. Here, data mode = 0 and command mode =1.
- Pin5 (Read & Write): This pin is used to read/write data.
- Pin6 (Enable): This enables the pin must be high to perform the Read/Write procedure. This pin is connected to the data pin of the microcontroller to be held high constantly.
- Pin7 (Data Pin): The data pins are from 0-7 which are connected through the microcontroller for data transmission. The LCD module can also work on the 4-bit mode through working on pins 1, 2, 3 & other pins are free.
- Pin8 – Data Pin 1
- Pin9 – Data Pin 2
- Pin10 – Data Pin 3
- Pin11 – Data Pin 4
- Pin12 – Data Pin 5
- Pin13 – Data Pin 6
- Pin14 – Data Pin 7
- Pin15 (LED Positive): This is a +Ve terminal of the backlight LED of the display & it is connected to +5V to activate the LED backlight.
- Pin16 (LED Negative): This is a -Ve terminal of a backlight LED of the display & it is connected to the GND terminal to activate the LED backlight.

METHODOLOGY



FLOWCHART


Start
Fingerprint scan
Enter valid finger
& Restart again
Incorrect password
if fingerprint is
matched
No
yes
Enter your
password
If Password
is
correct
No
yes
Procced to transection
of money

ALGORITHMS OF THE PROJECT

Algorithms:

The algorithms for the proposed system are described below

START

STEP 1: Scan your finger the ATM Machine

STEP 2: Enter PIN

STEP 3: If PIN is Valid GOTO STEP 7 ELSE GOTO STEP 2

STEP 4: Verify if Incorrect PIN has been entered trice

STEP 5: If incorrect PIN entered trice GOTO STEP 6 ELSE GOTO STEP 2

STEP 6: Block and Retain ATM card GOTO STEP 15

STEP 7: Input withdrawal amount

STEP 8: If withdrawal amount > maximum allowed GOTO STEP 7

STEP 9: Verify account balance

STEP 10: If balance is sufficient GOTO STEP 11 ELSE GOTO STEP 15

STEP 11: Terminate transaction GOTO STEP 15

STEP 12: Verify balance availability

STEP 13: If sufficient balance GOTO STEP 14 ELSE GOTO STEP 15

STEP 14: Disburse balance

STEP 15: Exit

STOP

IDENTIFICATION OF POTENTIAL RESEARCH PROBLEM

1. Noise in sensed data- The accuracy playa serious role in recognition of biometry. The accuracy of the biometric systemic extremely sensitive to the standard of the biometric input and also the noise gift within the information can lead to a big reduction within the accuracy. a. E.g. the fingerprints on a person can get damaged and also, it changes with age.

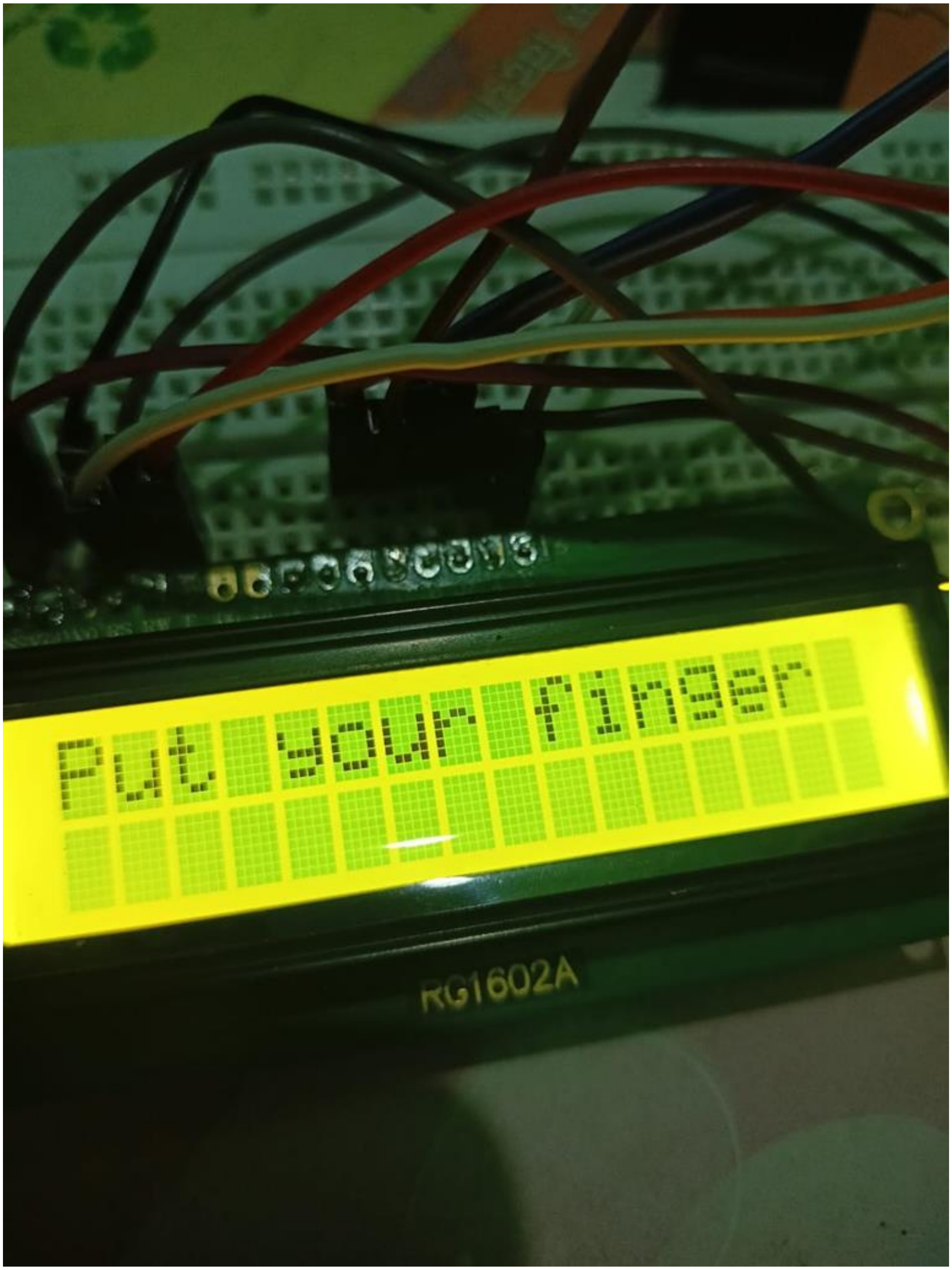
2. Lack of individuality- Feature extracted from completely different people could also be similar. This lack of individualism will increase the False settle for Rate (FAR) of a biometric system.

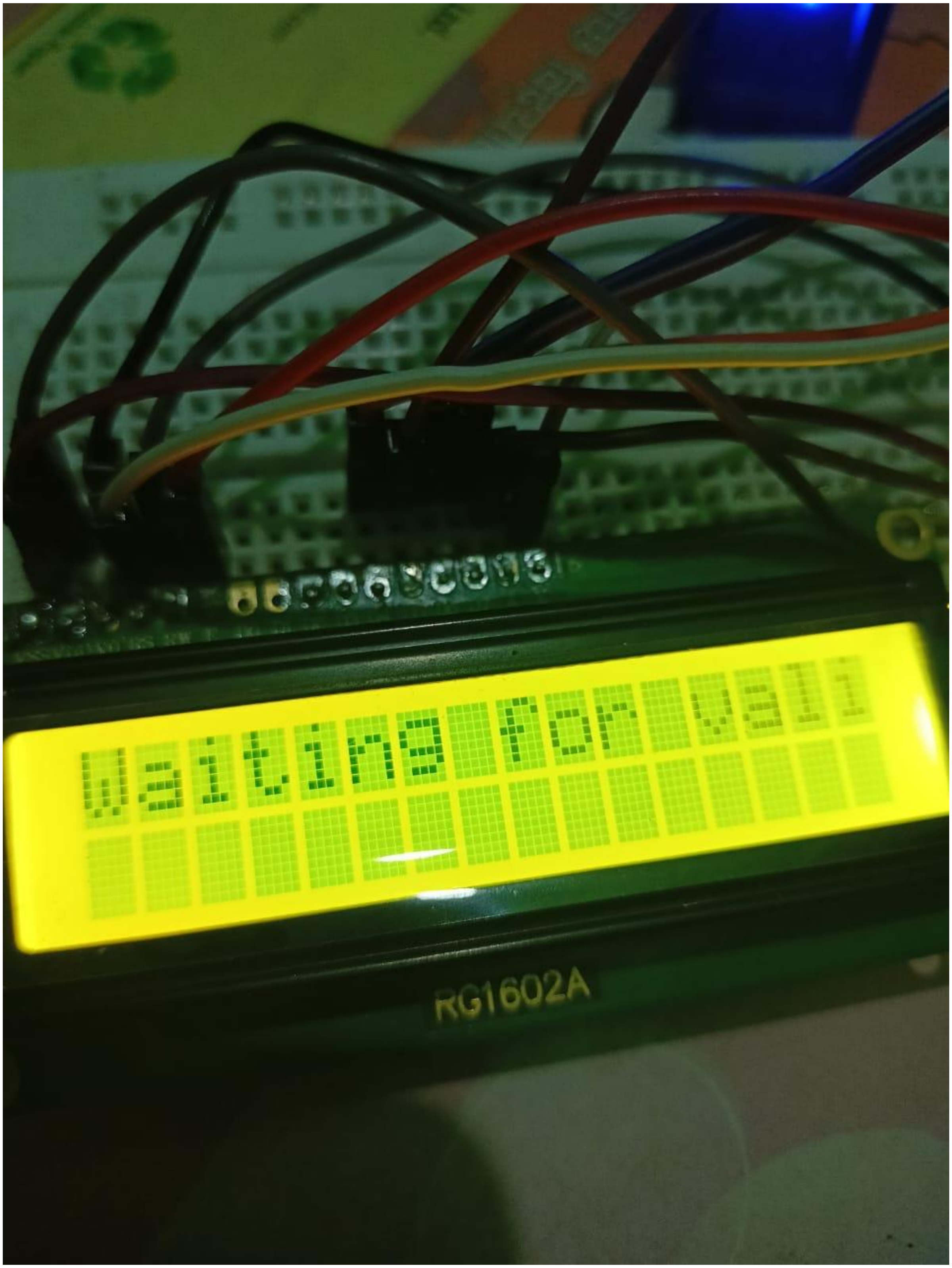
3. Intra-class variations- The data acquired for verification won't match to the information used for generating guide throughout enrollment. as an example the face biometric is capture dander Neath completely different angle. Massive intra-class variations increase the False Reject Rate (FRR) of a @biometric system.

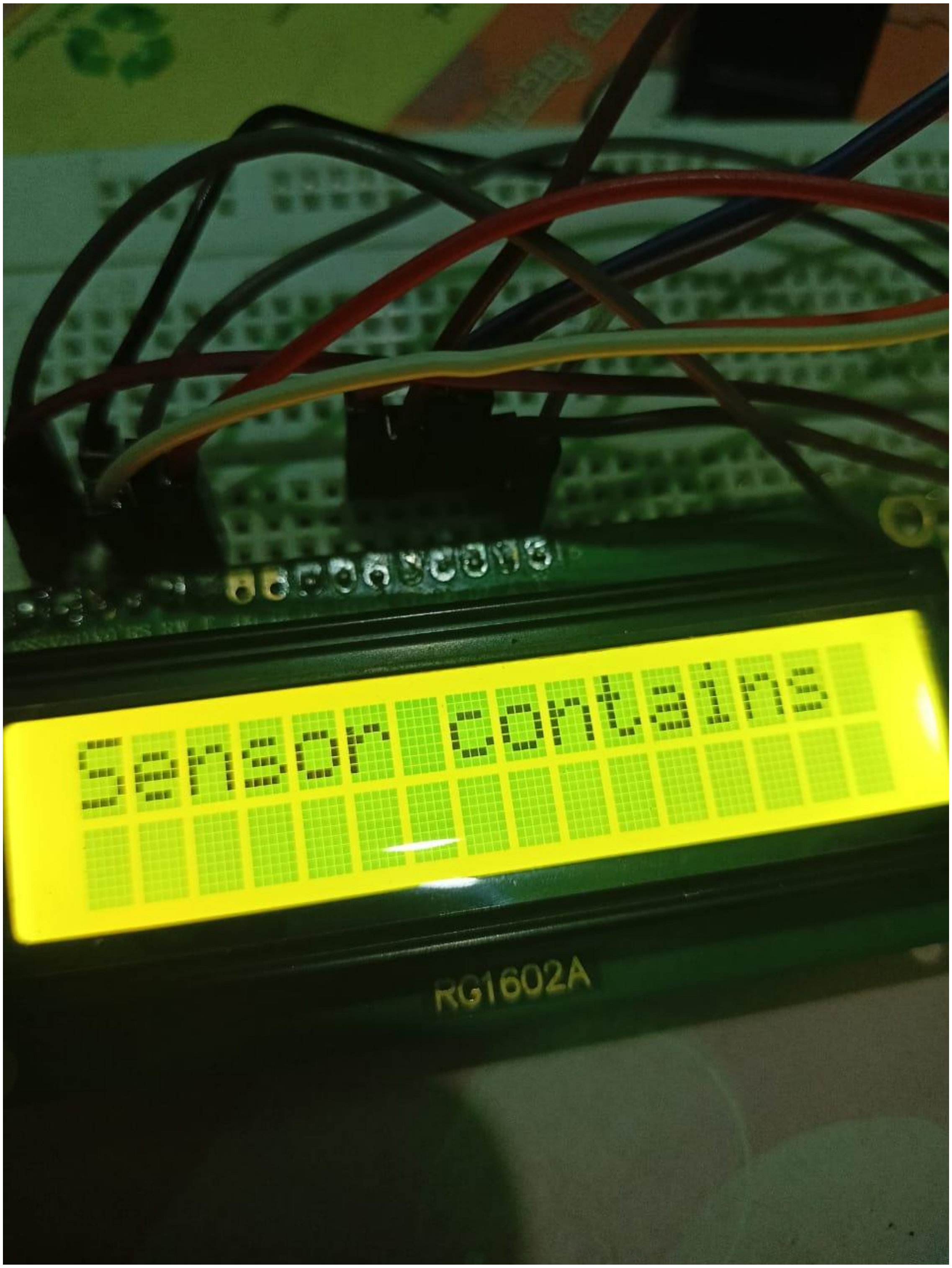
4. Inter-class variations- It happens primarily between twins. It refers to the overlap of feature are as similar to multiple people. Massive inter-class variations increase the False Acceptance Rate (FAR) of a biometric system.

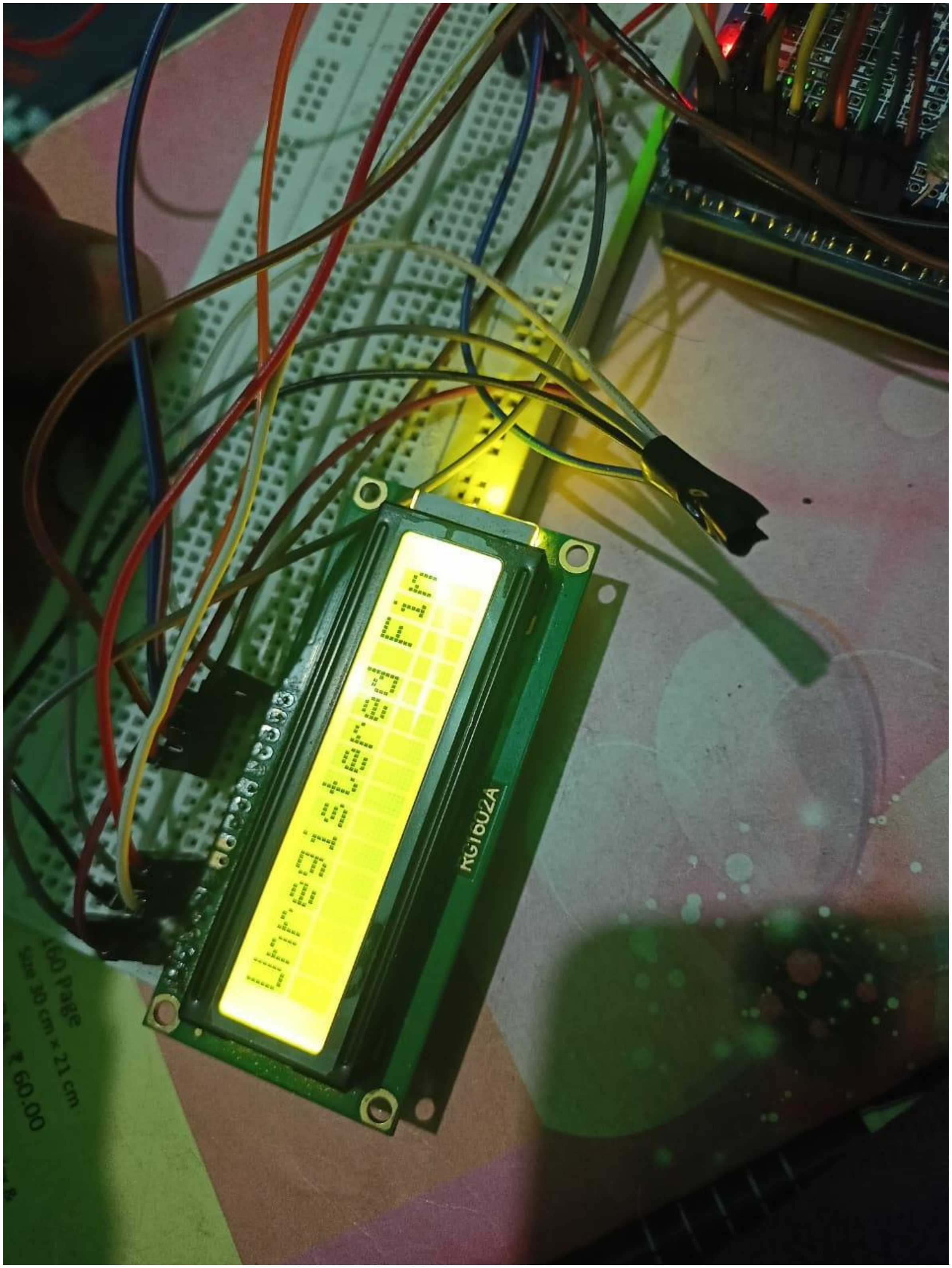
5. Spoofing- A biometric system could also be circumvented by presenting afflux biometric attribute to the detector.

PICS OF EXPERIMENT

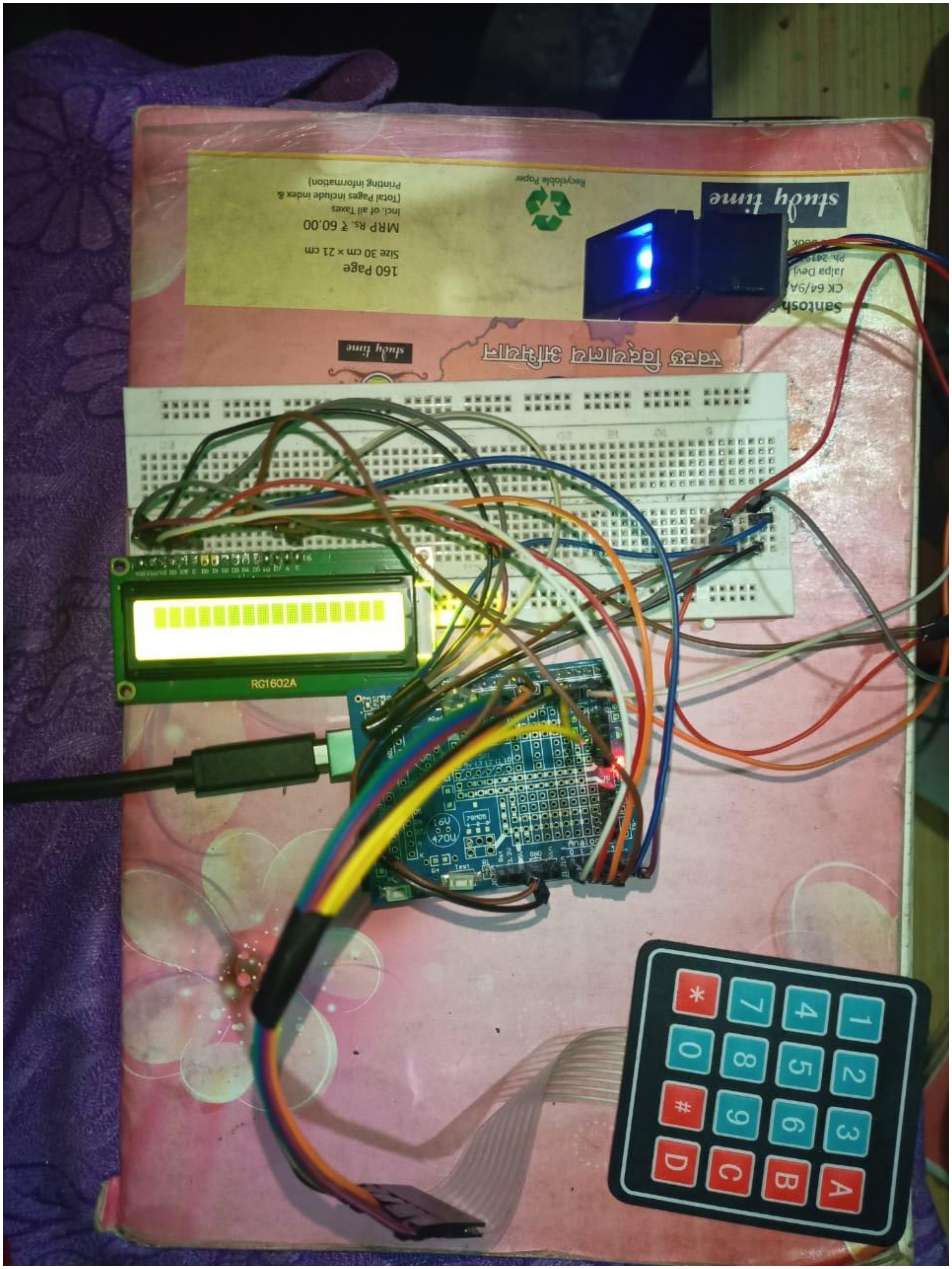



Waiting for vali
RG1602A


Sensor contains
RG1602A


Unregistered ID
RG1602A

RG1602A
160 Page
Size 30 cm × 21 cm
₹ 60.00


RG1602A
1
2
3
A
4
5
6
B
7
8
9
C
*
0
#
D

REFERENCES

[1] Jimoh, R.G. and Babatunde, A. N. (2014). Enhanced Automated Teller Machine using Short Message Service authentication verification. World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering 2014. Vol:8 No:1 pp.14-17

[2] Adepoju, A.S & Alhassan, M.E. (2010). Challenges of automated Teller Machine (ATM) usage and fraud occurrences in Nigeria – A case study of selected banks in Minna metropolis. Journal of Internet Banking and Commerce. Vol 15, No. 2. pp. 1-10. [Online]. Available: http://www.arraydev.com/commerce/JIBC/2010-08/Solomon.pdf

[3] Siddique, M.I & Rehman, S. (2011). Impact of Electronic crime in Indian banking sector – An Overview Int. International Journal of Business & Information Technology. Vol-1 No. 2 September 2011 pp.159-164.

[4] Leow, H.B. (1999). New Distribution Channels in banking Services. Banker‟s Journal Malaysia, No.110, June 1999, pp.48-56. E. H. Miller, “A note on reflector arrays (Periodical style—Accepted for publication),” IEEE Trans. Antennas Propagat., to be published.

[5] Aliyu, A.A. & Tasmin, R.B. (2012) Information and Communication Technology in Nigerian Banks: Analysis of Services and Consumer Reactions. In proceedings of 3rd International Conference in Business and Economic Research (3rd ICBER 2012) MARCH 2012. pp. 150-164 C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

[6]. https://www.rsisinternational.org/IJRSI/Issue41/56-59.pdf

[7]. http://www.ijaerd.com/papers/finished_papers/ATM_SECURITY- IJAERDV05I0640547.pdf

[8]. http://www.ijsrp.org/research-paper-0416/ijsrp-p5225.pdf

[9]. https://media.neliti.com/media/publications/264949-enhanced-atm-security-system-using-gsm-g-24b6dc5f.pdf

[10]. https://ieeexplore.ieee.org/document/7830093