International Journal Of Advanced Research In Engineering Technology & Sciences
ISSN: 2394-2819
Email: editor@ijarets.org March- 2015 Volume 2, Issue-3 www.ijarets.org

RF ID Based Main Power System & Theft Control Using Alarm

Ankit Gupta, Chinmay Jain, Jatin Kumar
B.Tech Student
Department of IT
SRM University NCR Campus
Modinagar

Yogesh Kushwaha
Assistant Professor
Department of IT
SRM University NCR Campus
Modinagar

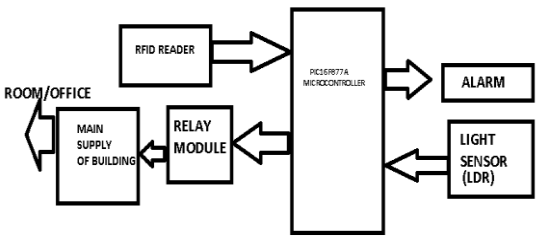
ABSTRACT—
This project RFID based Building main power system is developed to build a security system for a building to prevent the other persons (like thieves) to enter into building by controlling radio frequency identification by checking a suitable RFID card and if person enter in building breaking wall, door, windows etc, and USE any kind of light (torch, matches box, lighter etc) then buzzer ON (ALARM). The RFID tag gives the unique id whenever it reads the card information. This id information is send to the micro controller to check the correct card to take a action of ON/OFF main POWER. If the card id matches with the original information, it allows to ON/OFF the main power of building, if not gives the buzzer as an indication of wrong person tried to enter into the building sectors. This application will provide RFID tag based system which uses microcontroller. RFID is one the fast growing technology all over the world for identifying and tracing goods. This system can help hospitals to find expensive equipment in less time and provide better services for patients.

Keywords- Radio Frequency Identification Technology, Current State, Awareness

INTRODUCTION

Radio Frequency Identification (RFID) technology is a non-contact, automatic identification technology that uses radio signals to identify, track, sort and detect a variety of objects including people, vehicles, goods and assets without the need for direct contact (as found in magnetic stripe technology) or line of sight contact (as found in bar code technology). RFID technology can track the movements of objects through a network of radio-enabled scanning devices over a distance of several meters.

The RFID tag gives the unique id whenever it reads the card information. This id information is send to the microcontroller to check the correct card to take a action of ON/OFF main POWER. If the card id matches with the original information, it allows to ON/OFF the main power of building, if not gives the buzzer as an indication of wrong person tried to enter into the building sectors. This application will provide RFID tag based system which uses microcontroller. RFID is one the fast growing technology all over the world for identifying and tracing goods. This system can help hospitals to find expensive equipment in less time and provide better services for patients.



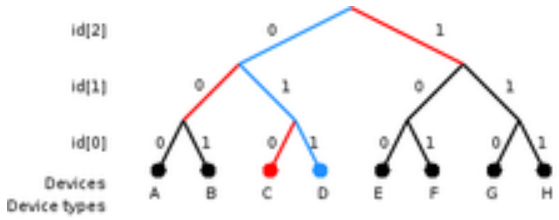
The security system is basically an embedded one. Embedded stands for hardware controlled by software. Here, the software using a Microcontroller controls all the hardware components.

An RFID module basically consists of two parts, namely, a tag and a reader. A typical RFID system consists of an antenna, a transceiver and a transponder (RF tag). The radio frequency is read by the transceiver and the information is transferred to a device for further processing. The information (the unique serial number) to be transmitted is stored in the RF tag or transponder [1].
The transponder contains a chip and an antenna mounted on a substrate. The chip transmits the relevant information through antenna. The antenna also receives the electromagnetic waves sent by the RFID reader.

Different RFID tags work on different frequencies. Here low frequency, 125 kHz, RFID tags have been used. These tags work within a range of 10 cm. When an RFID tag comes in this range, the reader detects it and sends a unique code of the tag serially. This serial code, consisting of 12 bytes, is received by the microcontroller.

A device called an RFID tag (or simply a tag) is a key component of the technology. An RFID tag usually has at least two components:
1. An integrated circuit for modulating and demodulating radio signals and performing other functions.
2. An antenna for receiving and transmitting the signal.
An RFID tag can perform a limited amount of processing and has small amount of storage. RFID tags are sometimes considered to be enhanced "electronic barcodes"[2] . RFID tags that do not have any integrated circuit are called chip less RFID tags (also known as RF fibers). These tags use "fibers or materials that reflect a portion of the reader's signal back and the unique return signal can be used as an identifier" [3].
RFID tags can be passive, active or battery-assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery-assisted passive (BAP) has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader. However, to operate a passive tag, it must be illuminated with a power level roughly a thousand times stronger than for signal transmission. That makes a difference in interference and in exposure to radiation.
Tags may either be read-only, having a factory-assigned serial number that is used as a key into a database, or may be read/write, where object-specific data can be written into the tag by the system user. Field programmable tags may be writing-once, read-multiple; "blank" tags may be written with an electronic product code by the user.

RFID Recognition
Often more than one tag will respond to a tag reader, for example, many individual products with tags may be shipped in a common box or on a common pallet. Collision detection is important to allow reading of data. Two different types of protocols are used to "singulate" a particular tag, allowing its data to be read in the midst of many similar tags. In a slotted Aloha system, the reader broadcasts an initialization command and a parameter that the tags individually use to pseudo-randomly delay their responses. When using an "adaptive binary tree" protocol, the reader sends an initialization symbol and then transmits one bit of ID data at a time; only tags with matching bits respond, and eventually only one tag matches the complete ID string.
An Electronic Product Code (EPC) is one common type of data stored in a tag. When written into the tag by an RFID printer, the tag contains a 96-bit string of data. The first eight bits are a header which identifies the version of the protocol. The next 28 bits identify the organization that manages the data for this tag; the organization number is assigned by the EPC Global consortium. The next 24 bits are an object class, identifying the kind of product; the last 36 bits are a unique serial number for a particular tag.



An example of a binary tree method of identifying an RFID tag

The diagram shows a possible search path to find a certain device or group of devices. where large numbers of tags can be probed and located by means of simple primitive commands such as "respond if bit i of your tag is 0/1".

Specific Circuit Elements

PERIFERAL INTERFACE CONTROLLER

PICs are popular with both industrial developers and hobbyists alike due to their low cost, wide availability, large user base, extensive collection of application notes, availability of low cost or free development tools, and serial programming (and re-programming with flash memory) capability.

Early models of PIC had read-only memory (ROM) or field-programmable EPROM for program storage, some with provision for erasing memory. All current models use Flash memory for program storage, and newer models allow the PIC to reprogram itself. Program memory and data memory are separated.

Features of different PIC controller are shown in the following table [4]:

TABLE 1-1: PIC16F87XA DEVICE FEATURES

Key Features	PIC16F873A	PIC16F874A	PIC16F876A	PIC16F877A
Operating Frequency	DC – 20 MHz	DC – 20 MHz	DC – 20 MHz	DC – 20 MHz
Resets (and Delays)	POR, BOR (PWRT, OST)	POR, BOR (PWRT, OST)	POR, BOR (PWRT, OST)	POR, BOR (PWRT, OST)
Flash Program Memory (14-bit words)	4K	4K	8K	8K
Data Memory (bytes)	192	192	368	368
EEPROM Data Memory (bytes)	128	128	256	256
Interrupts	14	15	14	15
I/O Ports	Ports A, B, C	Ports A, B, C, D, E	Ports A, B, C	Ports A, B, C, D, E
Timers	3	3	3	3
Capture/Compare/PWM modules	2	2	2	2
Serial Communications	MSSP, USART	MSSP, USART	MSSP, USART	MSSP, USART
Parallel Communications	—	PSP	—	PSP
10-bit Analog-to-Digital Module	5 input channels	8 input channels	5 input channels	8 input channels
Analog Comparators	2	2	2	2
Instruction Set	35 Instructions	35 Instructions	35 Instructions	35 Instructions
Packages	28-pin PDIP 28-pin SOIC 28-pin SSOP 28-pin QFN	40-pin PDIP 44-pin PLCC 44-pin TQFP 44-pin QFN	28-pin PDIP 28-pin SOIC 28-pin SSOP 28-pin QFN	40-pin PDIP 44-pin PLCC 44-pin TQFP 44-pin QFN

Power Supply

Here in our application we need a 5v DC power supply for all electronics involved in the project. This requires step down transformer, rectifier, voltage regulator, and filter circuit for generation of 5v DC power.

REGULATOR IC (78XX)

It is a three pin IC used as a voltage regulator. It converts unregulated DC current into regulated DC current.
Normally we get fixed output by connecting the voltage regulator at the output of the filtered DC.
It can also be used in circuits to get a low DC voltage from a high DC voltage (for example we use 7805 to get 5V from 12V).
There are two types of voltage regulators
1. fixed voltage regulators (78xx, 79xx)
2. Variable voltage regulators (LM317).

In fixed voltage regulators there is another classification:
1. +ve voltage regulators
2. -ve voltage regulators

The 78xx lines are positive voltage regulators: they produce a voltage that is positive relative to a common ground.
There is a related line of 79xx devices which are complementary negative voltage regulators.
78xx and 79xx ICs can be used in combination to provide positive and negative supply voltages in the same circuit.

RFID Working

Systems that make use of RFID technology are typically composed of three key elements:
1. An RFID tag, or transponder, that carries object-identifying data.
2. An RFID tag reader, or transceiver, that reads and writes tag data.
3. A back-end database, that stores records associated with tag contents.

In the RFID system, the reader sends out a radio frequency wave to the tag and the tag broadcasts back its stored data to the reader. The system has two antennas, one for the tag and the other on the reader. The data collected from the tag can either be sent directly to a host computer through standard interfaces or it can be stored in a portable reader and later updated to the computer for data processing. The automatic reading and direct use of tag data is called 'automatic data capture'.
When the tag which is battery free, is to be read, the reader sends out a power pulse to the antenna lasting for about 50ms.The magnetic field generated is collected by the antenna in the transponder that is tuned to the same frequency. This received energy is rectified and stored on a capacitor within the transponder.

When the power pulse has finished, the transponder immediately transmits back its data, using the energy stored within its capacitor as its power source. The data is picked up by the receiving antenna and decoded by the reader unit.
Once all the data has been transmitted, the storage capacitor is discharged resetting the transponder to make it ready for the next read cycle. The period between transmission pulses is called sync time and lasts between 20ms and 50ms depending on the system set up.

The scanning antennas can be permanently affixed to a surface; handheld antennas are also available. They can take whatever shape you need; for example, you could build them into a door frame to accept data from persons or objects passing through.

When an RFID tag passes through the field of the scanning antenna, it detects the activation signal from the antenna. That "wakes up" the RFID chip, and it transmits the information on its microchip to be picked up by the scanning antenna.

LCD Working

The interface used by LCD is a parallel bus, allowing simple and fast reading/writing of data to and from the LCD. This waveform will write an ASCII Byte out to the LCD's screen. The ASCII code to be displayed is eight bits long and is sent to the LCD either four or eight bits at a time. If four bit mode is used, two "nibbles" of data (Sent high four bits and then low four bits with an "Enable" Clock pulse with each nibble) are sent to make up a full eight bit transfer. The "Enable" Clock is used to initiate the data transfer within the LCD. Sending parallel data as either four or eight bits are the two primary modes of operation. While there are secondary considerations and modes, deciding how to send the data to the
LCD is most critical decision to be made for an LCD interface application.

Eight bit mode is best used when speed is required in an application and at least ten I/O pins are available. Four bit mode requires a minimum of six bits. To wire a microcontroller to an LCD in four bit mode, just the top four bits (DB4-7) are written to.
The "RS" bit is used to select whether data or an instruction is being transferred between the microcontroller and the LCD. If the Bit is set, then the byte at the current LCD "Cursor" Position can be read or written. When the Bit is reset, either an instruction is being sent to the LCD or the execution status of the last instruction is read back (whether or not it has completed).

Reading Data back is best used in applications which required data to be moved back and forth on the LCD (such as in applications which scroll data between lines).In our Project we have permanently grounded R/W pin which means we are not retrieving any data from LCD.
The LCD can be thought of as a "Teletype" display because in normal operation, after a character has been sent to the LCD, the internal "Cursor" is moved one character to the right. The "Clear Display" and "Return Cursor and LCD to Home Position"
Instructions are used to reset the Cursor's position to the top right character on the display.
To move the Cursor, the "Move Cursor to Display" instruction is used. For this instruction, bit 7 of the instruction byte is set with the remaining seven bits used as the address of the character on the LCD the cursor is to move to. These seven bits provide 128 addresses, which matches the maximum number of LCD character addresses available.
Eight programmable characters are available and use codes 0x000 to 0x007. They are programmed by pointing the **LCD's "Cursor" to the Character Generator RAM.**
The last aspect of the LCD to discuss is how to specify a contrast voltage to the Display. I typically use a potentiometer wired as a voltage divider. This will provide an easily variable voltage between Ground and Vcc, which will be used to specify the contrast (or "darkness") of the characters on the LCD screen. You may find that different LCDs work differently with lower voltages providing darker characters in some and higher voltages do the same thing in others.

SECURITY AND PRIVACY ISSUES

With the adoption of RFID technology, a variety of security and privacy risks need to be addressed by both organizations and individuals: TAG DATA RFID tags are considered “dumb” devices, in that they can only listen and respond, no matter who sends the request signal. This brings up risks of unauthorized access and modification of tag data. In other words, unprotected tags may be vulnerable to eavesdropping, traffic analysis, spoofing or denial of service attacks. We will look at each of these in turn:

TAG DATA

Eavesdropping (or Skimming)

Radio signals transmitted from the tag, and the reader, can be detected several meters away by other radio receivers. It is possible therefore for an unauthorized user to gain access to the data contained in RFID tags if legitimate transmissions are not properly protected. Any person who has their own RFID reader may interrogate tags lacking adequate access controls, and eavesdrop on tag contents. Researchers in the US has demonstrated a skimming attack on an RFID credit card, through which credit card information, such as the cardholder's name and account information, could be skimmed if not properly encrypted[6] .

Spoofing

Based on the data collected from eavesdropping or traffic analysis, it is possible to perform tag spoofing.
For instance, a software package known as "RFDump" [7], that runs on a notebook computer or personal digital assistant, allows a user to perform reading or writing tasks on most standard smart tags if they are not properly protected. The software permits intruders to overwrite existing RFID tag data with spoof data. By spoofing valid tags, the intruder could fool an RFID system, and change the identity of tags to gain an unauthorized or undetected advantage. One example is trying to save money by buying expensive goods that have had their RFID price tags spoofed to display cheaper prices. By combining the two capabilities of eavesdropping and spoofing, a replay attack is possible where an attacker can "query a tag, receive the information it sends, and retransmit this information at a later time" [8].

Denial of Service Attack

The problems surrounding security and trust are greatly increased when large volumes of internal RFID data are shared among business partners. A denial of service attack on RFID infrastructure could happen if a large batch of tags has been corrupted. For example, an attacker can use the "kill" command, implemented in RFID tags, to make the tags permanently inoperative if they gain password access to the tags. In addition, an attacker could use an illegal high power radio frequency (RF) transmitter in an attempt to jam frequencies used by the RFID system, bringing the whole system to a halt [2].

RFID READER INTEGRITY

In some cases, RFID readers are installed in locations without adequate physical protection. Unauthorized intruders may set up hidden readers of a similar nature nearby to gain access to the information being transmitted by the readers, or even compromise the readers themselves, thus affecting their integrity. Unauthorized readers may also compromise privacy by accessing tags without adequate access controls. As a result, information collected by readers and passed to the RFID application may have already been tampered with, changed or stolen by unauthorized persons. An RFID reader can also be a target for viruses.

APPROACHS FOR TACKLING SECURITY AND PRIVACY ISSUES

SOLUTIONS FOR TAG DATA PROTECTION

Password Protection on Tag Memory

Passwords can be used to protect tag data, preventing tags from being read without the original owner's permission. But if the passwords for all the tags are identical, then the data becomes virtually public. However, if each tag is going to have a different or unique password, there may be millions of passwords that need to be recorded, meaning the reader would have to access the database and perform a lot of comparisons for each reading attempt.

Physical Locking of Tag Memory

The tag manufacturer locks information such as a unique identifier into tag before the tag is released into an open environment. In other words, the chip is read-only and is embedded with information during the manufacturing process. This provides proof of origin.

The limitation of this method is that no rewriting of data can be done on the tag chip. Additional memory would be required for storing modifiable or extra information and an algorithm would be needed for finding the latest tag data. This would result in higher memory cost and a larger size memory.

Authentication of the "Author" in Tag Memory

The author or owner of the tag encrypts the tag data with his own private key (i.e. digitally signs the tag) and writes the encrypted data into tag memory along with the author's name, a reference to his public key and the algorithm used in non-encrypted form. When the reader wants to verify the authenticity of information, it retrieves the author's name and other non-encrypted information from the tag to verify that the data has been actually written by the original author as claimed. However, if the RFID reader needs to update the tag with new data, a key management system is required in order to manage the private key.

SOLUTIONS FOR RFID READER INTEGRITY

Reader Protection

Readers can reject tag replies with anomalies in response times or signal power levels which don't match the physical properties of tags. If passive tags are used, this can be a way to prevent spoofing attempts. Readers can also use random frequencies with tags designed to follow a frequency dictated by the reader. Readers can change frequencies randomly so that unauthorized users cannot easily detect and eavesdrop on traffic. On top of this, data transmitted between the reader and the RFID application server could require verification of the reader's identity. Authentication mechanisms can be implemented between the reader and the backend application to ensure that information is passed to the valid processor.

Read Detectors

RFID environments can be equipped with special devices to detect unauthorized read attempts or transmissions on tag frequencies. These read detectors may be used to detect unauthorized read/update attempts on tags, if they are used together with specially designed tags that can transmit signals over reserved frequencies, indicating any attempts to kill or modify tags.

ADVANTAGES

a) RFID technology permits no line of sight reading.
b) Robustness and reliability under difficult environmental conditions.
c) These tags can be read through water, snow, concrete, bricks, plastics, wood, and most non-metallic materials.
d) Available in a wide variety of physical forms, shapes, sizes and protective housings.
e) RFID tags can be read at very high speeds.
f) The tag need not be on the surface of the object (and is therefore not subject to wear).
g) The read time is typically less than 100 milliseconds
h) Large numbers of tags can be read at once rather than item by item.

APPLICATIONS

Principle areas of applications of RFID include:

1. Transportation
2. Manufacturing and processing.
3. Security.
4. Shopping

Texas Instruments Radio Frequency Identification (TIRFid) Systems has introduced its new RFID tag for textile rental and dry cleaning applications [5].
TI-RFid tags provide more accurate identification and greater accountability as well as improved handling through each stage of cleaning and processing to final customer delivery.

Car access
Texas Instruments car access products bring unique features and performance to the market. With its strong security, high sensitivity and unique, patented HDX technology it allows the design of best-in-class car access systems. The broad portfolio includes products required for the key fob and the vehicle.

Animal ID
Texas Instruments' RFID technology helps ranchers round up stock more efficiently, provide feed and water at optimal locations when necessary, and even handle some basic health monitoring such as the frequency with which animals visit feeding stations. A decrease in frequency can be an indication of illness.

Books Information
RFID system allows booksellers to gain such information as the range of books a shopper has browsed, the number of times a particular title was picked up, and even the length of time spent flipping through pages. The shelves can scan the contents of the shelves and, via computer, alert store employees when supplies are running low or when theft is detected.

Passport
RFID tags loaded with biometric information will be embedded in passports to ensure travelers comply with security regulations. RFID technology is also being used to improve luggage handling in airports.

CONSTRUCTION AND TESTING
In the process of realizing this project, the construction was initially carried out on a breadboard to allow for checking and to ascertain that it is functioning effectively. All irregularities were checked then tested and found to have a satisfactory output. The component were then removed and transferred to a Vero board strip and soldered into place and all discontinuous point were cut out to avoid short-circuiting.

TESTING OF PROJECT
With the knowledge of operation of the system was tested step by step to the transistor output and the load was connected across the collector terminal of the transistor

PROBLEMS AND ISSUES

PROBLEMS	SOLUTIONS
Motion detector has very small output voltage	Used operational amplifier to increase signal level
Need to create -12 VDC supply from +12 VDC	Used 555 timer
LCD display on EVAL board not working	Using LEDs for debug
Receiving RS-232 input on Microcontroller	In progress: adjusting timer, voltages& parameters of Rx8 module
Errors when building OS solutions for eBoxll	In Progress: working with lab TAs to troubleshoot

FUTURE DEVELOPMENT

1. We can send this data to a remote location using mobile or internet.
2. We can add the module of voice alarm system to indicate valid or invalid card entry.
3. Encryption techniques can be used to encrypt the information in RFID so that they cannot be stole.

CONCLUSION

In this review paper, we build a security system for a building to prevent the other persons (like thieves) to enter into building by controlling radio frequency identification by checking a suitable RFID card. Each authorized person is allotted with a specific RFID with which that person can access the particular room or building and the power supply of that particular room is also controlled with that RFID. The RFID reader reads the RFID information and ON/OFF the power supply of that room. A buzzer is also installed in these highly secured rooms which send information to the security personnel if person enter in building breaking wall, door, windows etc, and use any kind of light (torch, matches box, lighter etc). This kind of system can be used in museums where antiques are kept in highly secured volts or rooms and only authorized persons are allowed to enter in those rooms. This type of technology can be implemented and also upgraded very easily. We can apply encryption algorithms to the RFID so that their unique IDs cannot be hacked or stolen and duplicate RFIDs cannot be generated with that information.

REFERENCES

a) http://www.engineersgarage.com/microcontroller/8051projects/interface-rfid-AT89C51-circuit
b) http://www.eurosmart.com/Update/07-10/Eurosmart_White_paper_on_RFID_Oct07.pdf
c) http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=28
d) http://ww1.microchip.com/downloads/en/DeviceDoc/39582b.pdf
e) http://www.ti.com/lsds/ti/wireless_connectivity/nfc_rfid/overview.page
f) http://www.nytimes.com/2006/10/23/business/23card.html?pagewanted=1&_r=1
g) http://freshmeat.net/projects/rfdump/?branch_id=61265&release_id=264928
h) http://blogs.sun.com/ks/entry/rfid_technology_security_concerns