Implementation of Multi Level Authentication System For Person Identification

Dr B.Veera Jyothi, CBIT India.

ABSTRACT

Security is the most important aspect in any part of our lives. A need objective of the utilization of biometrics is to give character confirmation or capacity to precisely perceive people. One major drawback by using biometric fingerprint scanner is silica gel, by using silica gel we can develop latent finger prints on different substrates. This leads us to the next level authentication, by using password. As we know traditional password is a string of characters which is used for user authentication to prove identity. Here again, we can try to attempt to crack password by using brute force attack or dictionary attack To overcome these shortcomings we are enabling third level authentication using OTP. An OTP is a password that is valid for only one login session or transaction. With these three level authentication we have provided a threshold which makes it difficult to illegally access devices.

I. Introduction

In this present age, safety has becomes an essential issue for most of the people especially in the rural and urban areas. Some people try to cheat or steal the property, which may endanger the safety of money and valuable assets in the bank, house, and office. To overcome the security threat, a most of people will install bunch of locks or alarm system. There are many types of alarm systems available in the market, which utilizes different types of sensor. The sensor can detect different types of changes occur in the surrounding and the changes will be processed to be given out an alert according to the pre-set value. By the same time this system may not be good for all the time. Theft is one of the major problems in schools and offices. To minimize these incidents, different ways to secure belongings and documents were done. Most universities and offices use lockers and cabinets for storing files, securing belongings and keeping of important documents for privacy and security purposes. However, some lockers used ordinary padlocks and were shared by two or more users. Common lockers do not guarantee full safety and security of property because ordinary padlocks can be opened by force In this thesis we have implemented safety of the valuable belongings in the bank locker, house, and office (treasury) by using OTP, Keypad and a fingerprint scanner based multi layered security system.

Software programs are known as sketches. These sketches are coded using embedded c programming language using the Arduino IDE. The IDE enables to write, edit code and convert this code into guidelines that Arduino hardware able to recognise.

```
project
}
void setup()
{
pinMode(enroll, INPUT_PULLUP);
pinMode(up, INPUT_PULLUP);
pinMode(down, INPUT_PULLUP);
pinMode(del, INPUT_PULLUP);
pinMode(buzzer, OUTPUT);
lcd.begin(16,2);
lcd.print("WELCOME TO THE");
lcd.setCursor(0,1);
lcd.print("   PROJECT");
delay(1000);
finger.begin(57600);
Serial.begin(9600);
lcd.clear();
lcd.print("FINDING MODULE");
lcd.setCursor(0,1);
delay(1000);
if (finger.verifyPassword())
{
//Serial.println("FOUND FINGERPRINT");
lcd.clear();
lcd.print("FOUND MODULE");
delay(1000);
}
else
{
//Serial.println("FINGERPRINT NOT FOUND");
lcd.clear();
lcd.print(" FP NOT FOUND");
lcd.setCursor(0,1);
lcd.print("CHECK CONNECTION");
while (1);
}
}
```

Fig.1: Setup Code Snippet

The above code illustrates that as soon as the power is supplied to the board LCD displays a message "WELCOME TO THE PROJECT" and then it searches for the fingerprint module. If it founds the module then LCD displays "FOUND MODULE" else it displays a message to check the connection properly. Fig 1 is shown in the set up code.

4.2 FINGERPRINT ENROLLMENT

```
project
}
}
void Enroll()
{
int count=0;
lcd.clear();
lcd.print("ENROLL FINGER     ");
lcd.setCursor(0,1);
lcd.print("LOCATION:");
while(1)
{
lcd.setCursor(9,1);
lcd.print(count);
if(digitalRead(up) == 0)
{
count++;
if(count>25)
count=0;
delay(500);
}
else if(digitalRead(down) == 0)
{
count--;
if(count<0)
count=25;
delay(500);
}
else if(digitalRead(enroll) == 0)
{
return;
}
}
}
```

Fig.4.3: Finger print Enrolment Code Snippet

The above code illustrates the enrolment of fingerprint. Once the enrolment process is started the user is asked to place the finger. Once the fingerprint features are detected, it gets stored in the database with enrolment ID.

4.3 PASSWORD VERIFICATION

```
project
lcd.setCursor(0, 0);
lcd.print("ENTER PWD:");
lcd.setCursor(0, 1);
//Serial.print("ENTER PASSWORD");
x=0;
for(i=0;i<3;i++)
{
z[i]=(x);
x++;
delay(500);
}
z[i]='\0';
delay(1000);
if(!strcmp(z,"123"))
{
lcd.clear();
lcd.setCursor(0, 0);                    //move courser to second line
lcd.print("CORRECT PASSWORD");          //showing name
delay(1000);
randam();
delay(1000);
lcd.clear();
lcd.setCursor(0,0);
```

Fig.4.4: Password Verification Code Snippet

Password is the second authentication level in our project. Its a three digit passkey which user should register it before, if the fingerprint is successfully scanned the user is asked to enter the password. If the password matches with the predefined one then the LCD displays a message saying that the password is correct. The above code depicts about the password verification. The Code for the password verification is shown in Fig 4.4,

4.4 BUZZER ACTIVATION

```
project
}
else
{
digitalWrite(buzzer,HIGH);
delay(1000);
digitalWrite(buzzer,LOW);
lcd.clear();
lcd.setCursor(0, 0);                    //move courser to second line
lcd.print("WRONG PASSWORD");          //showing name
delay(1000);
lcd.clear();
lcd.setCursor(0,0);
lcd.print("SMS SENDING");
Serial.println("AT+CMGF=1");                    //To send SMS in Text Mode
delay(1000);
Serial.println("AT+CMGS=\"+919652196536\"\r");  // change to the phone number you using
delay(1000);
Serial.println("YOUR ACCESS IS DECLAINED DUE TO WRONG PASSWORD ");    //the content of the message
delay(200);
Serial.println((char)26);                       //the stopping character
delay(1000);
lcd.clear();
lcd.setCursor(0,0);
lcd.print("SMS SENT");
delay(1000);
}
}
```

Fig.4.5: Buzzer Activation Code Snippet

If the password entered by the user is an incorrect one then the buzzer will be activated alerting the bank officials and the registered user by sending a message which displays that “YOUR ACCESS IS DENIED DUE TO WRONG PASSWORD”. The message will be sent to the registered mobile number of the user. The above code is about the buzzer activation and sending message using GSM technology. Fig 4.5 depicts the buzzer activation alert.

4.5 OTP VERIFICATION

```
project
lcd.setCursor(0,0);
lcd.print("SENDING OTP");
Serial.println("AT+CMGF=1");                    //To send SMS in Text Mode
delay(1000);
Serial.println("AT+CMGS=\"+919652196536\"\r");  // change to the phone number you using
delay(1000);
//Serial.println("YOUR AUTHENTICATION IS SUCCESS ");     //the content of the message
Serial.println("OTP IS:");
Serial.println(p);
delay(200);
Serial.println((char)26);                       //the stopping character
delay(1000);
lcd.clear();
lcd.setCursor(0,0);
lcd.print("OTP SENT");
delay(1000);
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("ENTER OTP:");
lcd.setCursor(0, 1);
x=0;
for(i=0;i<3;i++)
{
z[i]=(x);
x++;
delay(500);
}
z[i]='\0';
delay(1000);
```

Fig.4.6: OTP Verification And Random Number Generation Code

Entering the One Time Password is the third level of authentication in our project. After the successful completion of the two levels of authentication an OTP will be sent to the registered user mobile number. OTP is a three digit number. Random numbers are generated from 0-9 for the OTP and for the generation of these random numbers “RANDOM NUMBER GENERATION” function is used in the program. Once the OTP is successfully entered a message will be sent to the user saying that the authentication is successful and the lockers will be opened. If user enters incorrect OTP buzzer will be activated and the lcd displays a message saying that the OTP entered is wrong. The OTP verification and random number generation is shown from Fig 4.6 to 4.8.

TESTING & RESULTS

Fingerprint enrolment

Fingerprint Enrolment is the first step in our project. The user must enrol with his fingerprint with location id in order to access the locker, then the user is asked to follow the steps as shown in fig.5.1 to fig.5.6. By following the steps the enrolment of fingerprint is successfully completed.

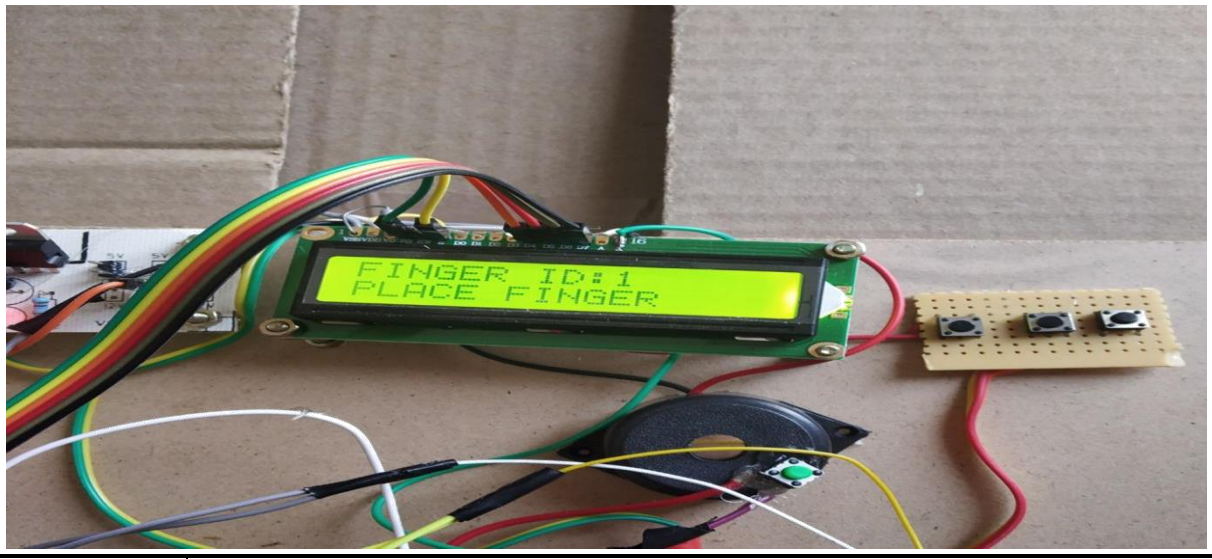

Fig.5.1: Enrolling the user fingerprint at location 1

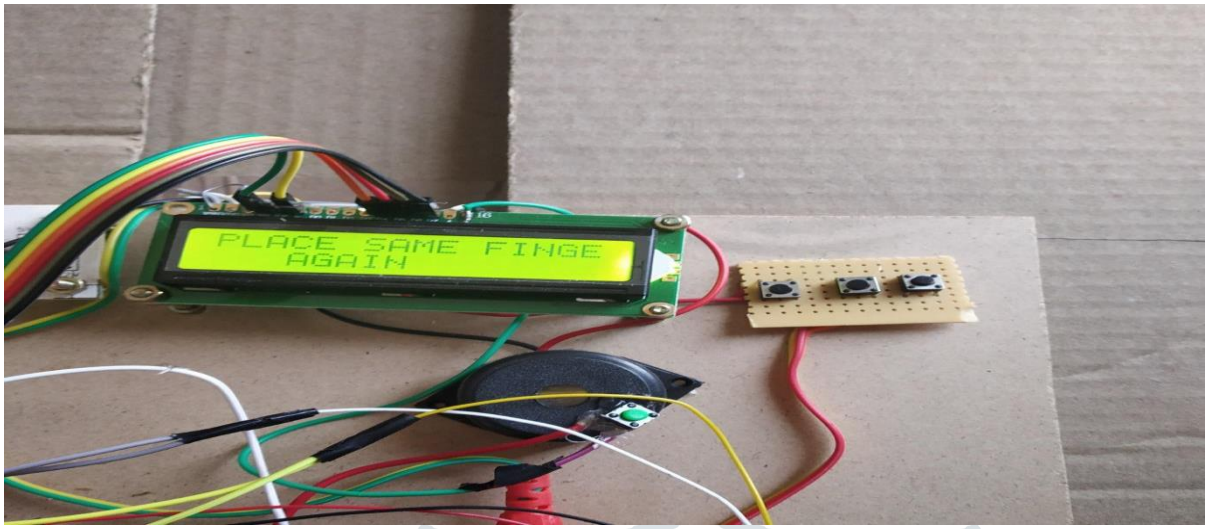

Fig.5.3: Placing the same finger again to match the fingers

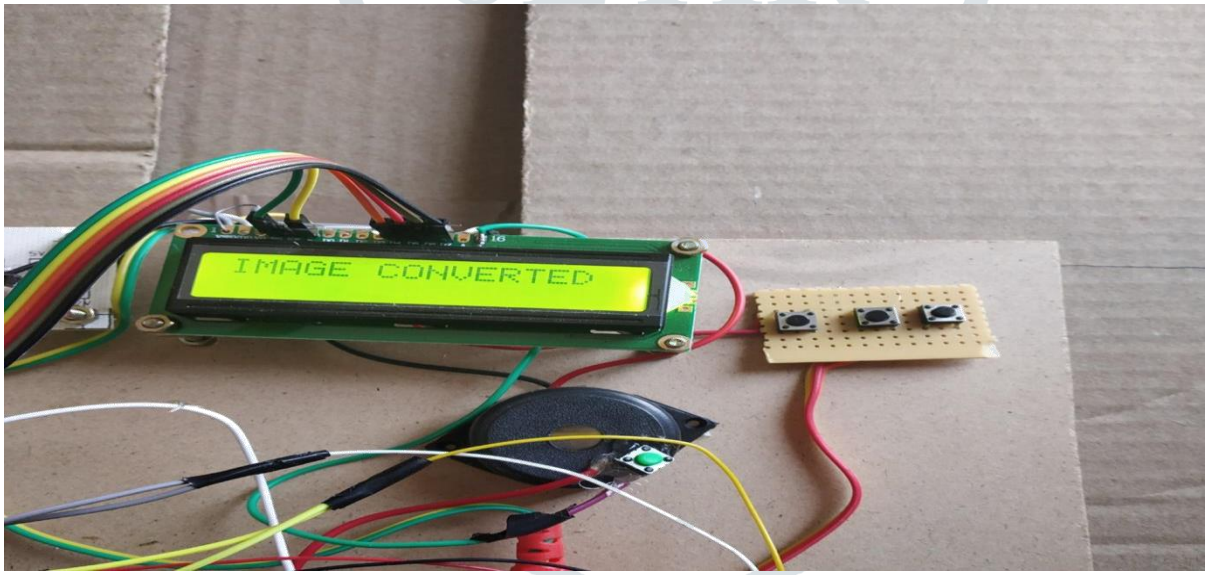

Fig.5.4: Image is converted

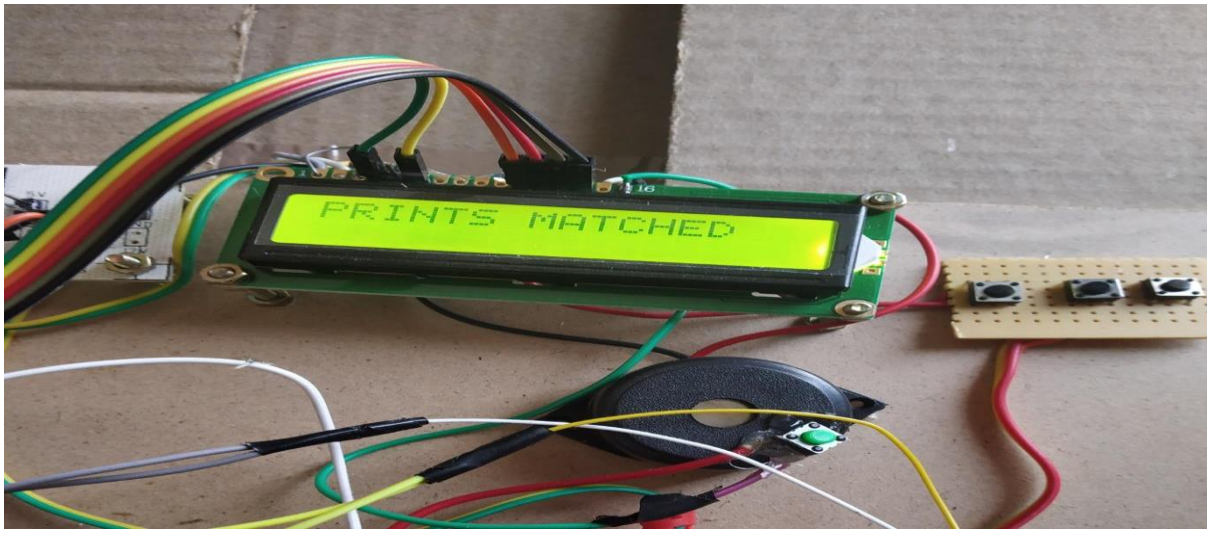

Fig.5.5: Prints are matched

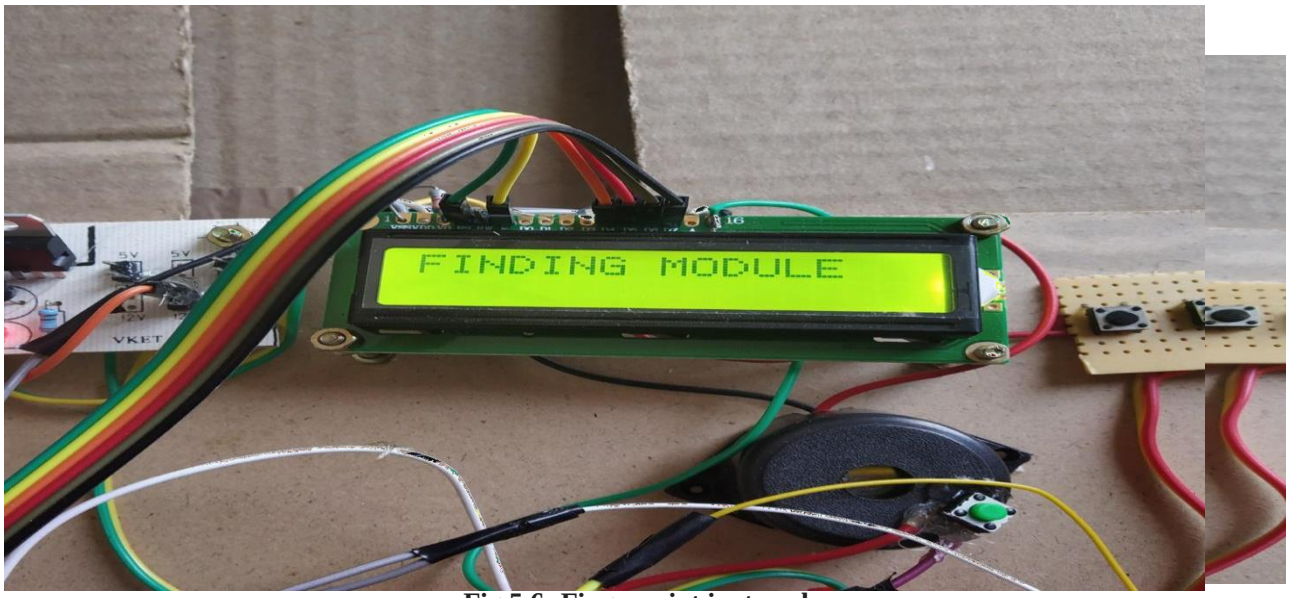

Fig.5.6: Fingerprint is stored

Three level authentication

There are three levels of authentication in our project. In the first level the user is asked to place his finger as shown in fig.5.10.If the fingerprint matches with the predefined one then the LCD displays a message “VALID PERSON” as shown in fig.5.11.Then the second step of authentication is password the user must enter the three digit password if the password matches with the predefined one then LCD displays a message as shown in fig.5.13 and an OTP will be sent to the registered mobile number. The third level of authentication is OTP the user must enter the three digit OTP sent to the target mobile number then a message will be sent to the user as shown in fig.5.16.

Fig.5.7: After the power supply LCD displays a message “WELCOME TO THE PROJECT”

Fig.5.8: Searching for the Fingerprint module

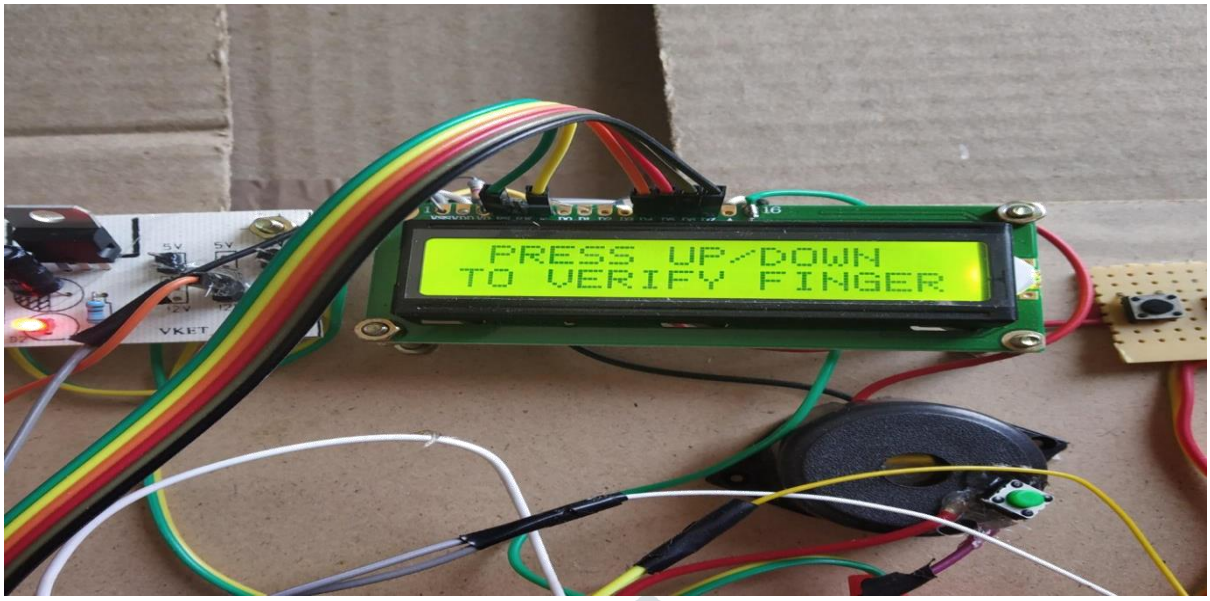

Fig.5.10: Place the finger for verification

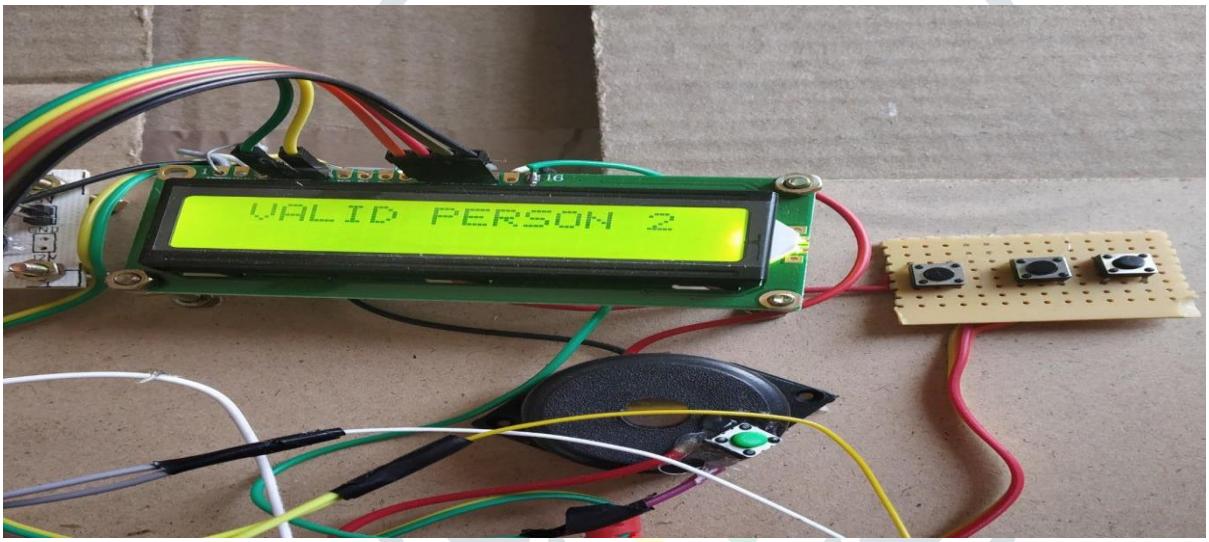

Fig.5.11: If the authentication is successful lcd displays a message "VALID PERSON"

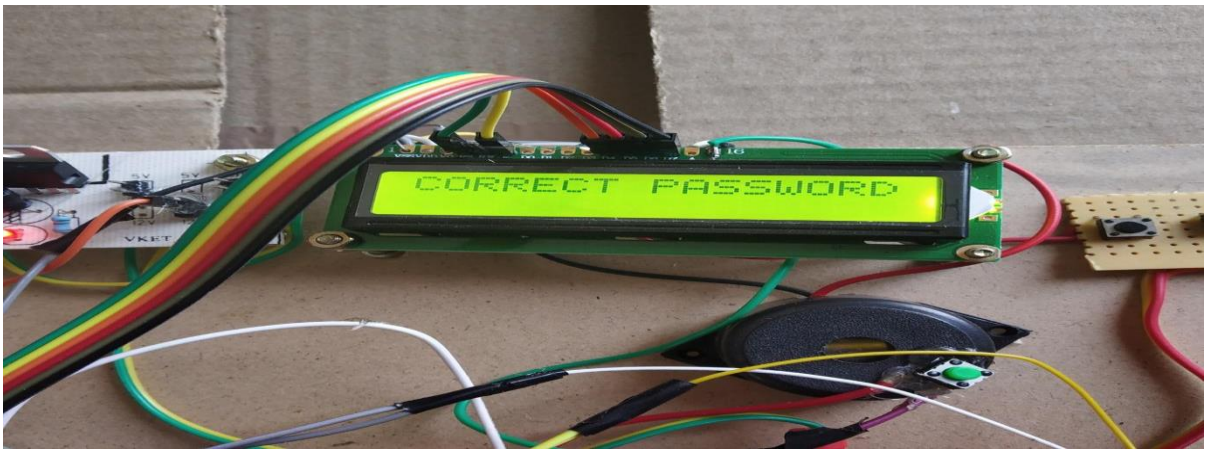

Fig.5.13: If the password is correct LCD displays a message "CORRECT PASSWORD"

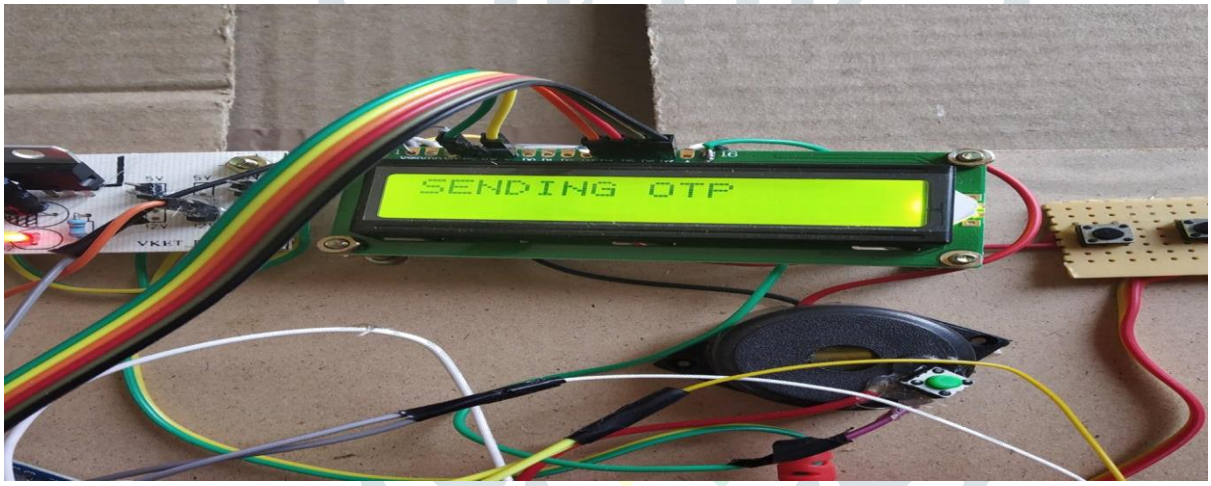

Fig.5.14: OTP will be sent to the registered mobile number

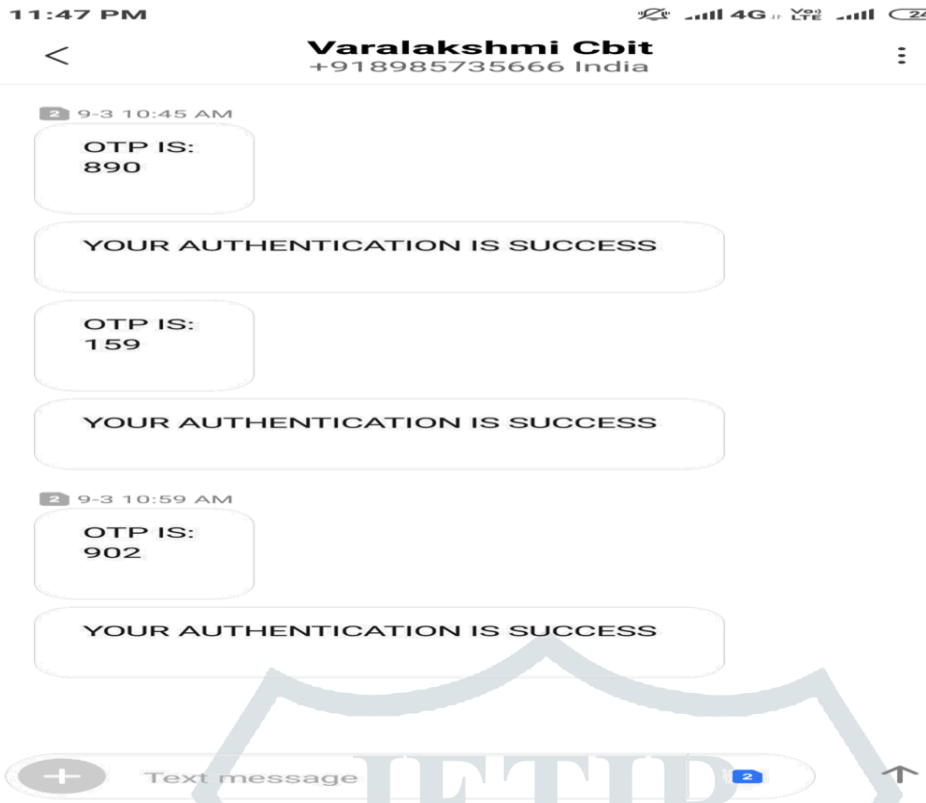

Fig.5.16: OTP is sent to the registered mobile number and if the OTP is correct then the user receives a message "YOUR AUTHENTICATION IS SUCCESS"

Invalid credentials

If the user entered the incorrect credentials in any of the levels then the buzzer will get activated alerting the bank people and a message will be sent to the user as shown in fig.5.20.

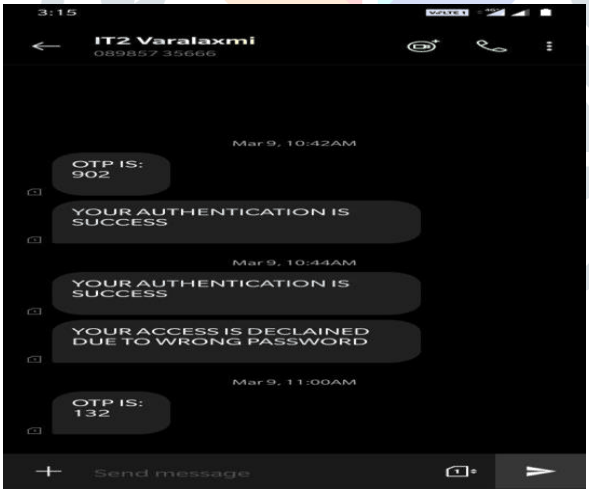

Fig.5.20: The user received a message "YOUR ACCESS IS DECLINED DUE TO WRONG PASSWORD"