TWO FACTOR AUTHENTICATION FOR HIGH SECURITY BANKING ATM USERS

[1]S.Naveen Kumar, [2]A.Mohammed Arif, [3]S.Naveen Kumar and [4]Mr.S.VijayMurugan,M.E.,(PhD.),

[1,2,3]Student – Department of ECE, Adhiyamaan College of Engineering, Hosur, India

[4]Assistant Professor – Department of ECE, Adhiyamaan College of Engineering, Hosur, India

ABSTRACT

The growth in electronic transactions at ATM has been increasing and so there is demand for fast and accurate user identification and authentication. Generally user has to provide two means of identification, one of which is a physical token, such as card and other of which is something memorized constant code. This work aims at improvising the security and authenticity of ATM. Instead of memorized code here in this work we generate random OTP (One Time Password) which is sent to mobile through GSM model and RF-ID reader to receive the user information. At the time of wrong input code (3 times) we would transmit video to control station via camera, as there would be more monitors to display it is made as in this way that if the person is trying any defaulting it would switch on monitor which need authentication and also when ATM machine is disturbed.

Keywords: ATM, ARM7, GSM modem, RF-ID, Camera, Zigbee.

1 INTRODUCTION

Inventor John Shepherd-Barron installed the world's first automatic cash dispenser at a Barclays Bank branch near London in 1967. The number of installed ATM machine has shown the trend of increasing continuously with the high increasing ratio in the first half of year 2000s, and gradual increase after the year [1]. Especially external ATM machine has been increased continuously. As the technology is growing, autonomous systems are gaining rapid popularity. ATM is the one among the autonomous system in banking services. With an ATM, a customer is able to access several banking activities such as cash withdrawal, money transfer, paying phone and electricity bills beyond the official hours and physical interaction with bank staff. In this aspect, ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. It is a computerized machine designed to dispense cash to bank customers without need of human interaction; it can transfer money between bank accounts and provide other basic financial services such as balance enquiries, mini statement, withdrawal and fast cash transfer among others.

PIN (Personal Identification Number) or Password is one of the important aspect in ATM which is commonly used to secure and protect financial information of customers from unauthorized access[2].Primary step of the functioning is the insertion of the ATM Card into the system. This process is followed by the phase that requests for the PIN of the ATM card inserted.

PIN (in India) is generally four digits that are kept in secrecy by the user. This PIN entry determines the transaction to continue or abandon. Also the three times wrong entry of a PIN would lead to the blocking of the ATM card [4] in sensing a possible fraudulent transaction. Once the ATM PIN number is successfully validated, the user is given options regarding the financial services to be performed. Once on selection of a particular financial service, the service is rendered by the ATM and the transaction is said to have come to an end. This is considered as entry level secure way to access the account information.

On the other side crime for financial organization, the cases of theft and robber have very high proportion of over 90% and the crime for the ATM has been increased because of the external ATM has been increased and it is always exposed to the crime [5]. Thus there is a need to develop the security part of the system. Considering several issues, in this work instead of PIN we generate OTP. The purpose of generating OTP is to achieve better identification with high security as during each transaction it asks for random password. Security of ATM center is also important for that there is a MEMS sensor which senses any temperature changes. This sensor identifies if anyone trying to do malpractices using the machine. This project aims to overcome the problems facing in ATM section and to increase the security wise authentication for both user and bank authorities.

2 EXISTING SYSTEM

Automated Teller Machine is one of the convenient way that was brought into this world as a replacement to the old banking system of the cash withdrawal. The main reason behind the invention of this system is to provide cash to the customers of the bank at the lightning speed when needed. The major sequential operations [4] that are currently involved in the ATM services are as follows,

1. Inserting or Swiping the ATM card in the respective ATM Terminal.
2. Entry of the secret Personal Identification Number (PIN) with respect to the ATM card by the card holder.
3. Transaction selection (Financial aspects like balance enquiry, withdrawal, deposits).
4. Completion of the transaction and termination of the session.

So, these are the factors incorporated into this system with the help of the ATM card that is provided to the each customer. Several model to replace this methodology have suggested mainly to improve the security factor. Some of those includes biometric authentication like (fingerprint, handshake), Random password generation using GSM[4] and reply for the message[7] to authenticate, etc. Though this multifactor authentication improvises the security but the method becomes more complex which results in taking more time and also sometimes this biometric becomes annoying to the customer who needs to accept his banking requirements through his colleague.Thereis need for reduction in the complexity of the transaction associated with that of the ATM.This two factor authentication can solve the issues faced in existing methodologies [8]. Here

the major considerations to improve safety and security include User authenticity, ATM machine and Bank authority.

Considering the above defined factors in this work we have concentrated on each step thereby reducing the system complexity which the existing system has. Here we will make you clear what the actual processing steps in our system. First the user is about to swipe the card to indicate he/she is having an account in bank. We are not actually asking for mobile number to enter as well-known fact each person has mobile phone and the number is given while opening an account so we store that in database and random OTP is sent to that number. Now user has to enter the OTP that he received in his mobile to continue the transaction. Suppose if entered OTP is wrong for three times then the camera functionality is made in the way that it sends the video clips to the control room as it display in the monitor. And also sensors placed in machine used to keep the ATM safe from robbers.

3 PROPOSED SYSTEM

Since all the population who have ATM have also mobile number registered officially with the finance institution by which our technique is being proposed. As the card is swiped machine will get the corresponding mobile number from the database and OTP is sent to the person. As the OTP is time dependent so that user is supposed to enter the received number before 5 minutes. If the person enters the password wrongly for three times then the video is transmitted to the control room as there will be more monitors to display it is made in that way it will switch the particular monitor on which needs authentication. Changing of mobile number is to be informed to the bank so that number can be updated in database from the next time OTP will received to the new number. Here in this work the UI and Flow execution have developed in java platform.

Java is the programming language that we used to execute the processing steps. From the accepting of card to the delivery of money, GUI, security precautions whole steps we have well developed coding in java and there will not be any delay in processing duration.

4 HARDWARE DESCRIPTION

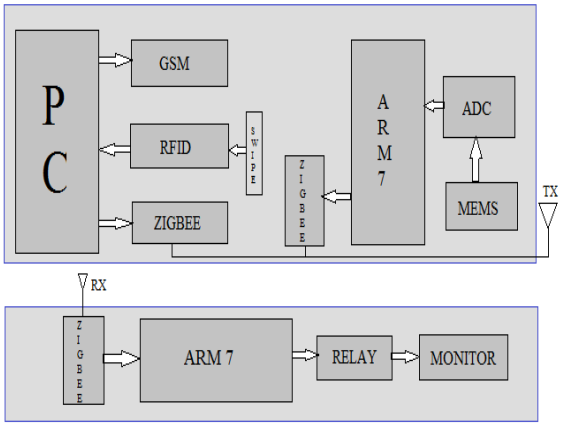

Fig 4.1: Block Diagram

The block diagram describes that the dual security of ATM which involve Radio Frequency ID and the reader which would get the basic details like the mobile number of the person using it. Then an OTP is sent to his mobile which is dynamically generated. For further transactions the person has to provide that OTP. Java platform based User interface and the desktop environment is developed to receive the RFID card details and the database is created to get the details of the person using the card. GSM modem is used to send the message to the user's mobile. AT commands are used to communicate with GSM modem and the dynamically generated OTP is sent through GSM modem to the user's mobile. If there is a chance that the user is using the same card thrice and not entering the OTP correctly monitor would be switched ON at the Control Station. If there is any changes in reading from output of ARM7 that observed from MEMS sensor which is converted to digital through ADC monitor would be switched ON at the Control Station. As there would be more monitors for display it is made in this was that if the person is trying any defaulting it would switch on the monitor which needs attention. Either it would be automatic or human interfere. For this video transmission to the control room we use ZigBee and Relay.

4.1 ARM7:

It is a 16/32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package, 16 kB on-chip Static RAM, 128/256 kB on-chip Flash Program Memory, 12 Mhz crystal on socket128-bit wide interface/accelerator enables high speed 60 MHz operation[7] as shown in fig 4.2.

In our project it gets the input from ADC through MEMS sensor and output to ZigBee at transmitter side, at receiver side it gets input from ZigBee and output is connected to Relay.

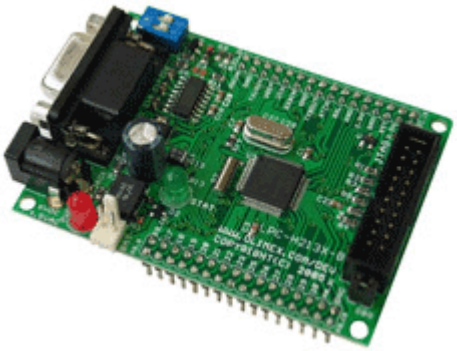

Fig 4.2: ARM 7

4.2 GSM Modem:

A GSM modem accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. GSM modem interfaced to PC as shown in fig 4.3 though Portfolio serial port and functions just as mobile phone to send a message to a number for which it has to send

In our project it is used for transmitting 4 digits OTP which is generated in java program to user's registered mobile number.

Fig 4.3: GSM Modem

4.3 ZigBee:

Itis a Transreceiver module which provides easy to use RF communication at 2.4 GHz. It can be used to transmit and receive data at 9600 baud rates from any standard CMOS/TTLsource[3].

In our project we use three ZigBee, two at transmitter side one at receiver side. At transmitter side one ZigBee as shown in fig 2.4 is to get the wrong user identity in ATM room and another is to get the unauthorized activity using machine. At receiver side it gets the transmitted signals from transmitter side and connected to ARM7 at receiver side

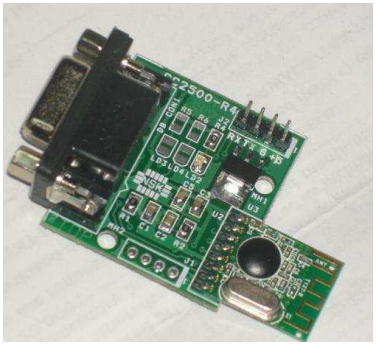

Fig 4.4: ZigBee

4.4 Relay:

It is a components which allow a low-power circuit to switch a relatively high current on and off, or to control signals that must be electrically isolated from the controlling circuit itself.

Here in our project Relay as shown in fig 4.5 is used to switching the monitor ON/OFF according to the input it getting from ARM7 on receiver side

Fig 4.5: Relay

4.5 RFID Reader:

It is a fast and reliable means of identifying objects. There are two main components: The Interrogator (RFID Reader) which transmits and receives the signal and the Transponder (tag) that is attached to the object. Radio waves are the carriers of data between the reader and tags. The approach generally adopted for RFID communication is to allocate frequencies depending on application. The frequencies used cover a wide spectrum.

In our project RFID which is 125 KHz is used to get the unique identification key from the user in such a way no information about the user can be traced by using this card by hackers.

Fig 4.6: RFID

4.6 Camera:

It is used to take continuous video clips and to send the video to control room

5 SOFTWARE DESIGN

5.1 Java:

Java programming platform is preferred to design our project. We design the GUI for our project using swing concept, Connecting GSM using comm.jar, connecting RFID using RXTXcomm.jar and ZigBee.

5.2 NetBeans IDE:

NetBeans IDE is the official Integrated Development Environment for java8. It is much more than the text editor. It gives us the clear overview of entire project files with folders and allows us to well organize the entire codes.

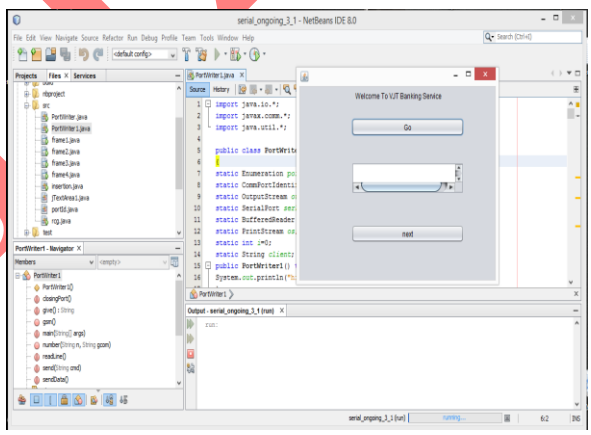

Fig 5.1: Software Display

6 CONCLUSION

ATM being used today are very essential for banking services. As both credit and deposit can be done using ATM, the security factor is important factor on which our project is concentrated. This project has considered both security and reliability. As RFID tag used no information can be hacked, as OTP is generated no password can be guessed, as sensor in machine placed no misbehavior can be tried.

7 RESULTS AND DISCUSSION

The results have been shown out through snapshot of our overall project which includes transmitter module and receiver module.

Transmitter module consist of PC which is connected to GSM, RFID, ZIGBEE through serial port and ARM7 which takes input from MEMS and output to ZIGBEE.Receiver module consist of ARM7 which takes input from receiver ZIGBEE and output is programmed and give it to Relay, which switches the monitor ON/OFF.

Fig 7.1: Snapshot of our Project Kit

REFERENCES

[1]http://en.wikipedia.org/wiki/Automated_teller_machine.

[2] Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani, “ATM Security Using Fingerprint Biometric Identifer: An Investigative Study”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012.

[3] Zigbee and RFID based System Design By Nilima D Thombare, Tukaram D Dongale, Rajanish K Kamnath.

[4] Sivakumar T, Gajjala Askok, k. Sai Venuprathap, "Design and Implementation of Security Based ATM theft Monitoring system", International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 3, Issue 1 (August 2013) PP: 01-07.

[5] M.R.Dineshkumar, M.S.Geethanjali, R.Karthika, M.Nagaraj, N.Vijayanandam," Protected Cash Withdrawal in Atm Using Mobile Phone", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 4 April, 2013 Page No. 1346-1350.

[6] Mrs.S.P.Balwir, Ms.K.R.Katole, Mr.R.D.Thakare, Mr.N.S.Panchbudhe, Mr.P.K.Balwir, Secured "ATM Transaction System Using Micro-Controller", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014 ISSN: 2277 128X.

[7] Khatmode Ranjit P1, Kulkarni Ramchandra V2, Ghodke Bharat S3, Prof. P. P. Chitte4, Prof. Anap S. D5, "ARM7 Based Smart ATM Access & Security System Using Fingerprint Recognition & GSM Technology", International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 2, February 2014) 856.

[8] Srivatsan Sridharan, Gorthy Ravi Kiran, Sridhar Jammalamadaka, "Improvising Authenticity and Security of Automated Teller Machine Services", International Journal of Computer Science and Mobile Computing, A Monthly Journal of Computer Science and Information Technology ISSN 2320–088X IJCSMC, Vol. 3, Issue. 2, February 2014, pg.666 – 674

[9] S.Vijay Murugan, K.G.Lavanya "An Intelligent Environmental Novelty System Using Mobile Technology For Warfields",International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 10, October – 2013 IJERTIJERT ISSN: 2278-0181

[10] ARM System-on-chip Architecture by Prof Steve Furber

[11] S.M. Shamsheer Daula Dr.K.E Sreenivasa Murthy Asst.Professor Principal, G.Pulla Reddy Engineering College SKTRMC,Kondair. Kurnool,A.P India. Andhra Pradesh,India, "An Embedded ATM Security Design using ARM Processor with Fingerprint recognition and GSM", International Journal of Advanced and Innovative Research ISSN: 2278-7844.

[12] Concepts of Java Programming and usage available online at www.freejavaguide.com