Location-Aware and Safer Cards: Enhancing RFID Security and Privacy

[1]K.Anudeep, [2]Mrs. T.V.Anantha Lakshmi

[1]Student, [2]Assistant Professor
ECE Department, SRM University, Kattankulathur-603203
[1]anudeepnike@gmail.com, [2]ananthalakshmi.tv@ktr.srmuniv.ac.in

***Abstract*- This document reports a new approach for enhancing security and privacy in certain rfid applications whereby location or location related information can serve a legitimate access context. Examples of these applications include access cards, toll cards, credit cards and other payment cards. We show that location awareness can be used by both tags and back-end servers for defending against unauthorized reading and relay attacks on RFID systems. On the tag side, we design a location-aware selective unlocking mechanism using which tags can selectively respond to reader interrogations rather than doing so promiscuously. On the server side, we design a location-aware secure transaction verification scheme that allows a bank server to decide whether to approve or deny a payment transaction.**

I. INTRODUCTION

LOW cost, small size, and the ability of allowing computerized identification of objects make Radio Frequency Identification (RFID) systems increasingly ubiquitous in both public and private domains. Prominent RFID applications supply chain management (inventory control), e-passports, credit cards, driver's licenses, vehicle systems (toll collection or car key), access cards (building, parking or public transport), and medical implants. NFC, or Near Field Communication, is yet another upcoming RFID technology that allows devices, such as smart phones, to have both RFID tag and reader functionality.

A typical RFID system consists of tags, readers, and/or back-end servers. Tags are miniaturized wireless radio devices that store information about their corresponding subject. Such information is usually sensitive and personally identifiable. Readers broadcast queries to tags in their radio transmission ranges for information contained in tags and tags reply with such information. The queried information is then sent to the server for further processing and the processing result is used to perform proper actions.

This renders sensitive tag information easily subject to unauthorized reading. Information identifier gleaned from a RFID tag can be used to track the owner of the tag, or be utilized to clone the tag so that an adversary can impersonate the tag's owner.

II. BLOCK DIAGRAM

Transmitting Section

In the transmitting section fig 2.1, first we take an RFID card and place it before the RFID reader then a password is generated and transmitted to the smart phone so that we can access the system. The password received at the receiver section fig 2.2 is used to access the atm system.

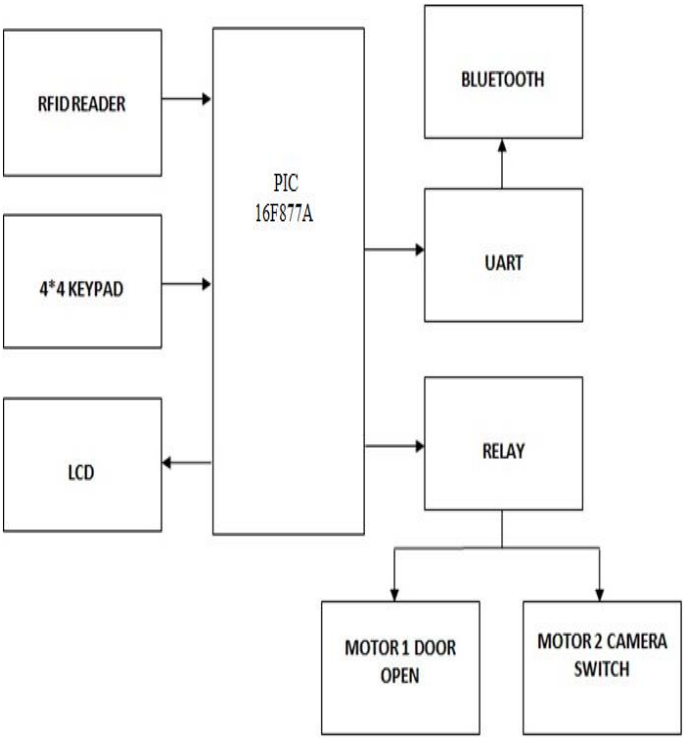


Fig:2.1 Transmitting section

Receiving Section

Fig:2.2 Receiving section

III. DESCRIPTION AND WORKING PRINCIPLE

A board of PIC16F877A is taken, which consists of slots for interfacing an LCD display, UART module consisting MAX232 IC. An RFID reader is taken and connected to the board as an external peripheral. RFID reader is used to detect the card which is operated at 125Khz frequency. It contain a password which can be used to access the card. If we take an ATM application and we take the card as ATM card, then we can access the card and take out the money.

A. Pic Controller

The name PIC initially referred to "Peripheral Interface Controller". PIC mc's (Programmable Interface Controllers), are electronic circuits that can be programmed to carry out a vast range of tasks. They can be programmed to be timers or to control a production line and much more. They are found in most electronic devices such as alarm systems, computer control systems, phones, in fact almost any electronic device.

Features:

- Only 35 single-word instructions
- Operating speed: DC – 20 MHz clock input DC – 200 ns instruction cycle
- Up to 8K x 14 words of Flash Program Memory, Up to 368 x 8 bytes of Data Memory(RAM), Up to 256 x 8 bytes of EEPROM Data Memory
- Timer0: 8-bit timer/counter with 8-bit pre scalar
- Timer1:16-bit timer/counter with pre scalar, can be incremented during Sleep via external crystal/clock
- Timer2:8-bit timer/counter with 8-bit period register, pre scalar and post scalar
- Synchronous Serial Port (SSP) with SPI™ (Master mode) and I2C™ (Master/Slave)

B. UART

A universal asynchronous receiver/transmitter is a type of "asynchronous receiver/transmitter", a piece of computer hardware that translates data between parallel and serial forms.

The UART takes bytes of data and transmits the individual bits in a sequential fashion. At the destination, a second UART re-assembles the bits into complete bytes. A UART is used to convert the transmitted information between its sequential and parallel form at each end of the link. Each UART contains a shift register which is the fundamental method of conversion between serial and parallel forms.

MAX232

The MAX232 is an integrated circuit that converts signals from an RS-232 serial port to signals suitable for use in TTL compatible digital logic circuits.

The drivers provide RS-232 voltage level outputs (approx. ± 7.5 V) from a single + 5 V supply via on-chip charge pumps and external capacitors. The receivers reduce RS-232 inputs (which may be as high as ± 25 V), to standard 5 V TTL levels.

C. RFID

Radio frequency identification (RFID) is a generic term that is used to describe a system that transmits the identity (in the form of a unique serial number) of an object or person wirelessly, using radio waves. . RFID data can be read through the human body, clothing and non-metallic materials. The basic components of an RFID system are an antenna or coil, a tranceiver (decoder) and a transponder (RF tag) electronically programmed with unique information.

A typical reader is a device that has one or more antennas that emit radio waves and receive signals back from the tag. The reader then passes the information in digital form to a computer system. The first access control systems used low-frequency RFID tags. Recently, vendors have introduced 13.56 MHz systems that offer longer read range. Most countries have assigned the 125 kHz or 134 kHz area of the radio spectrum for low-frequency systems, and 13.56 MHz is used around the world for high-frequency systems.

D. RELAY

A relay is an electrically operated switch. Relays allow one circuit to switch a second circuit which can be completely separate from the first.

There is no electrical connection inside the relay between the two circuits; the link is magnetic and mechanical.

Relays can switch AC and DC, transistors can only switch DC. Relays can switch many contacts at once.

Relays cannot switch rapidly (except reed relays), transistors can switch many times per second.

Relays use more power due to the current flowing through their coil.

E. KEYPAD

A 4*4 keypad is used for loading numerics into the microcontroller. It consists of 16 buttons arranged in a form of an array containing four lines and four columns.

F. LIQUID CRYSTAL DISPLAY (LCD)

LCDs are most commonly used because of their advantages over other display technologies. They are thin and flat and consume very small amount of power compared to LED displays and cathode ray tubes (CRTs).

LCDs have become very popular over recent years for information display in many ‘smart’ appliances. They are usually controlled by microcontrollers.

If RS=0 Instruction command Code register is selected, allowing user to send command

RS=1 Data register is selected allowing to send data that has to be displayed.

G. DC MOTOR

A direct-current motor is a shunt-wound motor in which the field windings and the armature may be connected in parallel across a constant-voltage supply. A 12V DC motor consists of two magnets facing the same direction, that surround two coils of wire that reside in the middle of the 12V DC motor around a rotor.

The coils are positioned to face the magnets, causing electricity to flow to them. This generates a magnetic field, which ultimately pushes the coils away from the magnets they are facing, and causes the rotor to turn. The current shuts off at the rotor makes a 180 turn, causing each rotor to face the opposite magnet.

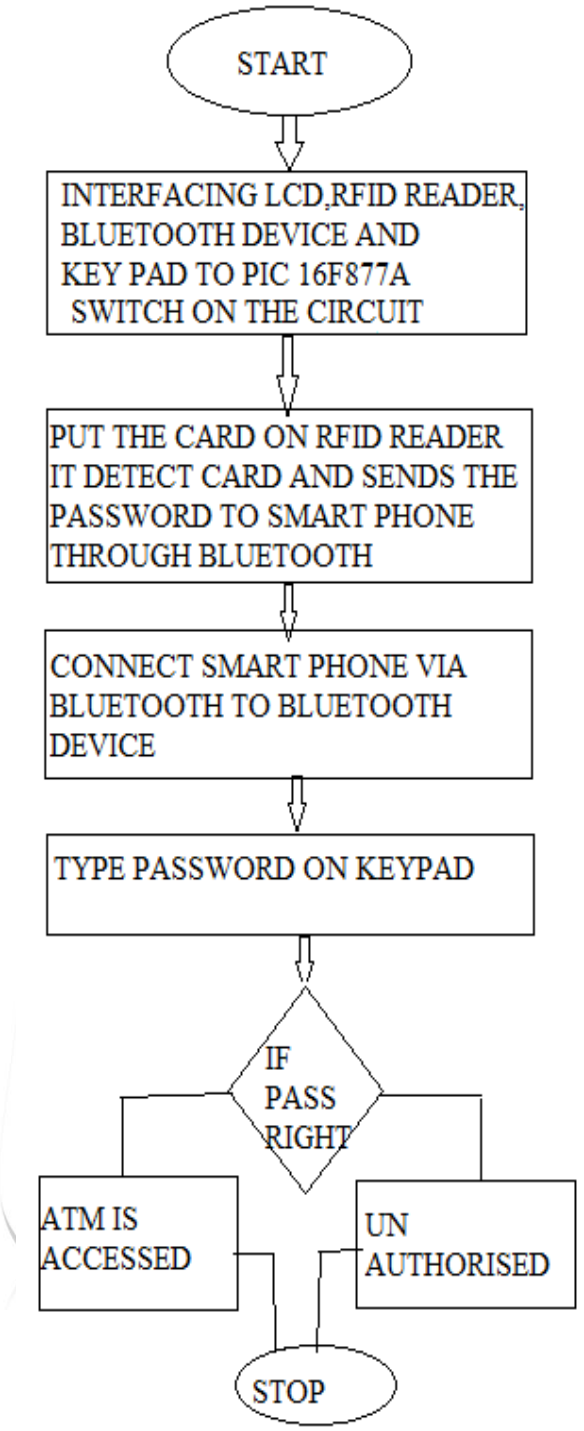
As the current turns on again, the electricity flows oppositely, sending another pulse that causes the rotor to turn once again. The brushes that are located within the 12V DC motor transfer the electricity from the rotor, controlling the motors timing; turning it on and off when instructed.

Here we are using blue tooth technology for sending the password to a smart phone. The smart phone holder can only access the card because the password is sent to the smart phone which is paired up to the blue tooth device in our board.

After that, when the password is typed on the keypad, it is displayed on LCD. If the password is right, relay in our cicuit activates one of the motor which shows us the person is authorised and the atm can be accessed. If it shows the password is wrong, then the person is unauthorised and the camera switch is switched on and the person cannot access the card.

Thus if any third person who doesn't get the password cannot access the card. Likewise the privacy of the user can be enhanced.

FLOW CHART:



IV. RESULT

As mentioned above the circuit and the result is as shown below. When the card is shown to the rfid reader, the password is generated. The password is sent to the smart phone, then it is typed on keypad. Then LCD displays whether the is password is right or wrong. According to the display relay comes in to the action.

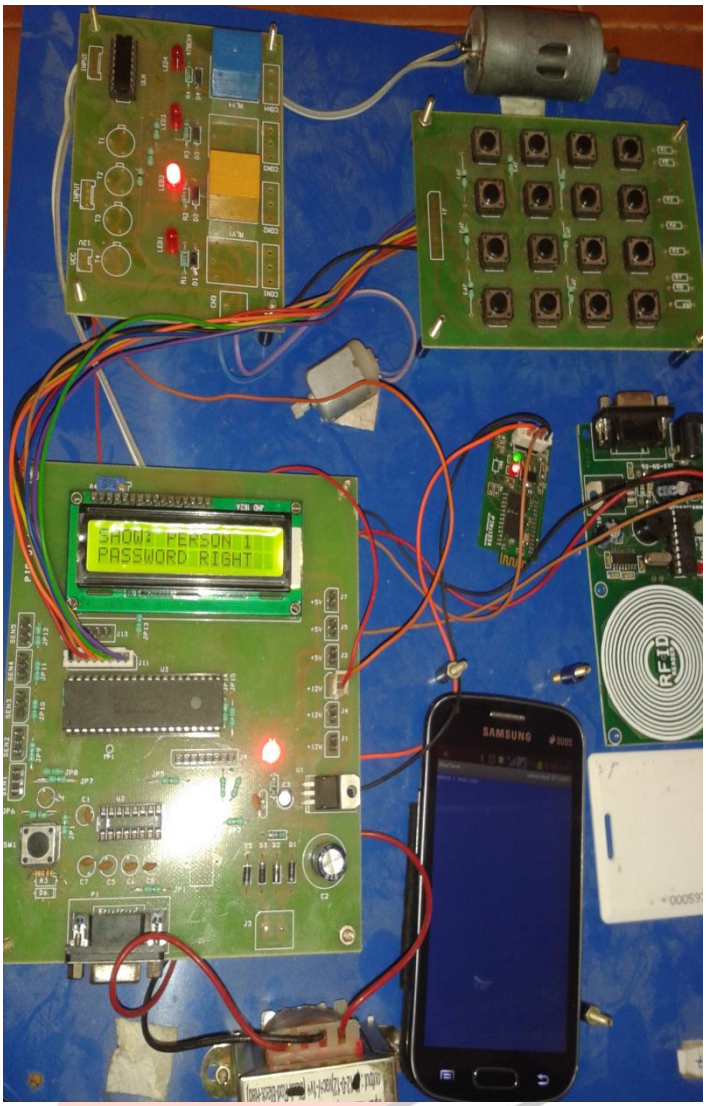


Fig 4.1: Result of the circuit

When LCD displays right, relay switches ON and motor 1 will be ON. When LCD displays wrong, relay switches OFF and motor 2 will be ON that is to show that the user is unauthorized and he cannot access the card. Thus this paper shows the enhancement of the security of the cards not to be accessed by the malicious users. It also provides security for the users if the is misplaced.

V. CONCLUSION AND FUTURE WORK

In this paper, we reported a new approach to defend against unauthorized reading. When any unauthorised user commits to access the card, he would not have the actual user's smart phone. So he cannot know the password and he cannot type the password and can't access the money. And also instead of a motor, if we connect a camera and write certain code for it, the camera takes the photograph of the person.

The extension for this paper would be, GPS can be used to track the malicious readers. Instead of blue tooth GPS can be used so as to send the password to smart phone from long distances.

REFERENCES

[1] RFID Toll Collection Systems, http://www.securitysa.com/news.aspx?pklnewsid=2591, 2007
[2] M. Buettner, R. Prasad, M. Philipose, and D. Wetherall, "Recognizing Daily Activities with RFID-Based Sensors," Proc. Int'l Conf. Ubiquitous Computing (UbiComp), 2009.
[3] http://www.datasheetarchive.com/pic%20microcontroller%2016F877A-datasheet.html
[4] http://www.maximintegrated.com/products/interface/controllers-expanders/uart.cfm
[5] http://www.engineersgarage.com/electroniccomponents/16x2-lcd-module-datasheet
[6] http://ww1.microchip.com/downloads/jp/DeviceDoc/39582b
[7] *www.microchip.com/wwwproducts/Devices.aspx?dDocName=en010242*