Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

GSM BASED ATM SECURITY SYSTEM USING FINGERPRINT SCANNER AND OTP

Vashist Upadhyay[1],Akash Shah[2], Ajay Valiya[3],Abhishek Tiwari[4]

Assistant Prof.Syed Amjed Ali[5]

[1]Department of Electronics and Telecommunication Engineering,Theem College Of Engineering,Boisar,Maharashtra,India

Abstract —**This Project is about improving the security of the ATM systems with the help of an RFID card using the OTP (one time password) with GSM technology and also fingerprint authentication. As a result, the paper proposes a framework for user identification and authentication in Automatic Teller Machines (ATMs) using fingerprints and RFID card as opposed to the PIN and magnetic stripe cards authentication method.**

Basically this system works on biometric authentication . in this atm system the person just have to go to atm and with the help of fingerprint scanner he/she can do their transactions without having to carry any card or remembering any password .Suppose if by any chance that person is not able to go to the atm machine and he/she is in need of money then for that we have optional rf id card facility . The rf id will belong to the main user and his/ her contact number will be associated with that rf id .The person whom they trust they can tell them where the card is at home so that other person can go to atm machine and collect the cash .When the rf id will be scanned a otp will be generated and will be sent to the original user .So after the OTP is entered through keypad the transactions will be proceeded .

Keywords-component;Fingerprint scanner R305,RFID card,GSM module,16*2 LCD display,4*4keypad

I.INTRODUCTION

We considered the numerous security challenges encountered by Auto-mated Teller Machines (ATM) and; given that the existing security in theATM system has not been able to address these challenges, we saw the need to enhance the ATM security system to overcome these challenges.We focused on vulnerabilities and the increasing wave of criminal activities occurring at Automated Teller Machines (ATMs) where quick cash is the prime target for criminals rather than at banks themselves.Security management for networks and data is a major issue now-a-days.Fraudsters are increasing day by day introducing new hacking techniques.With the advent of modern technology, there is a drastic increase in fraud.One easy way is ATM fraud which includes fraudulent cash transactions, so there is a need to regularly develop consumer favourable systems to deal with these frauds related to ATM transactions.

II.EXISTING SYSTEM

Most of the ATMs in India are easy targets for Hackers and Malware attacks.70 percent of 2 lacs ATMs in India still run on the Microsoft windows XP O.S, which has already stopped working in 2014. The authorized user carry multiple ATM cards which are of dierent banks and are secured with various passwords.The user has to swipe his ATM card and enter the password by the keypad to perform his transaction activities.

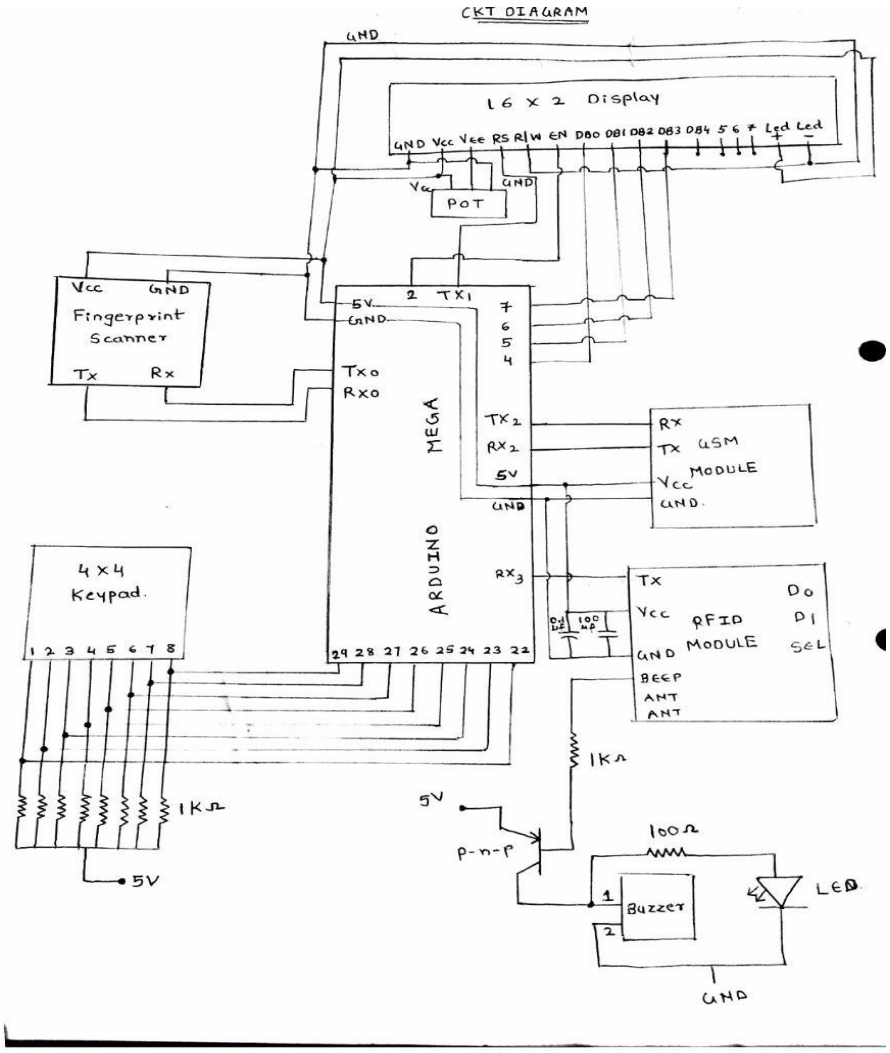
III.DISADVANTAGES OF EXISTING SYSTEM

If the ATM card is stolen and by any means the random password is known then the unauthorized user can access the account. The illitrate people cannot access their account through ATM system because they are not used to it.There is a possibility of system down failures.The existing system are highly prone to the malware attacks using skimming devices.

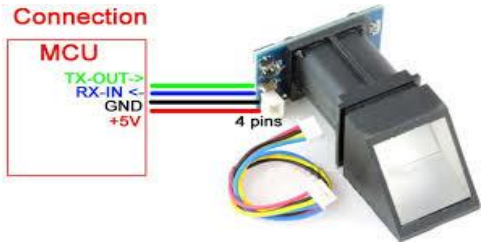
IV.RELATED WORK

Basically this system works on biometric authentication . In this atm system the person just have to go to atm and with the help fingerprint scanner he/she can do their transactions without having to carry any card or remembering any password . Suppose if by any chance that person is notable to go to the atm machine and he/she is in need of money then for thatwe have optional rf id card facility. The rf id will belong to the main user and his/ her contact number will be associated with that rf id .The person whom they trust they can tell them where the card is at home so that other persson can go to atm machine and collect the cash . When the rf id will be scanned a otp will be generated and will be sent to the original user . So after the otp is entered through keypad the transactions will be proceded

V.CIRCUIT DIAGRAM AND DESCRIPTION

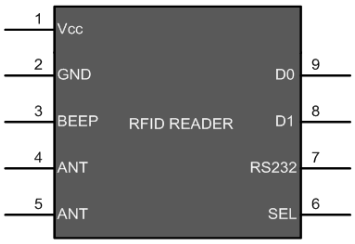


Fingerprint scanner:



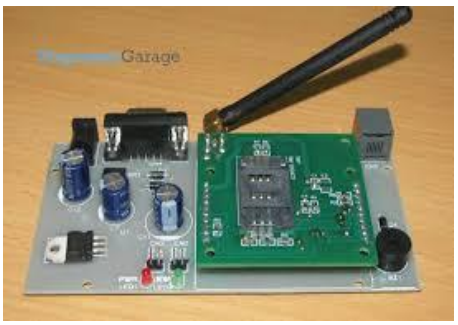
The fingerprint scanner we have used isR305. It has 4 pins i.e Vcc,Gnd,TD,RD.The transactions using the fingerprint scanner uses two step process. 1]fingerprint enrollment:during the enrolment the user scans his finger twice,a fingerprint template is generated it is convertedto the gray scale image and then in forn of 1 and 0s[2] . 2]fingerprint match- ing:during the fingerprint matching process the user needs to scan his finger as soon as he scans his finger the fingerprint template is generated and is sent from the Tx pin of fingerprint module to Rx pin of arduino and it is matched with the database of fingerprint module if match is found the the feedback is send from the Tx pin of Arduino to the Rx pin of Fingerprint module

RFID Module:



Here we are using RF ID as a optional in our project RF ID module - We are using EM-18 RF ID module. It is a device which read the RF-ID CARD by electromagnetic field in which tag is attached.[6] There are 9 pins in RF ID module Pin no. 1 and 2- These pins are Vcc and Ground. They are connected to Arduino for power supply
Pin no. 3 (BEEP) - It is used for buzzer. When the RF ID card reader successfully read then BEEP pin will be high and pnp transistor will be ON which act as a switch and it gives buzzer sound and LED will blink. Capac- itor are used for filteration purpose. The power supply which is given to Rf id module is filtered and given to module Pin no. 4 and 5 - These two pins are D0 and D1. These pins are called weigand data pins. In ideal mode these pins are high but when Logic 1 is send, D1 will move from high to low and D0 remains same and vice versa Pin no. 6- The SEL pin, when it is 1, it will transmit the readed data through Tx pin (Pin no. 7) to the Arduino at RX3 pin and when it is 0 it enable the weigand data pins.However transmitted pin is connected with RS232 IC for making interface with Arduino but here we connect directly. It can read RF-ID card under 10 cm distance and it operate on 125 kHz frequency. Pin no. 8 and 9 - These pins are ANTENNA pin. These pins are used when we want to increase the distance of scanning RF ID card.[7]

GSM Module:



With the help of gsm module The OTP is generated in mobile. It work as a path between RF ID and OTP, the communication between this two is done with the help of gsm module[9].

4*4 matrix Keypad:

Initially all switches are assumed to be released. So there is no connection between the rows and columns. When any one of the switches are pressed, the corresponding row and column are connected (short circuited). This will drive that column pin (initially high) low. Using this logic, the button press can be detected. The colors red and black is for logic high and low respectively. Here are the steps involved in determining the key that was pressed.[8]
Step 1: The first step involved in interfacing the matrix keypad is to write all logic 0s to the rows and all logic 1s to the columns. In the image, black line symbolizes logic 0 and red line symbolizes logic 1.
For now let us assume that, the circled key is pressed and see how the key press can be detected by a software routine.
Step 2: Now the software has to scan the pins connected to columns of the keypad. If it detects a logic 0 in any one of the columns, then a key press was made in that column. This is because the event of the switch press shorts the C2 line with R2. Hence C2 is driven low. Note: color of the lines indicate the logic values they return.
Step 3: Once the column corresponding to the key pressed is located, the next thing that the software has to do is to start writing logic 1s to the rows sequentially (one after the other) and check if C2 becomes high. The logic is that if a button in that row was pressed, then the value written to that row will be reflected in the corresponding column (C2) as they are short circuited. Note: color of the lines indicate the logic values they return.
Step 4: The procedure is followed till C2 goes high when logic high is written to a row. In this case, a logic high to the second row will be reflected in the second column.

16*2 LCD display:

In 16*2 Lcd display is 16 pin.pin1 and2 is ground and vcc .It is connected to Arduino mega for power supply Pin no 3 is VEE it is used for contrast adjustment the best way is to use variable resistor such as a potentiometer.The output of the potentiometer is connected to this pin VEE. Pin no 4 is Rs Register select there are two types of register 1)com- mand register 2) Data register. The command register stores the command instruction given to the lcd.Data register stores the data to be displayed on the LCD.when Rs=1 data register is selected.when Rs=0 command register is selected.pin no 5 is read/write pin.when it is high it will read data.when it is low it will write data.pin no 6 is enable pin it is used for send data to data pin when high to low clock pulses is given Pin no 7 to14 is 8 bit data pins here we use only 4 bit data pins for dis- playing the data.pin no 15 and 16 are LED+ and LED- pin.they are use for backlight.it is connected to arduino mega for power supply[9].

VI.RESULT DISCUSSION

The results from the research work support the set objectives.The findings indicate that a biometrics based fingerprint authentication system in ATMs could be deployed and implemented in Banks and other Point of Sale terminals. The most

common problem as with any other biometric method is that it may present some rejection problem because they involve human and biological characteristics. That means even a person whose fingerprint has already been recorded may not be recognized. This is called “false rejection” and happens with any technology and manufacturer [9]. This problem rarely occurs (below 0.1% of the cases), but it is important to keep this possibility in mind during the implementation, so that adequate precautions could be taken. However, many false rejections happen because of an error during registration, with the capture of a partial fingerprint, usually the tip or side of it. That increases the possibility of rejection, because the next time the fingerprint will be read, the captured image may be a different one, not registered yet. A correct registration is the best way to avoid false rejection. . From the point of view of image quality, the best fingers to use on a fingerprint reader or sensor are the index, middle and thumb fingers . In comparison to the other biometric methods, the fingerprint is the cheapest, fastest, most convenient and most reliable way to identify someone. That is why fingerprint alone has two third of the biometric identification market. And the tendency, due to scale, easiness and the existing foundation, is that the use of fingerprint will increase. Cars, cell phones, personal digital assistants (PDAs), personal computers and dozens of products and devices are using fingerprint. The veritable platform formed by the findings of this study could be exploited by future research work in area of implementing biometrics based access control system.

VII.LIMITATIONS

1.Due to multiple authentications the system is time consuming at the initial stage.
2.Also as the multiple users share the same bandwidth there is always a chance of signal interference in gsm technology and it also suffers from network problems in remote areas.
3.The RFID card used may be affected by the environmental factors.

VIII.CONCLUSION

Automatic Teller Machines have become a mature technology which provides financial services to an increasing segment of the population in many countries. Biometrics, and in particular fingerprint authentication, continues to gain acceptance as a reliable form of securing access through identification and verification processes.This paper identifies a high level model for the modification of existing ATM systems to economically
incorporate fingerprint authentication system. It shows that the fingerprint is a feasible method for identifying users and the RFID card is an additional feature of our project which can help the other close aides of the user to carry out the transactions easily.

IX.REFERENCES

1] NSTC-- National Science and Technology Council
(FINGERPRINTREC) http://www.nstc.com
2] H.Omar, R.Din, and H. M. Tahir, Journal of ICT, 2(1),
February, 2002
3] Ms. Archana S. Shinde, Prof. Varsha Bendre, “Fingerprint Matcher
System" , Paper Published in IJSER Volume 5, Issue10, October 2014
Edition (ISSN 2229-5518).
4] European ATM Security Team, “European ATM Security
Team”, Diebold, Incorporated 2006,
http://www.diebold.com/rd/whitepapers/atmfraud&security.pdf
5] A. Jain, R. Bolle, and S. Pankati, “Biometrics: personal
identification in networked society”, Kluwer Academic
Publishers, 1998
6]wikipedia