



Deployment of NFC for Security Purposes and Efficient Transaction in Real World

Thivya.G, Amutha.C

Department of Electrical and Electronics Engineering, Rajalakshmi Engineering College, Thandalam, Chennai, India

Department of Electrical and Electronics Engineering, Rajalakshmi Engineering College, Thandalam, Chennai, India

ABSTRACT-ATMs are predominantly used all over the world. However, the safety of any money transaction is always a concern, no matter how many technologies are developed to protect the transaction. The idea of this project is to develop the prevention of theft of the ATM card and to control the usage of the ATM card by unauthorized person. Conditional security is provided with protocol data unit. The additional feature of this project is that no transaction can be done without the knowledge of the respective card holder for the cause that NFC transactions are being implemented. Whenever the transaction has to be done, the RFID card is inserted inside the ATM machine and NFC devices are made to interact with some of the legacy systems. Granting that both RFID and NFC device is found to be accurate, a message is received to the mobile phone of the rightful proprietor with a pin number of four digits. In case of password being correct it moves on to the next level of money transaction, asking for the money withdrawal. Scenario like, the password is found to be defective, next in order of time, the image of the person is captured and the passage out will be locked.

KEYWORDS – NFC (Near Field Communication), ATM (Automated Teller Machine), RFID (Radio Frequency Identification).

1.INTRODUCTION

Near Field Communication (NFC) is based on a short-range wireless connectivity, designed for simple and safe interaction between electronic devices. It is easy to use wireless communication interface for few centimetres. Connection between two devices is established just by holding the devices close to each other or by touching them together. NFC traces its roots back to Radio frequency identification(RFID).[1-5] RFID is the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purpose of automatic identification. Some tags require no battery and are powered and read at short ranges via magnetic fields (electromagnetic induction). Others use a local power source and emit radio waves at radio frequency. The tag contains electronically stored information which may be read from up to several meters away. It was jointly developed by Sony and Philips. It is a wireless communication technology based upon 13.56 MHz. It is designed for read/write transactions with a very short range operating distances up to a few centimetres (less than 10cm). NFC offers a baud rate of 106 kbps to 424 kbps. At the transaction only two participants can be involved – one transmitter (initiator) and one receiver (target).[3]

There are three main use cases for NFC,

Card Emulation: the NFC device behaves like an existing contactless card.

Reader Mode: the NFC device is active and read a passive RFID tag.

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 2, April 2014

P2P Mode: two NFC devices are communicating together and exchanging information.

Plenty of applications are possible, such as:

- 1) Mobile ticketing in public transport — an extension of the existing contactless infrastructure.
- 2) Mobile payment — the device acts as a debit/ credit payment card.
- 3) Smart poster — the mobile phone is used to read RFID tags on outdoor billboards in order to get info on the move.
- 4) Bluetooth pairing — in the future pairing of Bluetooth 2.1 devices with NFC support will be as easy as bringing them close together and accepting the pairing. The process of activating Bluetooth on both sides, searching, waiting, pairing and authorization will be replaced by a simple "touch" of the mobile phones.

Rest of the paper is organized as follows: Section II explains the system model of NFC based ATM machine and its working principle. Design flow of the ATM machine is described in section III. Simulation results are given in section IV. Finally conclusions are presented in section V.

II. SYSTEM MODEL

Figure 1 shows the overall block diagram of the NFC in ATM machine.

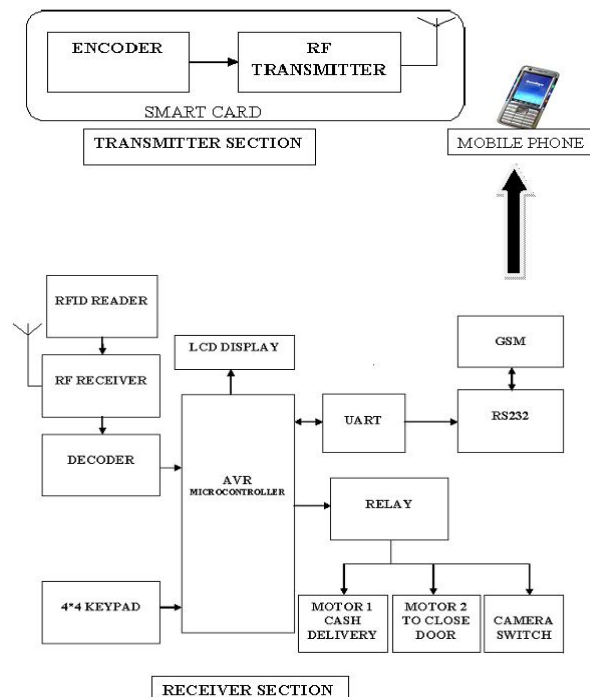


Fig 1. Block diagram of NFC based ATM machine

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

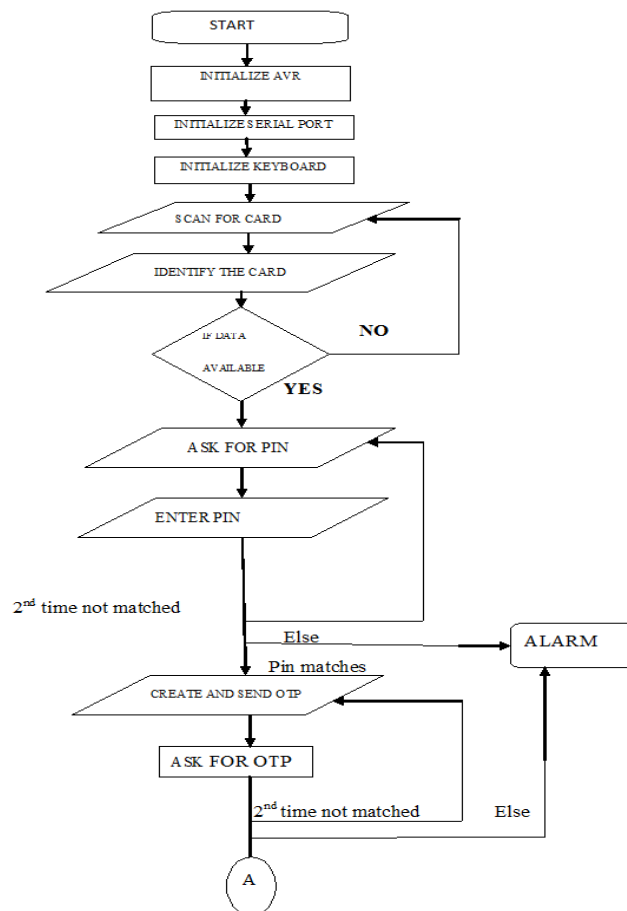
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 2, April 2014

The block diagram consists of two sections such as the transmitter and the receiver section along with a mobile phone and a GSM module. The transmitter section is the encoder with a RFID tag embedded in the ATM card.

The receiver section is the ATM machine which accepts the data from the transmitter section and verifies the data present inside it. If the data present are correct, then the machine asks for the pin number of the card holder then provides the OTP to the mobile of the cardholder through GSM technology. If the input data are correct then the transaction occurs and the image of the person is captured. If the data are incorrect then the passage out door is locked and an alarm is triggered.

III. DESIGN FLOW



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 2, April 2014

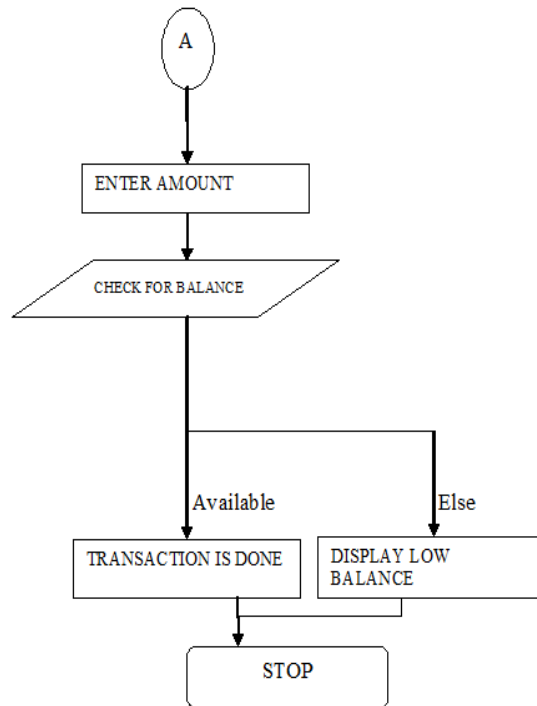


Fig 2. Design Flow of ATM transaction with NFC

The design flow of ATM machine is explained with the flowchart. The AVR, serial port and the LCD are initialized. The card is scanned, the pin number and the password are verified then a onetime password is generated to the mobile of the user. After entering the onetime password, transaction starts to proceed. If the password and the pin number goes wrong for more than three times a buzzer is triggered. If the available balance is too low for transaction a message is displayed in the LCD indicating the status.

VI. SIMULATION RESULTS

The simulation is done using Proteus and AVR studio software. Input variables are obtained using all the peripherals of the controller. The C code for processing of the AVR is compiled into hex code with AVR studio and fed into the AVR microcontroller block of the Proteus software.

The coding of the program is written in the embedded C language and it is debugged. After debugging, the hex file of the code is generated. The blocks of the system is placed in the platform of the Proteus Virtual System Modeling (VSM), which combines mixed mode, SPICE circuit simulation, animated components and microprocessor models to facilitate co-simulation of complete microcontroller based designs.

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 2, April 2014

After placing the blocks connections are made and the corresponding generated hex file is loaded into the microcontroller. of the block and made to run. The instructions to be followed are provided with the LCD display of the Proteus platform. The controller used in this section is the AVR atmega16.

A specified card number is entered in the simulation window to start the operation. When the card is been detected, the display in the LCD screen will ask for the pin number of the card. The pin number has to be typed in the keypad interfacing of the system. If the pin detected is correct, it generates the onetime password, which is displayed in the virtual terminal window. Then the LCD display will display command for entering the generated onetime password. The password is entered with the help of the keypad in the proteus work platform. If the created password matches with the once generated then it will display the transaction occurs else an error message is displayed in the LCD screen.

If the card number provided is not correct, the LCD displays a message with the command “insert card”. If the provided pin number or the onetime password entered in the keypad is wrong then the machine provides three chances. During transaction, the machine asks for the amount to be withdrawn from the machine. If the amount is lesser than the maximum then transaction occurs, else a “low balance” message is indicated.

When the amount is entered, then the debited amount and the balance is shown and the transaction is completed. This step is shown in the Figure 3 and Figure 4.



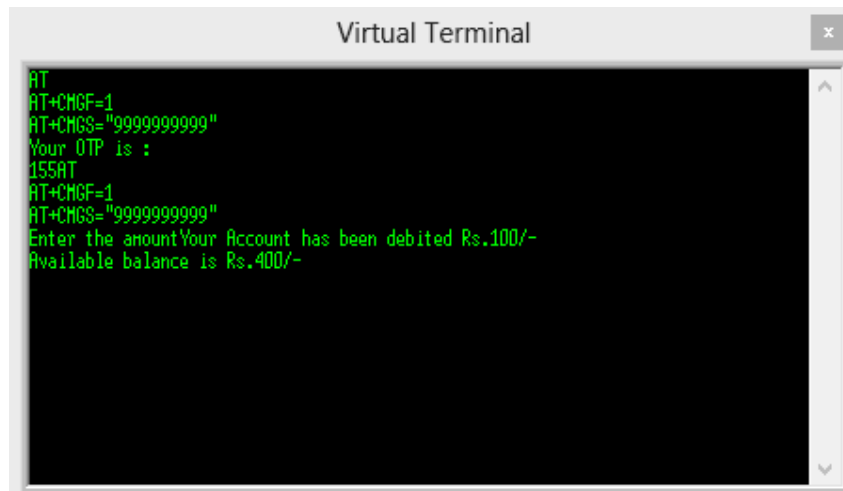
```
Virtual Terminal
AT
AT+CMGF=1
AT+CMGS="9999999999"
Your OTP is :
155RT
AT+CMGF=1
AT+CMGS="9999999999"
Enter the amount
```

Figure 3 Virtual Terminal

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 2, April 2014



```
Virtual Terminal
AT
AT+CMGF=1
AT+CMGS="9999999999"
Your OTP is :
155AT
AT+CMGF=1
AT+CMGS="9999999999"
Enter the amountYour Account has been debited Rs.100/-
Available balance is Rs.400/-
```

Figure 4 Virtual Terminal after final output

V. CONCLUSION

This project deals with the design and implementation of NFC based secure transaction system in ATM machines. This system consists of two modules, the transmitter and the receiver module in order to provide high end security for the ATM card users and the service providers. The password for transaction is send to the cardholder's mobile phone with the help of GSM technology, which is an added advantage. This increases the high usage of smart cards with radio frequency communication between the target devices

REFERENCES

- [1] Hasoo Eun, Hoonjung Lee, Heekuck Oh, Member "Conditional Privacy Preserving Security Protocol for NFC Applications", *Proceedings of the 2013 Research Challenges in Computer and Communication Engineering*, pp 153-160.
- [2] Rashid,R.A. ; Mahalin,N.H. ; Sarijari,M.A. ; Abdul Aziz,A.A."Security system using biometric technology: Design and implementation of Voice Recognition System(VRS)", *proceedings of the 2008 Proceedings of the 2009 Research Challenges in Computer and Communication Engineering*, pp 898-902.
- [3] Madlmayr.G, Langer.J, Kantner.C, Scharinger.J. "NFC Devices; Security and Privacy", *Proceedings of the 2009 Research Challenges in Availability,Reliability and Security*,. pp 642 - 647
- [4] Ghiron.S.L, Sposato.S, Medaglia. C.M. Moroni.A,"NFC Ticketing: A Prototype and Usability Test of anNFCBased Virtual Ticketing Application", *Proceedings of the 2009 Research Challenges in Near Field Communication*,. pp 45-50.
- [5] XiongYuning,"Research on NFC and SIMpass Based Application", *Proceedings of the 2009 Research Challenges in Management and Service Science*,. pp 1-4.
- [6] Francis.L, Hancke.G, Mayes.K, Markantonakis. K."A Security Framework Model with CommunicationProtocol Translator Interface for Enhancing NFC Transactions", *Proceedings of the 2010 Research Challenges in Telecommunications*,. pp 452 – 461.



ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 2, April 2014

- [7] Ok.K , Coskun.V, Aydin.M.N, Ozdenizci.B, “Current benefits and future directions of NFCservices “,*Proceedings of the 2010 Research challenges in Education and Management Technology*,. pp 334 - 338.
- [8] Peter. K.J, Nagarajan. G, Glory. G.G.S, Devi. V.V.S,Arguman.S, Kannan,”Improving ATM security via face recognition”, *Proceedings of the 2011 Research challenges in Electronics Computer Technology*,. pp 334 - 338.
- [9] Petrlic.R,”Integrity Protection for Automated Teller Machines”, *Proceedings of the 2011 Research challenges in Trust, Security and Privacy in Computing and Communications (TrustCom)*,. pp 829 – 834.
- [10] Husni. E, Purwantoro. S,” Shopping application system with Near Field Communication (NFC) based on Android”, *Proceedings of the 2012 Research challenges in System Engineering and Technology* .. pp 1-4.