IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

RFID & Mobile Fusion for Authenticated ATM Transaction

Nishigandha S. Deshmukh[1], J. N. Mohite[2]

PG Scholar, E&TC Department, MSSCET, Jalna, Maharashtra, India[1]

Assistant Professor, E&TC Department, MSSCET, Jalna, Maharashtra, India[2]

Abstract: In this paper we report on a new approach for enhancing security and privacy. In the meantime, it is more difficult to secure the privacy of a mobile RFID-enabled device with the change in consumption habits, trending practices have changed from the traditional to the entity stores patterns. They have gradually transformed into the network of online shopping patterns, and most of online shopping is completed by the transaction through the credit card. However, with the traditional trading protocol, the credit card number and code (three digit codes), can be faked by cardholders to carry out all transactions. When the card is lost, the system cannot detect the implementation of the transaction, whether it is by the legitimate credit card holder or not. The main objective of this project is to develop an embedded system, which is used for security applications. In this security system we give access to the authorized people through the RFID tags and mobiles. This project can provide security for the industries, companies, etc. This security system gives information about the authorized and unauthorized persons.

Keywords: DTMF Decoder, GPS, LCD, Keypad, Microcontroller, RFID, Voice synthesizer.

I. INTRODUCTION

A secure authentication protocol has been proposed to provide information to an authorized entity, which implements recognition technology in the insecure communication channel even for the communication between the database and the reader. Most of the previous works assume the communication channel between an RFID reader and its backend server is secure and concentrates only on the security enhancement between the RFID tag and RFID reader. However, once RFID reader modules gets extensively deployed in consumers' handheld devices, the privacy violation problems at reader side will become a matter of great concern for individuals and organizations . If the future communication environment for RFID systems is in wireless it increases the insecurity. We need to achieve security, anonymity, availability, and protection of information being stolen or tampered with. Under such infrastructure, handheld device, such as mobile phone, embedded RFID reader modules will be situated everywhere and operated with many RFID tags in various RFID application systems.
This project can provide security for the industries, companies, etc. This security system gives information about the authorized and unauthorized persons. Primarily, the two main components involved in a Radio Frequency Identification system are the Transponder (tags that are attached to the object) and the Interrogator (RFID reader).In this

Project RFID with GSM will used to provide the complete security. In this project, when the card is brought near to the RFID module it reads the data in the card and make a call to the user. The data on the call is compared with the data in the program memory and displays authorized or unauthorized message. The door opens for an authorized person, closes for an unauthorized person; it alerts the persons. This call is made with the help of GSM technology. GSM technology is worldwide this is the main advantage of our project.

II. REVIEW ON LITERATURE

We had gone through the various papers and research work it seems that previous work assumes that the communication channel between an RFID reader and its server is secure and concentrate only on the security improvement between the RFID tag and RFID reader But the privacy destruction problems at reader side will become a matter of great concern for individuals and organizations, once RFID reader modules gets extensively deployed in consumers' handheld devices.

Ref [2] discussed security and privacy issues. Unprotected tags may be susceptible to eavesdropping, traffic analysis, spoofing or denial of service attacks, approaches for tackling security and privacy issues like Password Protection on Tag Memory, Physical Locking of Tag Memory, active jamming, and personal privacy.
Ref [3] discussed attacks at physical, network layer and application layer, approach to avoid tag and reader collision using anti-collision protocol like ALOHA, TDM/FDM. Using AT commands only authenticated user can perform transaction.
Ref [4] this paper reported a new approach to defend against unauthorized reading and relay attacks in some RFID applications whereby location can be used as a valid context.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Ref [5] Discussed secure approach via location sensing. If location is matched then trigger the web cam & authenticate the user.

III. BASIC BLOCK DIAGRAM of SYSTEM

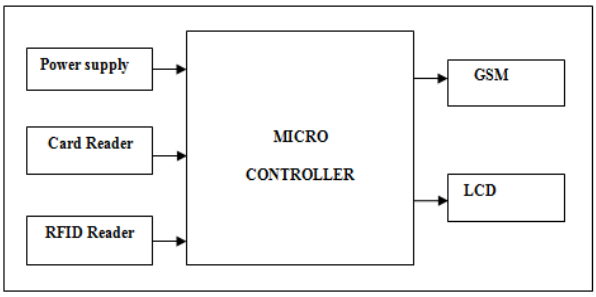

Fig 1 Basic block diagram system

Working principle is as follows:

1. When the RFID card or Debit card brought into the vicinity of the ATM center the reader reads the account number and detail of the card holder.
2. This information is sent to the microcontroller.
3. Call will be generated to the user or card holder, here details are checked for genuineness and confirms weather to precede the transaction or not. This is done with the help of GSM technology.
4. If all this information matches with entered information and information on call then transaction will be successful or fail.

IV. HARDWARE DESCRIPTION

POWER SUPPLY

The microcontroller and its auxiliaries need supply for its functioning. This is derived from the power supply unit. There are two power supply terminals. One of them is for the microcontroller unit and the other is for driving the LCD display. The output of this unit is 5v. It has a step down transformer of 230/15 v rating. The 15 v ac supply is connected to a full wave bridge rectifier. The output of the rectifier is pulsating in nature. So to reduce this effect a smoothening capacitor is provided and the output of this capacitor is connected to two general purpose regulators IC – 7805.

MICROCONTROLLER:

The Microcontroller forms the heart of the project because it controls the devices being interfaced and communicates with the devices according to the program being written. In this project PIC 18f4550 Microcontroller is used. PIC 18f4550 comes under the category of advanced 8 bit microcontroller includes universal serial bus (USB) features. It has 24 Kbytes of Flash Memory. It is 40 pin microcontrollers.

Liquid-crystal display (LCD):

Liquid crystal display is a flat panel display, electronic visual display that uses the light modulation properties of liquid crystals. Liquid crystals do not emit light directly. LCDs are available to display arbitrary images or fixed images which can be displayed or hidden, such as Preset words, digits, and 7-segment displays as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements. In this project 16*2 LCD is used.

GSM:

GSM is a mobile communication modem; it is stands for global system for mobile communication (GSM). The idea of GSM was developed at Bell Laboratories in 1970. It is widely used mobile communication system in the world. GSM is an open and digital cellular technology used for transmitting mobile voice and data services operates at the 850MHz, 900MHz, 1800MHz and 1900MHz frequency bands.

RFID:

Many types of RFID exist, but at the highest level, we can divide RFID devices into two classes:

1. Active tag.
2. Passive tag.

Active tags require a power source i.e., they are either connected to a powered infrastructure or use energy stored in an integrated battery. In the latter case, a tag's lifetime is limited by the stored energy, balanced against the number of read operations the device must undergo. However, batteries make the cost, size, and lifetime of active tags impractical for the retail trade.

Fig 2: Active and passive tags

Passive RFID is of interest because the tags don't require batteries or maintenance. The tags also have an indefinite operational life and are small enough to fit into a practical adhesive label. A passive tag consists of three parts: an antenna, a semiconductor chip attached to the antenna and some form of encapsulation. The tag reader is responsible for powering and communicating with a tag. The tag antenna captures energy and transfers the tag's ID (the tag's chip coordinates this process). The encapsulation maintains the tag's integrity and protects the antenna and chip from environmental conditions or reagents

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

V. SYSTEM BLOCK DIAGRAM

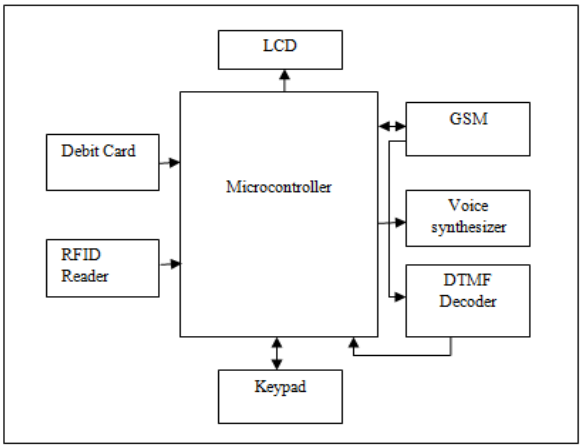

Fig 3: Detail Block Diagram of system

First Debit card or RFID card brought into the vicinity ATM centre. RFID reader reads the details of the card holder that is user's password and amount entered by the user. Radio-frequency-identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. We will use Non magnetic Debit card.

RFID sends parallel data to the microcontroller input. It is then checked with the database present in it. The card number and account number read from the card reaches the microcontroller database. It is crosscheck and mobile number is send to the GSM. Voice synthesizer is an electronic device that combines basic sounds to imitate the speech of a person. Messages are recorded using voice synthesizer. These recorded messages will be played depending on key pressed by the user for example if press 1 voice synthesizer will play "Enter the password".

In this way Interactive voice response system will guide or take sensitive or authenticated details like account number or card number or Debit card pin or secondary password. If all this information matches with entered information and information on call then transaction will be successful or fail. DTMF Decoder determines the key is pressed by the user or card holder. DTMF stands for Dual Tone Multi Frequency. It is used in cell phones, landline phones etc. to identify the key pressed. Corresponding to every row and column of our keypad, there is a frequency associated with it. When a key is pressed, a signal is sent, which is the superposition of sinusoids of the 2 frequencies associated with that key. This signal when decoded, gives us the key pressed. Liquid crystal display displays the information entered by the card holder. 4*4 Keypad is used to enter the information.

VI. ADVANTAGES

1. The every transaction of the account is done with the consent of the customer or card holder.
2. Unworthy persons will not be able to do the transactions.
3. This system can be used worldwide.
4. Has ability to pinpoint location
5. Extremely low error rate.
6. Simultaneous and multiple tags read 10s to 1000s in short time interval.
7. Tags available in range of types, sizes and materials.
8. GSM system used in our project provides quick data communication over long distance also.
9. RFID system helps us to provide the maximum security to authenticate the user

VII. EXPERIMENTAL SETUP

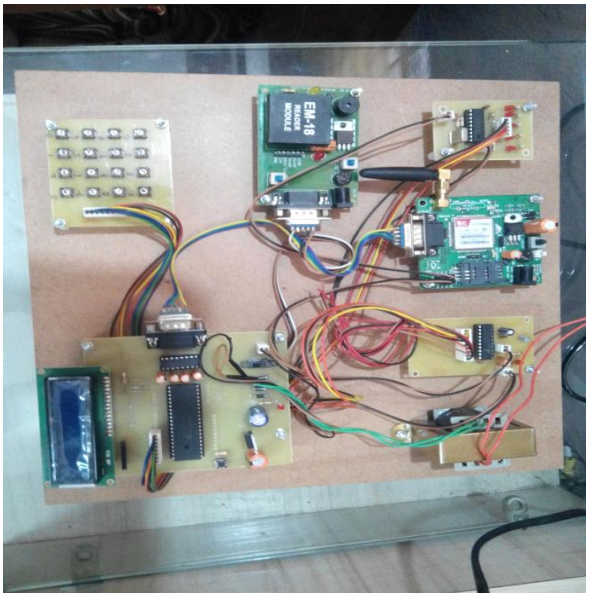

Fig 4: Experimental Setup

GSM, LCD, Keypad, voice synthesizer, RFID Detector are serially connected to the PIC 18f4550 Microcontroller.

VIII. RESULTS

Fig. 5

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Fig 5.1

Fig. 5.2

GSM module will make a call to the user; user will follow voice synthesizer instructions and respond to the instructions. If all this information matches with entered information and information on call then transaction will be successful otherwise it will fail.

This system will provide maximum security than other inventions. In this system double cross check of information will be done.

In one time password system transaction will be made with only respective response YES or No.

Fig 5.3

In Location aware system only Owner will give permission using the one time password. If person is authorized owner will send positive acknowledgement. If person is authorized then login pin will ask. If person is not authorized then owner will send negative acknowledgement If negative acknowledgement then alarm will blow and door lock system will on. This may take a longer time and if the door is locked other users will have to wait for doing transaction.

IX. CONCLUSION

This whole implementation ensures us a secured and authenticated transaction at lowest cost and minimum maintenance. The only thing is that initial cost of RF ID and GSM conversion of the entire system is the required one time investment. The value added service that this system provides increases the credibility of the financial institutions, the banks improves the convenience to its customer. Hence as the world progresses through the inevitable and an indomitable quest for knowledge, the aspect of security bound systems are bound to concede with the growing innovations and obviously more vulnerabilities. Hence our application might well solve the aspect of transaction security to a precise and great extent.

REFERENCES

[1] J.N. Mohite, N.S.Deshmukh "RFID & Mobile fusion for Authenticated ATM Transaction" Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-10, 2016 ISSN: 2454-1362.

[2] The Government of the Hong Kong Special Administrative Region, "RFID Security", Feb 2008.

[3] Kopparapu Srivatsa, Madamshetti Yashwanth, & A.Parvathy, "RFID & Mobile fusion for Authenticated ATM Transaction" International Journal of Computer Applications (0975 – 8887) Volume 3 – No.5, June 2010.

DOI 10.17148/IJARCCE.2016.51165

[4] R. Naveen & G. Sreedhar Kumar "RFID & Mobile fusion for Authenticated ATM Transaction" International Journal OF Professional Engineering studies Volume III/Issue3/SEP2014.
[5] Pooja J. Deshmukh & Bharati Patil "Location Aware and Safer Cards: Enhancing RFID Security and Privacy during Money Transaction" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013).
[6] X. Liu and L. A. Bailey, "PAP: A privacy and authentication protocol for passive RFID tags," Comput. Commun. vol. 32, pp. 1194-1199, 2009.
[7] N. W. Lo and K.H. Yeh, "Novel RFID Authentication Schemes for Security Enhancement and System Efficiency," Lecture Notes in Computer Science, Secure Data Management, vol. 4721/2007, pp. 203-212, 2007
[8] N.W. Lo, Kuo-Hui Yeh, Chan Yeob Yeun, New mutual agreement protocol to secure mobile RFID-enabled devices Information Security Technical Report, Volume 13, Issue 3, August 2008, Pages 151-157S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.
[9] Mikko Lehtonen, Thorsten Staake, Florian Michahelles, and E. Fleisch, "From Identification to Authentication–A Review of RFID Product Authentication Techniques," Printed handout of Workshop on RFID Security—RFIDSec, Springer, 2006.
[10] E.W.T. Ngai, Karen K.L. Moon, Frederick J. Riggins, Candace Y. Yi " RFID research: An academic literature review (1995–2005) and future research directions" International Journal of Production Economics, Volume 112, Issue 2, April 2008, Pages 510-520
[11] Vinay S, Niha Noor Shaikh and Sridhar Aithal, Design of a Smart Stick Prototype Using Goal Oriented Requirements Engineering Methodology International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 29 Jan 2010