Red Tacton Based Smart Card Security for ATM

Yumna Birjis [1], M M Yusuf [2], Imran Ahmed [3]
[1] *M.S student, Dept. of electrical engineering,UC,Denver, USA*
[2] *Dept. of E&EC,MSRIT,Bengarulu, India*
[3] *Electrical engineer, KSA*

Abstract

This paper proposes RedTacton based smart security card for ATM system. RedTacton is a Human Area Networking technology that uses human body as a safe high speed network transmission path. RedTacton uses minute electric field on the surface of the human body as a medium for transmitting the data. A transmission path is formed at the moment a part of human body comes in contact with RedTacton transceiver. RedTacton transmitter consists of a DTMF encoder which generates both valid and invalid signals and can be transmitted through human body to RedTacton receiver (DTMF receiver) for further processing. In order to enhance the security for ATM cards, RedTacton based smart security card is presented.

Keywords - *ATM, DTMF, HAN, RedTacton (Red-warmth, T-touch, Acton-act on),*

I. INTRODUCTION

The focus on ubiquitous service has brought about the shortening of distances in communication. RedTacton is positioned as the last 1m solution to ultimate close-range communication. Wireless communication creates connections when signals arrive, allowing for easy connections because connectors are unnecessary. However, seen from another aspect, the arriving signals can be intercepted, so security becomes an issue. Wired communication transmits data between two connection points, so interception is difficult and security can be considered to be high.

The self-containment of Smart Card makes them resistant to attack as they do not need to depend upon potentially vulnerable external resources. Because of this, Smart Cards are often used in applications which require strong security protection and authentication. Technology and security are strongly related. Crackers find sophisticated ways to get at supposedly secure data on cards, Manufacturers have to come up with more sophisticated locks and keys on cards, Crackers come up with better techniques to bypass these, thus forming an infinite improvement loop, with both sides driving each other to use and invent better technology. [1]

RedTacton can achieve duplex communication over the human body at a maximum speed of 10 mbps. The RedTacton transmitter induces a weak electric field on the surface of the body. The RedTacton receiver senses changes in the weak electric field on the surface of the body caused by the transmitter .RedTacton relies upon the principle that the optical properties of an electro-optic crystal can vary according to the changes of a weak electric field. RedTacton detects changes in the optical properties of an electro-optic crystal using a laser and converts the result to an electrical signal in an optical receiver circuit. The transmitter sends data by inducing fluctuations in the minute electric field on the surface of the human body. Data is received using a photonic electric field sensor that combines an electro-optic crystal and a laser light to detect fluctuations in the minute electric field. [2]

Using a RedTacton electro-optic sensor, two-way communication is supported between any two points on the body at a throughput of up to 10 Mbps. Communication is not just confined to the surface of the body, but can travel through the user's clothing to a RedTacton device in a pocket or through shoes to communicate with a RedTacton device embedded in the floor. Unlike wireless technologies, the transmission speed does not deteriorate even in the presence of large crowds of people all communicating at the same time in meeting rooms, auditoriums or stores. Because the body surface is the transmission path, increasing the number of connected users directly increases the available number of individual channels. RedTacton can utilize a wide range of materials as a transmission medium, as long as the material is conductive and dielectric, which includes water and other liquids, various metals, certain plastics, glass, etc. Using ordinary structures such as tables and walls that are familiar and readily available, one could easily construct a seamless communication environment at very low cost using RedTacton. [3]

II. BLOCK DIAGRAM OF THE SYSTEM

The block diagram of smart security card system is shown in Fig 1. It consists of RedTacton transmitter, RedTacton receiver, Driver, Microcontroller unit and the Voice bank.

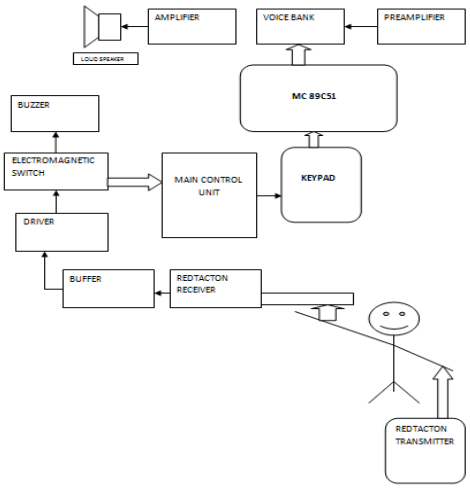

Fig 1: Block Diagram of smart security card system

RedTacton is a HAN; body of human being is used for transmission of signals. RedTacton transmitter consists of a DTMF encoder which generates both valid and invalid signals and can be transmitted through human body through the RedTacton receiver (DTMF decoder) for further processing. [4] In RedTacton receiver by the use of DTMF decoder the transmitted signal is identified.

As the transmitted signal is of very low voltage, buffers and drivers are used to send the received signal to the electromagnetic switch. Electromagnetic switch checks the received signal with the predefined valid code. If an invalid code is received and detected in the switch then the buzzer starts ringing indicating that an invalid card is trying to access the ATM. If a valid code is received, then only the switch sends the signal to the main control unit which is the microcontroller. If microcontroller gets active it switches on the keyboard where predefined options are stored to perform various tasks such as: Enter password, Change of password, New password, etc.

After entering the valid password the voice bank gets activated. In voice bank predefined options with keys are present which guides the user to select appropriate action in the ATM such as: Cash withdrawal, Pin change, Account balance, etc

III. CIRCUIT DIAGRAM AND ITS EXPLANATION

The Circuit Diagram of the system consists of:

- DTMF encoder
- DTMF decoder
- Driver and Buffer
- Main Control Unit

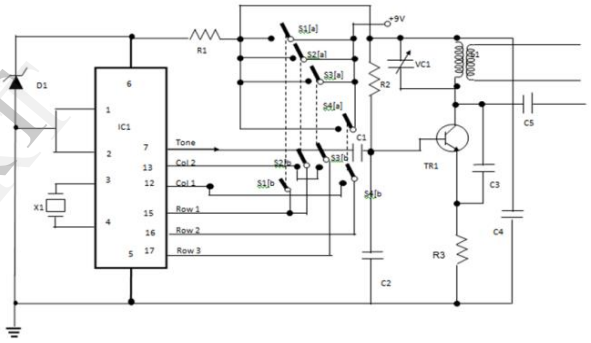

Fig 2: Circuit Diagram of DTMF encoder

The circuit shown in Fig 2 makes use of radio frequency to transmit the control signals for generating the DTMF frequencies, a dedicated IC UM91214B (which is used a dialer IC in telephone instruments) is used here. It uses a quartz crystal of 3.58 MHz.

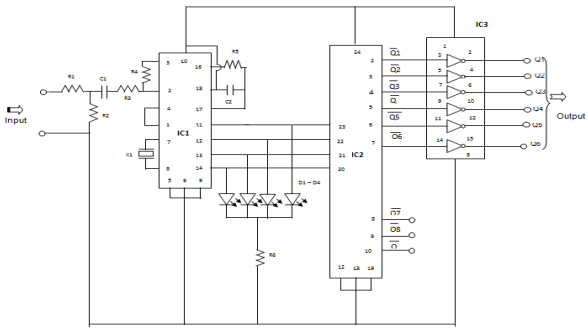

Fig 3: Circuit Diagram of DTMF Decoder

The circuit shown in Fig 3 uses DTMF decoder UM 92870 IC.The DTMF decoder identifies the transmitted signal. If a valid code is received then only the switch sends the signal to the microcontroller, the microcontroller used is 89C51.

IV. HARDWARE AND ITS RESULTS

The model consists of three sections: ATM card section, ATM machine section and Head office section.

4.1 ATM card section

It consists of mainly DTMF encoder which gives the signal out to the copper plates which will be in contact with the human body. Circuit is powered by 9V battery. A switch is included to indicate that different cards can be made to generate different frequencies.

Fig 4: ATM card section

4.2 ATM machine section

It consists of decoder to decode the incoming signals, a microcontroller to interface with LCD display to display the various conditions. This paper proposes a two-level security. Another feature that has been implemented is GSM model that sends a message of Authorization to designated mobile number.

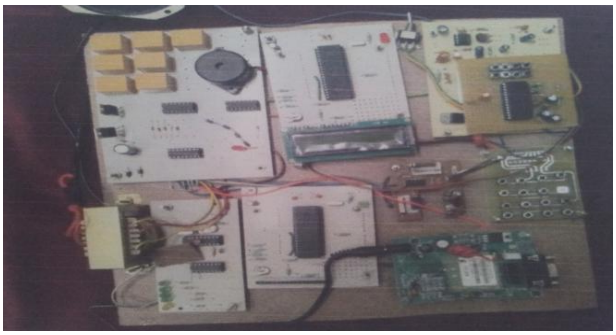

Fig 5: ATM machine section

4.3 Head office section

This section consists of mainly RF receiver that receives the signal from RF transmitter in the ATM machine section and this signal will carry the information as to the person is authorized or un-authorized.

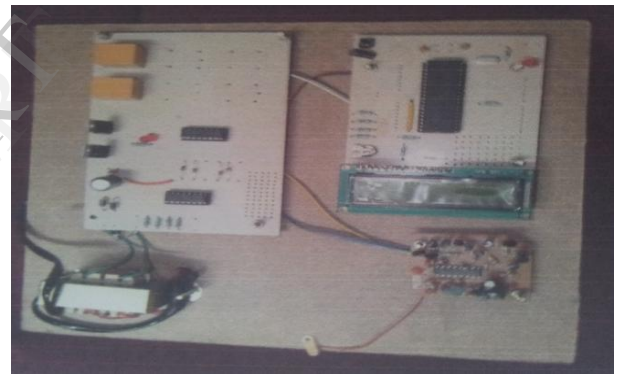

Fig 6: Head Office section

When the switch in the ATM card is put in the unauthorized mode and when the correct codes are received by the DTMF receiver, the switch powers the microcontroller. Then we enter the password using the keypad. The micro controller asking us to enter the password is shown in Fig 7.

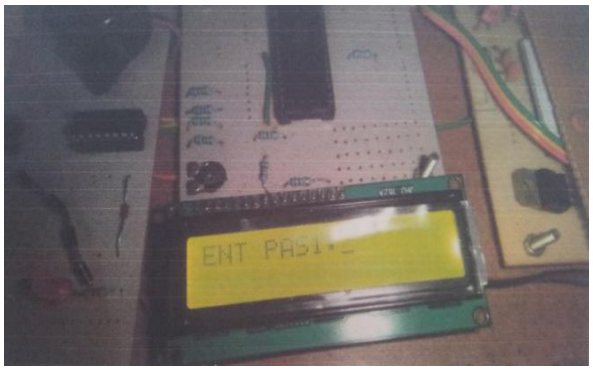

Fig 7: LCD display: 'Enter Password'

The result of the password entered correctly is shown in the Fig 8. The voice bank section gets activated when the correct password is typed in.

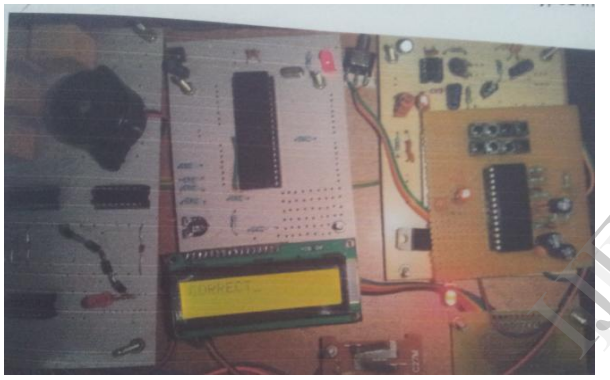

Fig 8: LCD Display: 'Correct'

When the typed password is incorrect, the result is shown in Fig 9.

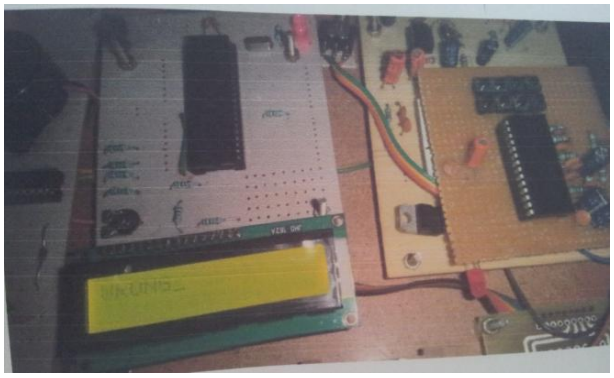

Fig 9: LCD Display: 'Wrong'

The head office receives the signal through the RF receiver and it sends the signal to the microcontroller to display the appropriate message according to the signal from the RF receiver. The microcontroller displays "AUTHORIZED" or "UNAUTHORIZED" depending on the signal.

V. CONCLUSION

The proposed RedTacton based smart security card system for ATM has been implemented successfully and is tested on hardware. Experimental results verify the effective developed operation. When we compare RedTacton with other technologies, it can give a better security since there is no problem of hackers as our body itself acts as transmission medium and can be used more in the fields where there is a need to upgrade the security in times of high theft rate.

REFERENCES

[1] Siu-Cheng, Charles Chang, "*Overview of smart card security*", 1997

[2] Reena Antil, Pinki, Mrs. Sonal Beniwal, "*Red Tacton : A Review*" International Journal of Scientific & Engineering Research, *Volume 4, Issue3*, March,2013.

[3] Bhawik Kotadia , Vibhor Agrawal, "RedTacton", IEEE

[4] J.E Flood ,*Telecommunication switching, Traffic and networks*

[5] Mazidi, *The 8051 microcontroller and embedded system*