GSM Based Implementation of RFID Authentication Protocol Using ARM

Kaustubh U.Pathak, Prof. K.N.Pawar

***Abstract*— RFID is widely used technology to identify the objects with a (EPC) unique electrical code. The purpose of this paper is to create such system that will prevent the hacking of the data base. Implemented system is designed in such a way that it will Activate, Validate and Authenticate the user. In the proposed system XOR operation is conducted within card and predefined string and result is stored in data base. This will further authenticate the desired user.**

***Index Terms*— RFID,LPC2148,LCD,GSM MODEM.**

I. INTRODUCTION

In day to day life where technology plays vital role, a secure and healthy transaction with the help of technology is a major challenge. RFID is a well known phenomenon that we use in case of an authentication protocol, which is nothing but the give and take relation between card readers and card. Whatever the data that reads by the reader is compare with the database and success or failure of the transaction is based on that comparison. But as we know the whole system is connected through internet, the hackers are able to hack the data base which makes ease for creation 0f a cloning of a card. So one can also say that ,the purpose of this paper is to prevent the prevention of such cloning of cards which is possible after implementation of XOR system which we discuss in coming sessions.

II. LITERATURE RIVIEW

Existing system: As mentioned earlier for identifying the objects as well as for maintaining the secure system RFID has been widely used because with creation of an unique electrical code, the identity of the code is valid for the object and system itself. This was studied by Chetan V.R. under the guidance of Dr.V.Venkateswarlu HOD and PRINCIPAL VTU extension centre Bangalore. But certain drawbacks are there in the system which we tried to eliminate.

A) Drawbacks: As we know the whole system is connected online due to which the hackers hack the data base and hence the authentication system is been challenged.

B) How this Hacking can be made possible:

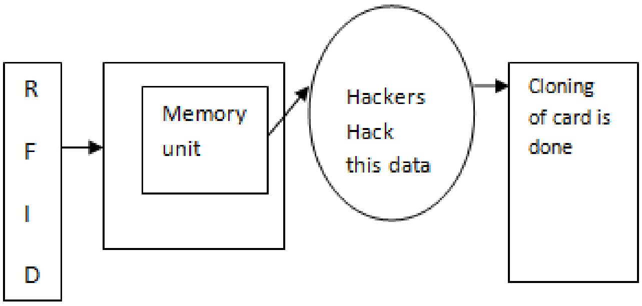


Fig1: Hacking Process

C) How to overcome: This is the purpose of this paper where we are not focusing on reception of data from TAG to RFID or transferring that data to desired person but instead how to secure the information from the hackers.

Here we are using the XOR system here the original card number is XOR with the predefined string and hence the hack data is a result of XORed. So, obviously every time when such XOR result is read by the reader it will creates multiple XOR'S which is differ than the data base. And hence the further transaction is stop.

III. PROPOSED SYSTEM

In this system a predefined string is located in the RFID reader which is in form of code of hex file, once the card number is entered in RFID reader, the number get XORed with the predefined string and result is stored in the data base. In worse case if such XOR result has been hack from the data base and a mirror image or cloning of a card is done still our system is secure. HOW?

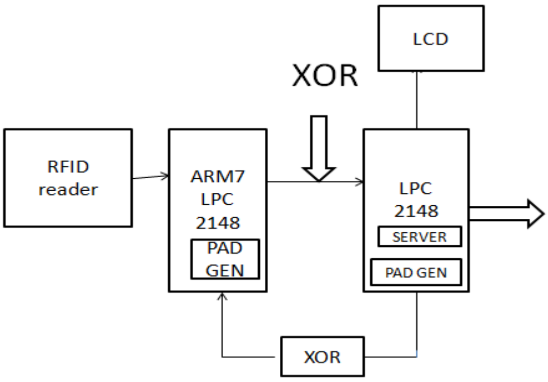


Fig2: Design and implementation of XOR.

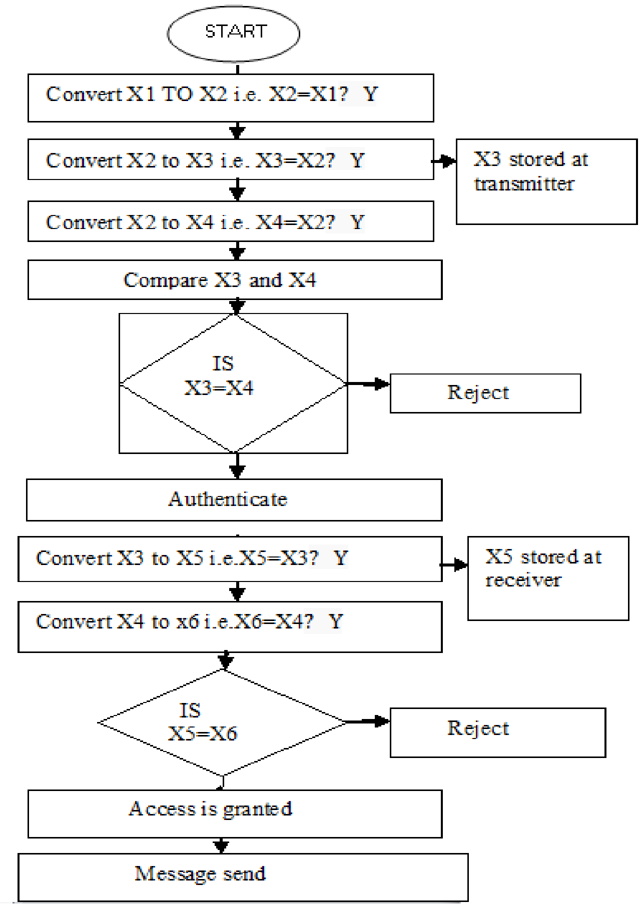
In above case, when card number is XORed with the predefined string in the RFID reader then such XORed number is transferred to ARM 7 LPC2148 where the data from reader is coded using pad gen process. Such XOR data is transferred to another ARM 7 LPC2148 where authentication

Kaustubh U.Pathak, PG Student [COMM.], Dept. of ECE, SSVPS Engineering College, Dhule, Maharashtra, India

Prof. K.N.Pawar, Associate professor, Dept. of ECE,SSVPS Engineering College, Dhule, Mharashtra, India

of received data with the data base is done and success or failure message is send to LCD. If result obtained due to XOR is differ than the data base then RFID doesn't allow card to process. Because of which our system is secure from the clone card as well.

IV. IMPLEMENTATION PLAN


START
Convert X1 TO X2 i.e. X2=X1? Y
Convert X2 to X3 i.e. X3=X2? Y
X3 stored at transmitter
Convert X2 to X4 i.e. X4=X2? Y
Compare X3 and X4
IS X3=X4
Reject
Authenticate
Convert X3 to X5 i.e.X5=X3? Y
X5 stored at receiver
Convert X4 to x6 i.e.X6=X4? Y
IS X5=X6
Reject
Access is granted
Message send

V. DESIGN AND IMPLEMENTATION

1) LPC2148: ARM7TDMI-S based high-performance 32-bit RISC Microcontroller with Thumb extensions .512KB on-chip Flash ROM with In-System Programming (ISP) and In-Application Programming (IAP), 32KB RAM, Vectored Interrupt Controller, Two 10bit ADCs with 14 channels, USB 2.0 Full Speed Device Controller, Two UARTs, one with full modem interface. Two I2C serial interfaces, Two SPI serial interfaces. Two 32-bit timers, Watchdog Timer, PWM unit, Real Time Clock with optional battery backup, general purpose I/O pins.CPU clock up to 60 MHz, On-chip crystal oscillator and On-chip PLL.

2) RFID MODULE: This module consists of RFID passive tag. The RFID reader is of low frequency of 125khz.It do not contain a battery instead power transmitted by reader through radio waves, useful to draw the power.

This tag is sufficiently capable of transmitting information within few cms. The secured information like identification number password can be stored in the memory.

RFID reader is nothing but RF transceiver, as it used the RF energy to activate and power the passive RFID card. The magnetic flux that is created between the card and reader is helpful for receiving the data from the card, which will be further decoded and sent to ARM.

A predefined string is located inside the RFID reader, which get XORed with the card number. One may also ask that, why should not the predefined string is hack?

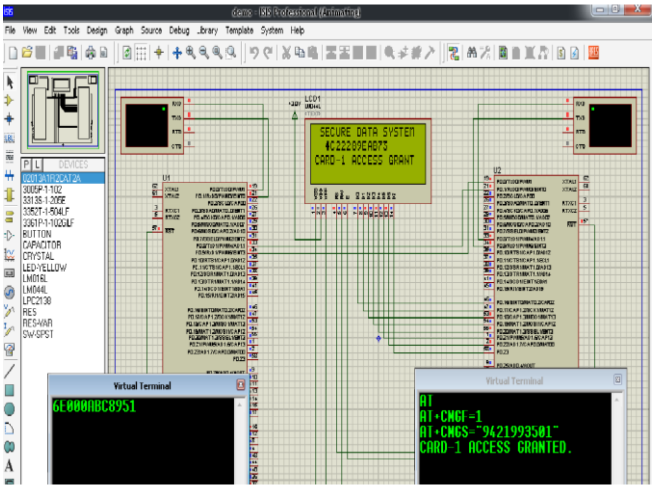
Because as it is stored in the form of code of hex file which is in the uneditable form and after setting it in the RFID reader it itself gats locked.

3) GSM MODEM: During transfer of message to a desired person it's very essential that network may not get blocked. And hence a modem that we used here supports GPRS class 10 for high speed data transfer. For the same purpose UART1 of ARM2 is connected to GSM.

It can works on 900 to 1800 MHz range. It can be easily controlled by AT commands for various operations.

4) LCD:A high level like C can be used for programming as well as interfacing purpose with ARM. Pin no.P16 to P23of the ARM are connected toD0 TO D7 of Port D of the LCD. Where success or failure of the message can be displayed.

VI. TESTING AND RESULTS



```
SECURE DATA SYSTEM
 4C22289EAB73
CARD-1 ACCESS GRANT
```

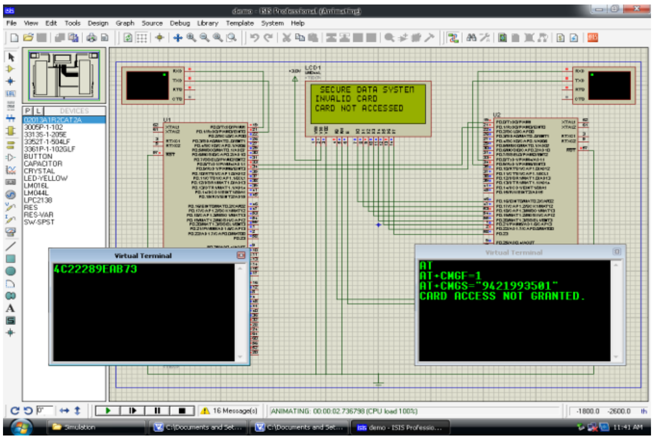
```
6E000ABC8951
```

```
AT
AT+CMGF=1
AT+CMGS="9421993501"
CARD-1 ACCESS GRANTED.
```

Fig3: Authentication of the card

The figure 3 depicts the authentication of the card with respect to data received from RFID card and is declared bit wise for 8 number of RFID cards. This means the digital bits in hexadecimal form stored in each card have been verified with the stored data bits in ARM.

In above case both the card number and data base number gets verified and hence message of card access is generated on the LCD.



```
SECURE DATA SYSTEM
INVALID CARD
CARD NOT ACCESSED
```

```
4C22289EAB73
```

```
AT
AT+CMGF=1
AT+CMGS="9421993501"
CARD ACCESS NOT GRANTED.
```

Fig4:Un Authentication of the card

The above figure shows the successful compilation result using Micro vision compiler software for the embedded C code written for uart communication and also for the LCD and GSM modem for sending sms.

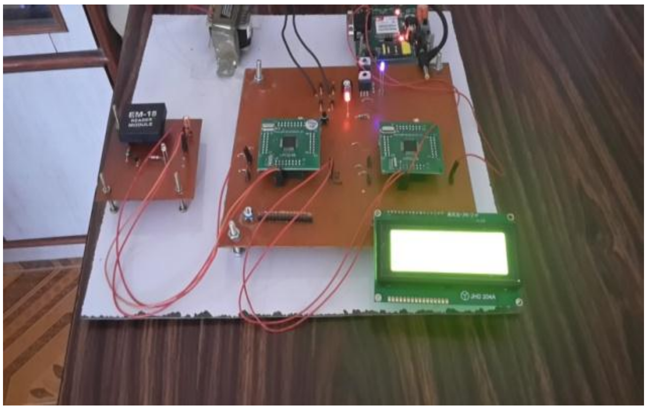


Fig5: Project setup

The fig 5 depicts the project hardware model. It consists of power supply unit; step down transformer, RFID reader, LPC2148, LCD (32bits) display, and GSM modem. The authentication of the card is done after sending the success message on LCD.

From fig 5; The card number which is XORed with predefined string and those bits are transferred to UART0 of ARM1,such bits from UART1 of ARM1 are transferred to UART0 of ARM2 for authentication of the message, which we have seen in fig2.UART1 of the ARM2 is reserved for connecting GSM to avoid the network blockage.

VII. CONCLUSION

Due to the Implementation of XOR scheme, When a predefined string is XORed with the card number, a new result is generated, but in worse case if this result is been hack and clone of a card is done, still transaction is made secure because predefined string located in reader is in uneditble form and it's cannot be hack because it is in code of hex file which is once encoded cannot be decoded.

ACKNOWLEDGMENT

I would like to take this opportunity to express my deep sense of gratitude to my l guide, Prof.K.N.Pawar, HOD Electronics and Communication SSVPS COE,Dhule,for his invaluable inspiration and guidance without which the project work would not have progressed to its present state. I also want to express my thanks to our coordinator Prof.P.V.Baviskar, who provided constant

Encouragement whenever I faced difficulties in my project work. I would finally like to extends my thanks to all the teaching and non teaching staff at SSVPSCOE, Dhule.

REFERENCES

[1] GSM based hardware implementation of RFID authentication system using FPGA. By V.Venkateswarlu, IEEE, Journal of Engineering vol-2,pp.2249-8958,August 2013.

[2] Yu-Jung Huang, Senior member, IEEE, Ching-Chien Yuan, Ming-Kun Chen, Wei-Cheng Lin, and Hsien-Chiao Teng "Hardware implementation of RFID Mutual Authentication Protocol", IEEE Trans. Ind. Electron., vol.57, no.5, pp.1573-1582, May 2010.

[3] R. V. Kulkarni and G. K. Venayagamoorthy, "Particle swarm optimization in wireless-sensor networks: a brief survey," IEEE Transactions on Systems, Man, and Cybernetics - Part C: Applications and Reviews, vol. 41, no. 2, pp. 262-267, 2011.

[4] [38] S. L. Sabot and L. Ali, "The hyper spherical acceleration effect particle.

[5] M. R. AlRashidi and M. E. El-Hawary, "A survey of particle swarm optimization applications in electric power systems," IEEE Transactions on Evolutionary Computation, vol. 13, no. 4, pp. 913-918, 20] .

[6] Mohanavelu.S and Ramya.T, "Secured Authentication Protocol for RFID System Using MOD Scheme", IJSR - INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH,Vol 2,No.5,May 2013

[7] Yu-Jung Huang, Senior Member, IEEE, Wei-Cheng Lin, and Hung-Lin Li, "Efficient Implementation of RFID Mutual Authentication Protocol", IEEE transactions on industrial electronics, vol. 59, no. 12, December 2012.

Mr.Kaustubh U.Pathak is pursuing his final year M.E. degree in communication at SSVPSCOE at Dhule. His research interest includes embedded systems.

Proff.K.N.Pawar is working as a HOD in dept. of ELECTRONICS and Communication at SSVPSCOE, Dhule.His research interest includes Power Electronics.