A Project Report

On

ATTENDANCE MONITORING USING RADIO FREQUENCY IDENTIFICATION

As partial fulfillment of the Degree of Bachelor of Technology

Submitted by:-

TAMISH AREN	**051015**
HARSHWINDER SINGH	**051016**
SWARANDEEP SINGH CHOPRA	**051021**
AAKASH SHARMA	**051054**

MAY - 2009

DEPARTMENT OF ELECTRONICS AND COMMUNICATION
JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY-WAKNAGHAT

CERTIFICATE

This is to certify that the work entitled, **"Attendance registration using PC based RFID"** has been submitted **by Tamish Aren, Harshwinder Singh, Swarandeep Singh Chopra** and **Aakash Sharma,** in partial fulfilment for the award of degree of Bachelor of Technology in Electronics and communication of Jaypee University of Information Technology has been carried out under my supervision. This work has not been submitted partially or wholly to any other university or institute for the award of this or any other degree or diploma.

Mrs. Shruti Jain
(Project guide)

ACKNOWLEDGMENT

No Project or task can be successfully completed without the help of those people who act as “guiding light” helping to smoothen out the rough edges, providing the inspiration when you feel you have reached a spot you can’t seem to get out of.

We are extremely grateful to Mrs Shruti Jain, our respected teacher for her guidance and motivation .Her thinking and straightforward attitude has inspired us to complete this project under stiff time limits.

We are also grateful to our HOD Dr. Sunil Vidya Bhooshan for acting as the guiding force to us and our guide.

We would also like to thank all the faculty members for their sincere devotion to impart us with the best of knowledge and skills available.

Also, we would like to thank our friends, who have supported, encouraged, and criticized our efforts which have been instrumental in giving the project

its final shape.

Harshwinder

Tamish Aren (051015)

Harshwinder Singh (051016)

Swarandeep

Swarandeep Singh Chopra (051021)

Aakash Sharma (051054)

TABLE OF CONTENTS

Topic *Page No.*

- **Chapter 3**:

HARDWARE DISCRIPTION

- **Chapter 4:**

Software Schematics

- **Chapter 5:**

Results and Discussions

- **CHAPTER 6:**

Controversies and Future Work

LIST OF FIGURES AND TABLES

CHAPTER 1

INTRODUCTION

1.1 Overview

The most common devices used to control access to private areas where sensitive work is being carried out or where data is held, are keys, badges and magnetic cards. These all have the same basic disadvantages: they can easily be duplicated and when stolen or passed on, they can allow entry by an unauthorized person. The smart card overcomes these weaknesses by being very difficult to be reproduced and capable of storing digitized personal characteristics. With suitable verification equipment, this data can be used at the point of entry to identify whether the user is the authorized controller. The card can also be individually personalized to allow access to limited facilities, depending on the holder's security clearance. A log of the holder's movements through a security system can be stored on the card as a security audit trail.

The card could contain information on the user's privileges (i.e. access to secure areas of the building, automatic vehicle identification at entrances to company car parks etc. All the information is checked on the card itself. Furthermore it will also record the time and attendance of user. Smart card constitute an essential trust element in a security infrastructure to provide the appropriate level of security, the workable interoperability of technical and organizational framework and supporting interoperability framework and supporting infrastructure must be achieved.

Personal identification is the process of associating a particular individual with an identity. Identification can be in the form of verification (also known as authentication), or recognition (also known as identification). When an individual's claims of identity and privilege are verified in a truly reliable way, the identification is authoritative.

In our study, we propose to monitor the attendance of an organization using a Radio Frequency Identification unit. Based on our framework we developed an RFID unit comprising of a transmitter and receiver interfaced to a computer through the parallel port. Our given project is to consider the attendance monitoring for five employees of a company. The project consists of an RF transmitter and a duly aligned RF receiver with relay switching section to interface with PC parallel port to provide data input to this. One may modify the same hardware with single receiver and multiple transmitters for all employees with encoder decoder technique. RFID is a wireless technology with variable a range and it is not a 'line of sight' technology like the one using bar codes. In our project a transmitter activates the receiver at the entry gate of the office/company where it is fitted duly with motorized door. The computer connected to the receiver, will activate the relay and give instruction to the motor to open the door for the pre-selected time duration and then close the door afterwards. A buzzer beep will also show the presence and entry of that specific employee whose transmitter is being activated. The computer with on line real time application will enter and store the data in the employee's file. Thus we have five data files handled by PC each for each employee. At the time of exit, he again does the same process to open the gate/door again.

1.2 Identification system

An identification system determines who is allowed to enter or exit, where they are allowed to exit or enter and when they are allowed to exit or enter. Mechanical locks and keys do not provide records of the key used on any specific door and the key can be easily copied and transferred to another person. When a mechanical key is lost or the key holders no longer authorized to, use the protected area, the locks must physically be changed.

Electronic access control uses the power of computers to solve the limitations of mechanical locks and keys. Electronic access control determines whether to grant access to the protected area based on the credential presented and when it is presented. If access is granted, the door is unlocked for a predetermined time period and the transaction is recorded. If access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and declare an alarm if the door is forced opens or held open too long after being unlocked.

Knowing the position of the door is an important element of the system and is typically accomplished with a magnetic switch concealed in the frame of the door. The user's primary interface with an access control as reader reflects the technology of the credential. The reader for a magnetic strip, bar code, Wig and card is typically called a swipe reader and is commonly used in retail stores and ATMs. Some swipe readers require the card to be swiped in a specific direction in order to get a good read. The reader for a proximity or contact less smart card is actually a radio transceiver when data transmission via radio frequency.

1.3 What is RFID?

As the name RF signifies, it is a kind of identification system, which uses radio frequency. RFID uses wireless technology operating with the 50 kHz to 2.5 GHz (in our project-95 kHz) frequency range. It does not require any physical connection for identification between the unit to be identified and the identifier unit, which in this case is the reader. For automatic identification purposes, each piece of equipment (which is to be identified) shall be fitted with a small electronic device (called tag) containing unique identification code.

The tag as mentioned in Figure 1,in the presence of sensing equipment (reader) operating on ultra high frequency (UHF) radio waves reflects altered radio waves (modulated) to determine the identification of the equipment.

For further analysis, the reader shall optionally add its own identification number, the date and time and shall transmit this data with tag information to the user's computer system.

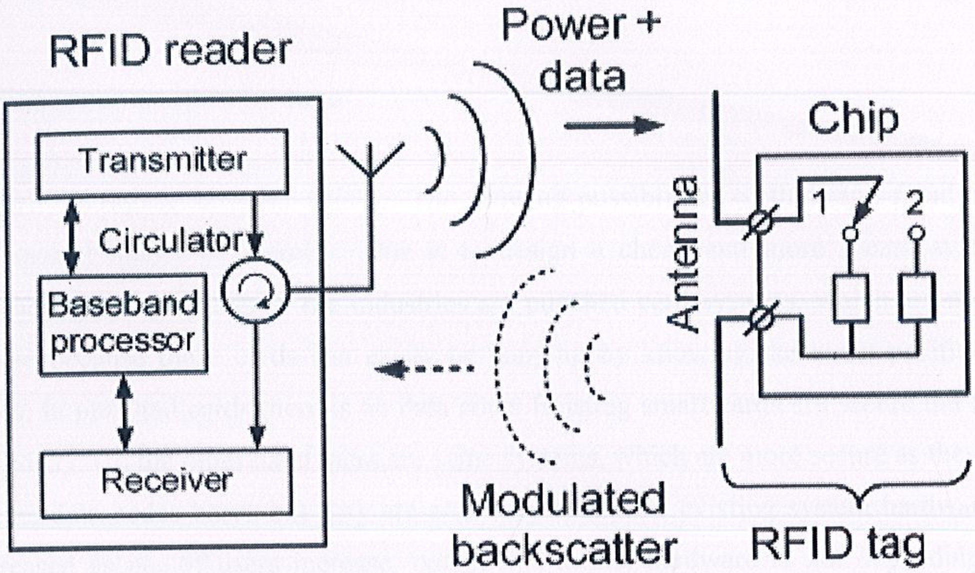


Figure 1.1: Working Mechanism of an RFID Unit

1.4 Problem definition

Increasingly companies and individuals are using wireless technology for important communication they want to keep private and corporate data transmission. Contact less smart card is used to provide secure physical access to authorized person. The card should allow for the secure transportation of data in an efficient manner, the card should allow the positive identification of the user and store information for third parties. The card should allow for authorization data to be stored and possibly executed on the card to give access to a number of devices. Information on the card should be updateable so that it adapts to the changing world, however only authorized parties should have access to change the data for authorization purpose of the card. Where code is executed on the card it must be executed in a protected form. All data on the card must be provided in such a fashion that data cannot be directly accessible without going through certain security mechanism contained within the card.

1.5 Need of the work to be done

Security is highly demanded today. The growing possibilities of theft and fraud need the special means of security. This is to design a cheap and more secure system. Already existing system in the industries are punched card systems, which are not so secure because these cards can easily be copying by knowing the exact position of holes. In punched cards there is no data code. Existing smart cards are secure but they are costly. On the other hand there are some systems, which are more secure as they are on the data codes bases but they are also very costly. In existing system hardware is increased as no. of users increase, but in this thesis, hardware is not depending on number of users .By using this system it can make your device to work in the presence of a particular person. In existing systems, everyone can access any device. So there is a need to design a security system which on the one hand is cheap and on the other hand provide the security of access to particular person having particular card.

1.6 Objectives of our project

Electronic access system control generally refers to the substitution of keys with electronically created cards. Biometric identification is more reliable and capable than the traditional knowledge based techniques differentiating between an authorized and an imposter. In this technology distinguishing traits such as fingerprint, face or voice recognizes a person. An ideal biometric should be universal, permanent and collectable. Fingerprint technology of biometric identification has high uniqueness, high permanence and high performance. But its circumvention is also high, that means it is easy to fool the system through fraudulent method. Environmental conditions also affect the biometric system. When humidity level is increased, the exact fingerprint cannot be taken. Combination of electronic access system and biometric system will give good results.

The objective of present dissertation is to develop a low cost physical secure system and to minimize power loss. This electronic identification system will allow convenient and efficient access to all card-related services. Smart cat allows elimination of inefficiencies that have characterized public service systems in the past paper based cards. Also storage and transmission of sensitive personal data will be handled securely. Users should gain confidence in these systems as everyone will be benefit from the efficiencies and reduced cost. This provides maximum security to the overall system. Therefore, in our project of attendance registration to accomplish this objective we do the following things:

- To construct two RF transmitter and receiver unit with frequency alignments and design a port relay sensor unit with a mechanical door including buzzer, at the out port of PC parallel port.
- To design a software (using c language) for attendance registration for five employees of a company

CHAPTER 2

LITERATURE SURVEY AND RELEVANT THEORY

2.1 Literature survey and history

This section is intended to give a background to the work performed in the thesis. The purpose of this master's thesis is to investigate what secure electronic access system is feasible. This investigation will be based on a theoretical study and a practical test assessment and a prototype will therefore have to be built.

In 1946 Léon Theremin invented an espionage tool for the Soviet Union which retransmitted incident radio waves with audio information. Sound waves vibrated a diaphragm which slightly altered the shape of the resonator, which modulated the reflected radio frequency. Even though this device was a passive covert listening device, not an identification tag, it is considered to be a predecessor of RFID technology. The technology used in RFID has been around since the early 1920s according to one source (although the same source states that RFID systems have been around just since the late 1960s).

Similar technology, such as the IFF transponder invented in the United Kingdom in 1939, was routinely used by the allies in World War II to identify aircraft as friend or foe. Transponders are still used by most powered aircrafts to this day.

Another early work exploring RFID is the landmark 1948 paper by Harry Stockman, titled "Communication by Means of Reflected Power" (Proceedings of the IRE, pp 1196–1204, October 1948). Stockman predicted that "...considerable research and development work has to be done before the remaining basic problems in reflected-power communication are solved, and before the field of useful applications is explored."

Mario Cardullo's U.S. patent 3,713,148 in 1973 was the first true ancestor of modern RFID; a passive radio transponder with memory. The initial device was passive, powered by the interrogating signal, and was demonstrated in 1971 to the New York Port Authority and other potential users and consisted of a transponder with 16 bit memory for use as a toll device. The basic Cardullo patent covers the use of RF, sound and light as transmission media. The original business plan presented to investors in 1969 showed uses in transportation (automotive vehicle identification, automatic toll system, electronic license plate, electronic manifest, vehicle routing, vehicle performance monitoring), banking (electronic check book, electronic credit card), security (personnel identification, automatic gates, surveillance) and medical (identification, patient history).

A very early demonstration of reflected power (modulated backscatter) RFID tags, both passive and semi-passive, was performed by Steven Depp, Alfred Koelle, and Robert Freyman at the Los Alamos National Laboratory in 1973[2]. The portable system operated at 915 MHz and used 12-bit tags. This technique is used by the majority of today's UHFID and microwave RFID tags. Now what exactly is a tag is explained below.

2.2 Tag

An RFID tag is a microchip combined with an antenna in a compact package; the packaging is structured to allow the RFID tag to be attached to an object to be tracked. The tag's antenna picks up signals from an RFID reader or scanner and then returns the signal, usually with some additional data (like a unique serial number or other customized information). RFID tags can be very small – the size of a large rice grain. Others may be the size of a small paperback book. The two major types of tags are:-

2.2.1 Active tag

An RFID tag is an active tag when it is equipped with a battery that can be used as a partial or complete source of power for the tag's circuitry and antenna. Some active tags contain replaceable batteries for years of use; others are sealed units. (Note that it is also possible to connect the tag to an external power source.)

The major advantages of an active RFID tag are:

- It can be read at distances of one hundred feet or more, greatly improving the utility of the device
- It may have other sensors that can use electricity for power.

The problems and disadvantages of an active RFID tag are:

- The tag cannot function without battery power, which limits the lifetime of the tag.
- The tag is typically more expensive, often costing $20 or more each
- The tag is physically larger, which may limit applications.
- The long-term maintenance costs for an active RFID tag can be greater than those of a passive tag if the batteries are replaced.
- Battery outages in an active tag can result in expensive misreads.

Active RFID tags may have all or some of the following features:

- longest communication range of any tag
- the capability to perform independent monitoring and control
- the capability of initiating communications
- the capability of performing diagnostics
- the highest data bandwidth
- Active RFID tags may even be equipped with autonomous networking; the tags autonomously determine the best communication path.

2.2.2 Passive tag

A passive tag is an RFID tag that does not contain a battery; the power is supplied by the reader. When radio waves from the reader are encountered by a passive RFID tag, the coiled antenna within the tag forms a magnetic field. The tag draws power from it, energizing the circuits in the tag. The tag then sends the information encoded in the tag's memory.

The major disadvantages of a passive RFID tag are:

- The tag can be read only at very short distances, typically a few feet at most. This greatly limits the device for certain applications.
- It may not be possible to include sensors that can use electricity for power.
- The tag remains readable for a very long time, even after the product to which the tag is attached has been sold and is no longer being tracked.

The advantages of a passive tag are:

- The tag functions without a battery; these tags have a useful life of twenty years or more.
- The tag is typically much less expensive to manufacture
- The tag is much smaller (some tags are the size of a grain of rice). These tags have almost unlimited applications in consumer goods and other areas.

2.3 Important terms and components

2.3.1 Antenna

The antenna in an RFID tag is a conductive element that permits the tag to exchange data with the reader. Passive RFID tags make use of a coiled antenna that can create a magnetic field using the energy provided by the reader's carrier signal.

2.3.2 Back Scatter

RFID tags sometimes make use of a method of communication called back scatter. Tags using back scatter technology reflect the reader's signal right back, modulating the signal to transmit data.

2.3.3 Smart card:

It is another way to refer to a contact less smart card. This term refers to identification cards (for example, some credit cards) that do not need to make contact with the reader to be read, or swiped in a special slot. This capability is implemented using a tiny RFID tag in the card; the intent is to provide the user with greater convenience by speeding checkout or authentication processes.

2.3.4 Transponder

An RFID transponder is a special kind of radio transmitter and receiver. It is activated when it receives a signal of a specific kind. RFID transponders are present in smart cards and Radio Frequency Identification tags.

2.3.5. Reader

An RFID reader is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data. A number of factors can affect the distance at which a tag can be read (the read range). The frequency used for identification, the antenna gain, the orientation and polarization of the reader antenna and the transponder antenna, as well as the placement of the tag on the object to be identified will all have an impact on the RFID system's read range.

2.3.6 Error Correcting Code (ECC) and Error Correcting Protocol (ECP)

When product data is placed on an RFID tag, a special piece of data called an error correcting code is created based on the product data using a known algorithm. The algorithm (or rule) used to create the correcting code is called the error correcting protocol. When the tag is activated and read, the reader pulls out the product data as well as the ECC. The reader uses the error correcting protocol on the product data, and compares the result to the ECC. If they match, the reader knows that the data has been read correctly. Similar methods are used in most data transfer systems to ensure the correctness of each data packet as it moves from one part of the system to another. A reader that performs this check automatically is said to be in error correcting mode.

2.4 APPLICATIONS OF RFID

Radio Frequency Identification has many applications because of its efficient and cheap service. A lot of research is being done to find better uses of this technology. Some of the applications of RFID are discussed below.

2.4.1 RFID and asset management

RFID (Radio Frequency Identification) combined with mobile computing and Web technologies provide an effective way for organizations to identify and manage their assets. Mobile computers, with integrated RFID readers, can now deliver a complete set of tools that eliminate paperwork, give positive proof of identification and prove attendance. Errors are virtually eliminated as this approach removes manual data entry. Web based management tools allow organizations to monitor their assets and make management decisions from anywhere in the world. Web based applications now mean that third parties, such as manufacturers and contractors can be granted access to update asset data, including for example, inspection history and transfer documentation online ensuring that the end user always has accurate, real-time data. Organizations within the Plant industry are already using RFID tags combined with a mobile asset management solution to record and monitor the location of their assets, their current status, whether they have been maintained and most importantly if they comply with HSE regulations. Fitters within depots and those working remotely on project/client sites use mobile computers to complete and record job instructions. These completed work records are then synchronized with a web based database allowing support and administration staff to respond accordingly.

2.4.2 Transportation and logistics

- Logistics & Transportation is a major area of implementation for RFID technology. For example, Yard Management, Shipping & Freight and Distribution Centers are some areas where RFID tracking technology is used. Transportation companies around the world value RFID technology due to its impact on the business value and efficiency.
- The North American railroad industry operates an automatic equipment identification system based on RFID. Locomotives and rolling stock are equipped with two passive RFID tags (one mounted on each side of the equipment); the data encoded on each tag identifies the equipment owner, car number, type of equipment, number of axles, etc. The equipment owner and car number can be used to derive further data about the physical characteristics of the equipment from the Association of American Railroads' car inventory database and the railroad's own database indicating the lading, origin, destination, etc. of the commodities being carried.[17]
- Baggage passing through the Hong Kong International Airport is individually tagged with "HKIA" RFID tags as they navigate the airport's baggage handling system, which improves efficiency and reduces misplaced items.

2.4.3 Human implants

Implantable RFID chips designed for animal tagging are now being used in humans. An early experiment with RFID implants was conducted by British professor of cybernetics Kevin Warwick, who implanted a chip in his arm in 1998. In 2004 Conrad Chase offered implanted chips in his night clubs in Barcelona, Spain and in Rotterdam, The Netherlands, to identify their VIP customers, who in turn use it to pay for drinks.

Figure 2.1: Just after insertion of RFID tag.

In 2004, the Mexican Attorney General's office implanted 18 of its staff members with the Verichip to control access to a secure data room.

Security experts have warned against using RFID for authenticating people due to the risk of identity theft. For instance a man-in-the-middle attack would make it possible for an attacker to steal the identity of a person in real-time. Due to the resource constraints of RFIDs it is virtually impossible to protect against such attack models as this would require complex distance-binding protocols.

2.4.4 Libraries

Among the many uses of RFID technologies is its deployment in libraries. This technology has slowly begun to replace the traditional barcodes on library items (books, CDs, DVDs, etc.). The RFID tag can contain identifying information, such as a book's title or material type, without having to be pointed to a separate database (but this is rare in North America). The information is read by an RFID reader, which replaces the standard barcode reader commonly found at a library's circulation desk. The RFID tag found on library materials typically measures 50 mm X 50 mm in North America and

50 mm x 75 mm in Europe. It may replace or be added to the barcode, offering a different means of inventory management by the staff and self service by the borrowers. It can also act as a security device, taking the place of the more traditional electromagnetic security strip and not only the books, but also the membership cards could be fitted with an RFID tag.

While there is some debate as to when and where RFID in libraries first began, it was first proposed in the late 1990s as a technology that would enhance workflow in the library setting. Singapore was certainly one of the first to introduce RFID in libraries and Rockefeller University in New York may have been the first academic library in the United States to utilize this technology, whereas Farmington Community Library in Michigan may have been the first public institution, both of which began using RFID in 1999. In Europe, the first public library to use RFID was the one in Hoogezand-Sappemeer, the Netherlands, in 2001, where borrowers were given an option. To their surprise, 70% used the RFID option and quickly adapted, including elderly people.

Worldwide, in absolute numbers, RFID is used most in the United States (with its 300 million inhabitants), followed by the United Kingdom and Japan. It is estimated that over 30 million library items worldwide now contain RFID tags, including some in the Vatican Library in Rome.

2.4.5 Social retailing

When customers enter a dressing room, the mirror reflects their image and also images of the apparel item being worn by celebrities on an interactive display. A webcam also projects an image of the consumer wearing the item on the website for everyone to see. This creates an interaction between the consumers inside the store and their social network outside the store. The technology in this system is an RFID interrogator antenna in the dressing room and Electronic Product Code RFID tags on the apparel item.

2.4.6 Transportation Payments

RFID is being used for E – Tolling in Motorways, Pakistan, Implemented by NADRA.Throughout Europe, and in particular in Paris (system started in 1995 by the RATP), Lyon, Bordeaux, Nancy and Marseilles in France, in the whole of the Portuguese highway system and in many Portuguese public car parks, Milan, Turin, and Florence in Italy, and Brussels in Belgium, RFID passes conforming to the Calypso (RFID) international standard are used for public transport systems. They are also used now in Canada (Montreal), Mexico, Israel, Bogotá and Pereira in Colombia, Stavanger in Norway, Luxembourg, etc.

In Electronic Road Pricing gantry at Singapore. Gantries such as these collect tolls in high-traffic areas from active RFID units in vehicles.

In Toronto, Ontario, Canada and surrounding areas, Electronic Road Pricing systems are used to collect toll payments on Highway 407.

In Seoul, South Korea and surrounding cities, T-money cards can be used to pay for public transit. Some other South Korean cities have adopted the system, which can also be used in some stores as cash. T-money replaced Pass, first introduced for transport payments in 1996 using MIFARE technology.

- In Turkey, RFID has been used in the motorways and bridges as a payment system over ten years. It is also used in electronic bus tickets in Istanbul.
- In Hong Kong, mass transit is paid for almost exclusively through the use of an RFID technology, called the Octopus Card. Originally it was launched in September 1997 exclusively for transit fare collection, but has grown to be similar to a cash card, and can still be used in vending machines, fast-food restaurants and supermarkets. The card can be recharged with cash at add-value machines or in shops, and can be read several centimeters from the reader. The same applies for Delhi Metro, the rapid transit system in New Delhi, capital city of India.

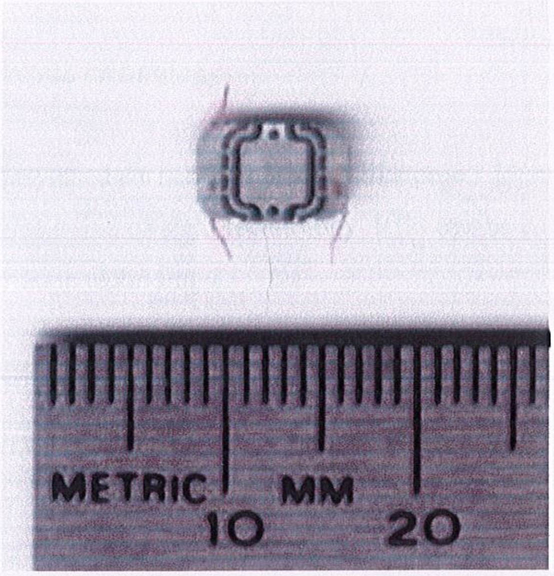


Figure 2.2: Pay Pass RFID chip removed from a MasterCard.

- **The Moscow Metro, the world's second busiest,** was the first system in Europe to introduce RFID smartcards in 1998.

2.5 Potential uses

RFID can be used in a variety of applications such as

- Access management
- Tracking of goods and RFID in retail
- Tracking of persons and animals
- Toll collection and contact less payment
- Machine readable travel documents
- Smart dust (for massively distributed sensor networks)
- Location-based services
- Tracking Sports memorabilia to verify authenticity

2.6 Comparison to Barcode technology

The technology commonly used earlier for purposes like object identification was bar code technology. This was a line of sight technology. Rfid can be called a far better and advanced version of bar code technology.

RFID	**Barcode**
Counterfeiting is difficult	Counterfeiting is easy
Scanner not required. No need to bring the tag near the reader	Scanner needs to see the bar code to read it
RFID is comparatively fast	
Can read multiple tags	Can read only one tag at a time
Relatively expensive as compared to Bar Codes (Reader 1000$, Tag 20 cents a piece)	
Can be reused within factory premises	Cannot be reused

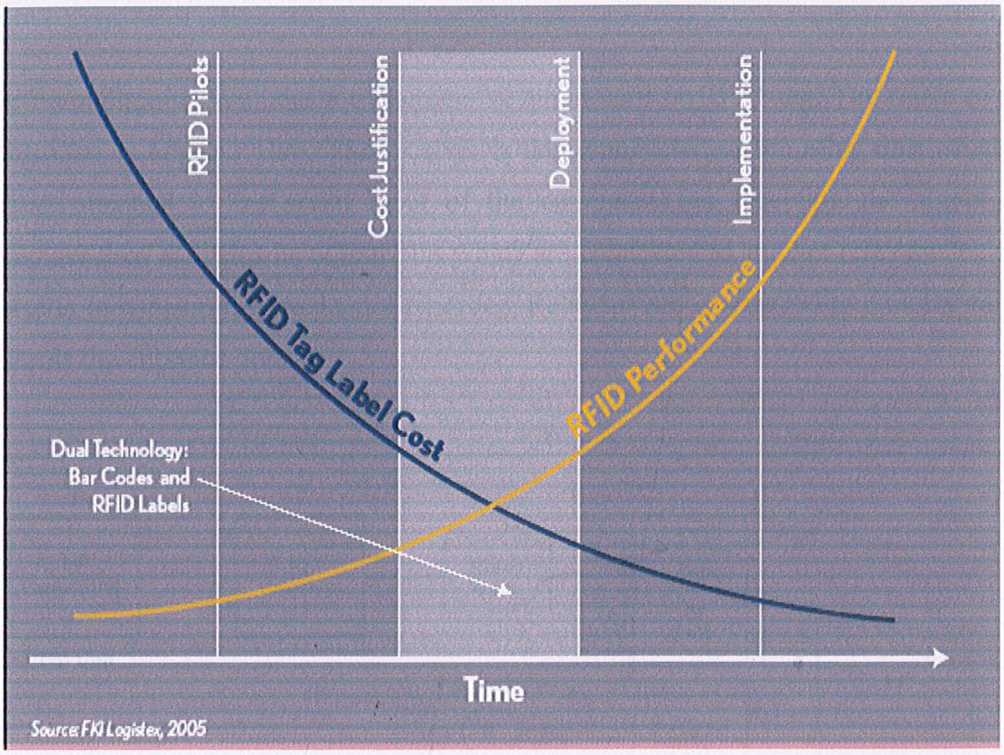
Table 2.1: Comparison of RFID and Barcode technology

It offers many more features than bar code or other previously used technology, though the technology is on the expensive side at the moment but with recent advancements manufacturers have been able to cut off cost and the technology is becoming hugely popular with its various benefits.

Because radio waves are used to sense the tag, RFID has the advantage that no line-of-sight alignment is required between the RFID tag and the reader. What this means is that the RFID reader can read multiple tags simultaneously and instantly. The tags may be embedded inside an object such as a container or in a garment. Furthermore, RFID tags can store a lot more information than bar codes. Imagine a big carton with hundreds of boxes of shirts of different sizes and colors, each tagged with an RFID. The moment the carton reaches the warehouse or the store, the RFID reader immediately identifies all the RFID tags and information about the inventory such as the number of shirts, types, sizes, colors etc, is instantly available on a PC terminal, without even having to open the carton!

2.7 RFID GAINING POPULARITY

Interest in radio frequency identification (RFID) is on the rise, according to a survey conducted by the Computing Technology Industry Association (CompTIA). The worldwide survey of 155 IT companies found that 46% of their customers have implemented one or more RFID solutions, either as pilot projects or production deployments. This represents a 12% jump over 2007-2008, when IT companies reported 34% of their customers had initiated RFID projects. The most popular RFID deployments, according to the survey, are asset tracking (32%), personal identification (28%), supply chain (25%), retail marketing (15%), and closed-loop manufacturing (9%), according to the CompTIA survey.



Source: FKI Logistex, 2005

Figure 2.3: Graph showing increasing efficiency and declining cost of RFID technology.

Chapter 3
HARDWARE DISCRIPTION

3.1 Block Diagram of System

The main circuitry includes a transmitter or smart card or RFID tag. The range of the transmitter is approx. 10m. The receiver is then connected to the relay unit which is further attached to the serial input of the computer. On receiving the signal the computer then activates its output pins which are connected to another relay switch and a buzzer to confirm the attendance recorded. Relay switch is attached to a motor which controls the entrance door.

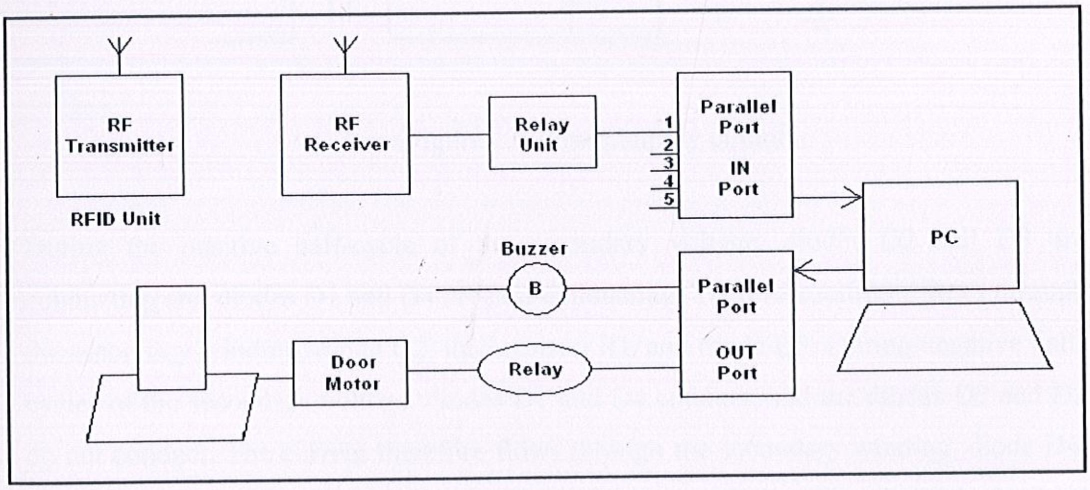


Figure 3.1: System Block Diagram

The basic components used for the design of "RFID based attendance monitoring system" are:

- Power supply source
- Radio Frequency Transmitter Unit
- Radio Frequency Receiver Circuit

- Relay switching unit
- RFT (RF transformer)
- Trimmer (Variable Capacitor)

3.2 Power supply source

The source of the power supply is the ac input from the normal 220v switch. The supply is then rectified using a Bridge Wave Rectifier. The figure below shows the circuit diagram and the components used

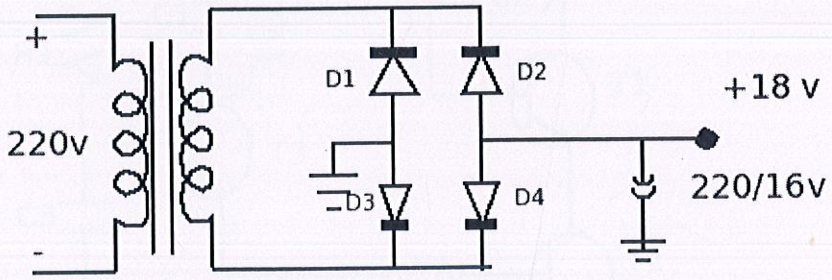


Figure3.2: Power supply circuit

During the positive half-cycle of the secondary voltage, diodes D2 and D3 are conducting and diodes D1 and D4 are non-conducting. Therefore, current flows through the secondary winding, diode D2, load resistor RL and diode D3. During negative half-cycles of the secondary voltage, diodes D1 and D4 conduct, and the diodes D2 and D3 do not conduct. The current therefore flows through the secondary winding, diode D4, load resistor RL and diode D4. In both cases, the current passes through the load resistor in the same direction. Therefore, a fluctuating, unidirectional voltage is developed across the load.

3.3 Radio Frequency Transmitter Unit

This part of the project is supposed to be in the hands of the employee. This is in form of a card which contains the code known as EPC (Electronic Product Code) which further contains the identity of an employee. The circuit diagram of the transmitter is shown below with the component list used in the circuit.

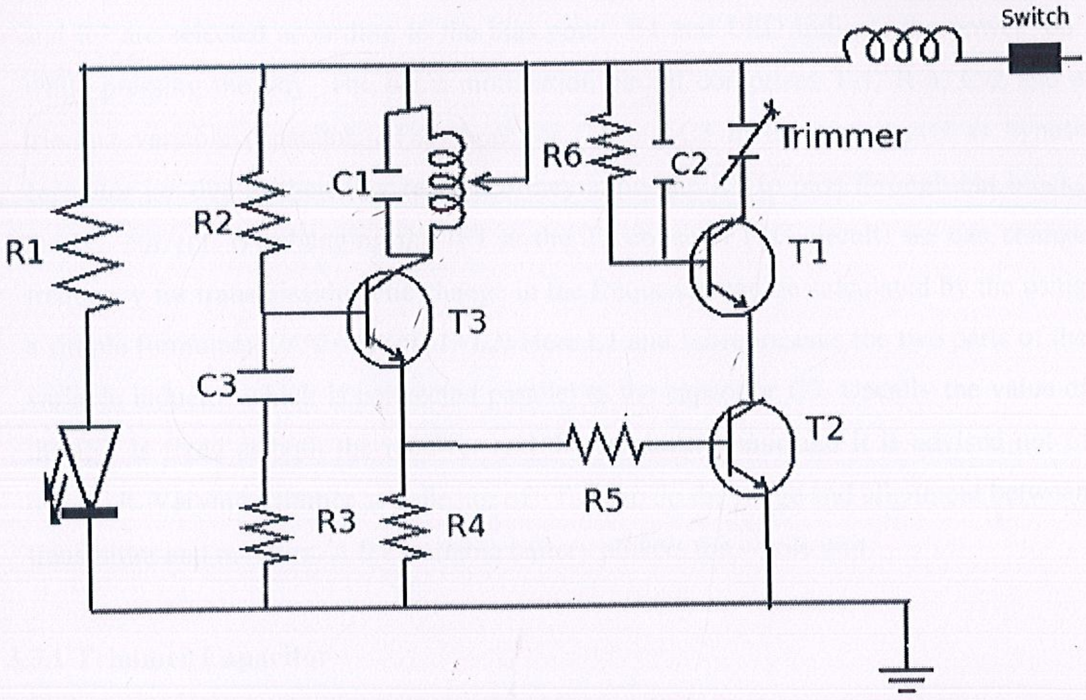


Figure 3.3 Circuit Diagram of Transmitter Unit

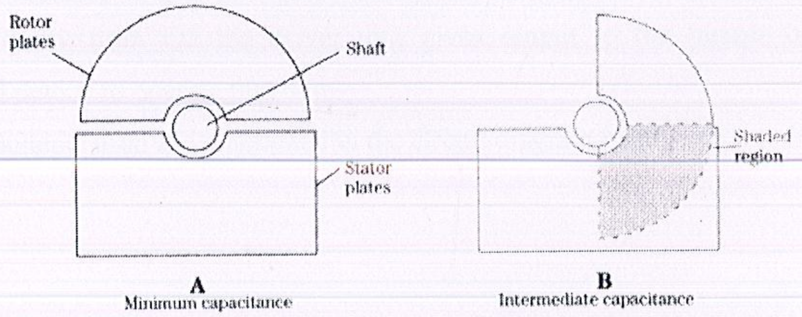
The components used here are:

R1	-	100 ohms
R2	-	330K ohm
R3, R4, R5	-	2K ohm
R6	-	47K ohm
C1	-	.022
C2, C3	-	.001
T1,T3	-	BF494
T2	-	BC548

As shown in figure 3.2, the RF remote transmitter contains an oscillator comprising one BF-194 {T1} which is used as radio frequency modulator transistor. This transistor is coupled with CE configuration with other NPN 548 {T2} transistor for biasing. The basic oscillator is formed by transistor T3 working under CE configuration. From the collector an LC circuit is generating the source oscillation that super imposes to the T-2 base from its emitter follower circuit. R2 provides biasing Vcc to T3.The value of R2 and R3 are selected according to the bias point. R1 and LED indicate the power 'on' while pressing the key. The basic modulation circuit comprises T-1, R-6, C-2 and a trimmer variable capacitor. The capacitor C2 and C3 in the circuit acts as bypass capacitor i.e. due to their low reactance they allow the RF to pass through but blocks the DC current. By changing the IFT at the T3 collector (LC circuit) we can change frequency for transmission. The change in the frequency can be calculated by the using a simple formulae: $1/f\,\hat{}\,2= C1*(L1+L2)$ Here L1 and L2 represents the two parts of the variable inductor which is connected parallel to the capacitor C3. Usually the value of the IFT is fixed at both the receiver and the transmitter unit and it is advised not to disturb it. Varying trimmer at collector of T-1 can do the range and alignment between transmitter and receiver. A 9V portable battery powers the whole unit.

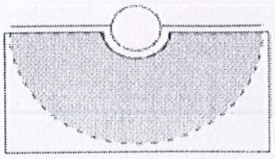
3.3.1 Trimmer Capacitor

Trimmer capacitor is used both at the transmitter or the receiver end to do range and alignment. Rotating the shaft changes the capacitance value and thus the frequency also changes. While rotating the shaft never uses a metal strip prefer a plastic material.



A
Minimum capacitance

B
Intermediate capacitance



C
Maximum capacitance

Figure 3.4: Variation in Trimmer capacitance with shaft rotation

The capacitance of the air variable capacitor is determined by how much of the rotor plate is shaded by the stator plates. In the above figure A) represents minimum capacitance, B) intermediate capacitance, C) maximum capacitance. By varying the capacitance we can adjust the frequency of the circuit to align the receiver and transmitter unit.

3.4 Radio Frequency Receiver Circuit

In the receiver circuit, in Figure3.4, the transmitter Q1 also working as LC tank circuit basic oscillator that receives the variable frequencies. The different frequencies mentioned here are the signals received from different cards. R1 and LED indicate the reception of the signal while pressing the key. Q2, Q3 are two basic low power amplifier provides amplification to all frequencies. L2 coil (IFT) selects the specific frequency to further amplifiers and fed at the base of Q4 via R-14 resistor. The power amplification is provided by Q5 transistor. In the circuit R2 and R3 provides biasing Vcc to Q1. The values of R2 and R3 are set according to the bias point. Similarly R10 provides biasing Vcc+ to Q2 transistors. C1 and R5 give CE follower circuit for Q1 and same as for Q2 as R8 and C6 doing the same function. Rest other resistor and capacitor provides necessary basing Vc and frequency cut off function at different stages of the circuit. Finally from Q5 the driver unit gives output to the buzzer or any other connected device to operate that unit.

The components used are mentioned in the circuit diagram itself.

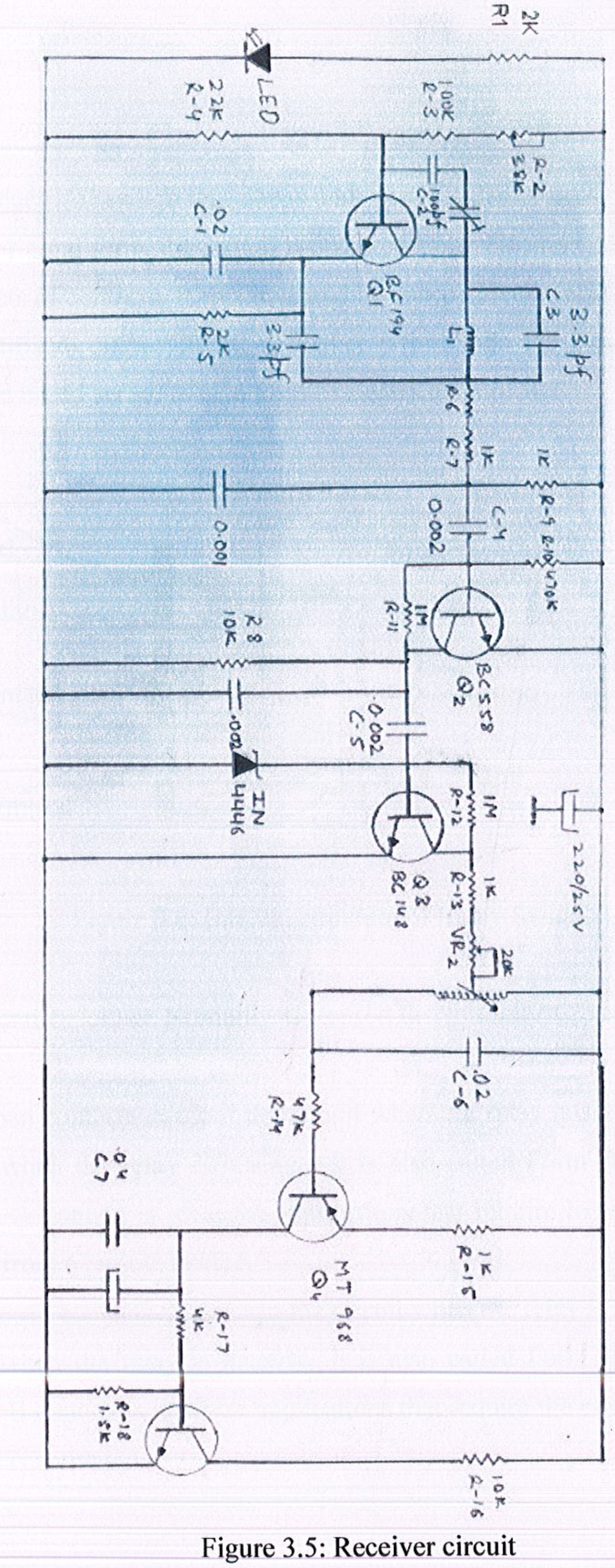


Figure 3.5: Receiver circuit

3.5 Relay unit

A relay is an electrical switch that opens and closes under control of another electrical circuit. In the original form, the switch is operated by an electromagnet to open or close one or many sets of contacts. It was invented by Joseph Henry in 1835. Because a relay is able to control an output circuit of higher power than the input circuit, it can be considered, in a broad sense, to be a form of electrical amplifier.

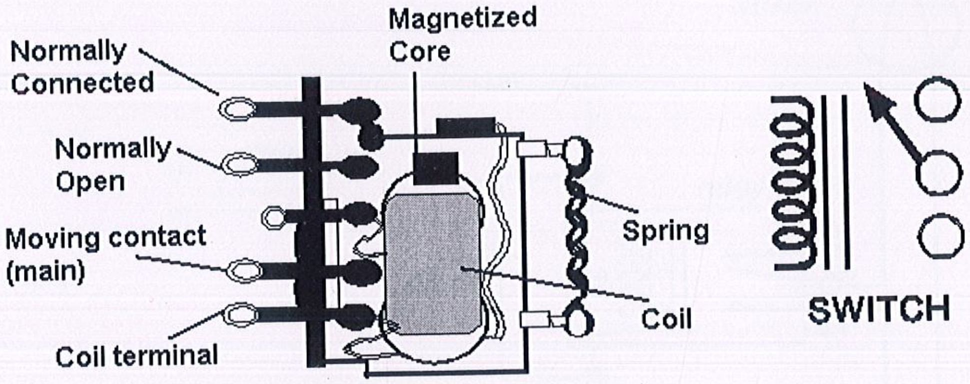


Figure 3.6: Internal structure of Relay Switch

The contacts can be either Normally Open (NO), Normally Closed (NC), or change-over contacts.

- Normally-open contacts connect the circuit when the relay is activated; the circuit is disconnected when the relay is inactive. It is also called Form A contact or "make" contact. Form A contact is ideal for applications that require to switch a high-current power source from a remote device.
- Normally-closed contacts disconnect the circuit when the relay is activated; the circuit is connected when the relay is inactive. It is also called Form B contact or "break" contact. Form B contact is ideal for applications that require the circuit to remain closed until the relay is activated.

- Change-over contacts control two circuits: one normally-open contact and one normally-closed contact with a common terminal. It is also called Form C contact.

3.5.1 Relay operation

Relay requires a current through their coils, for which a voltage is applied. This voltage for a relay can be D.C. low voltages up to 24V or could be 240V a.c.

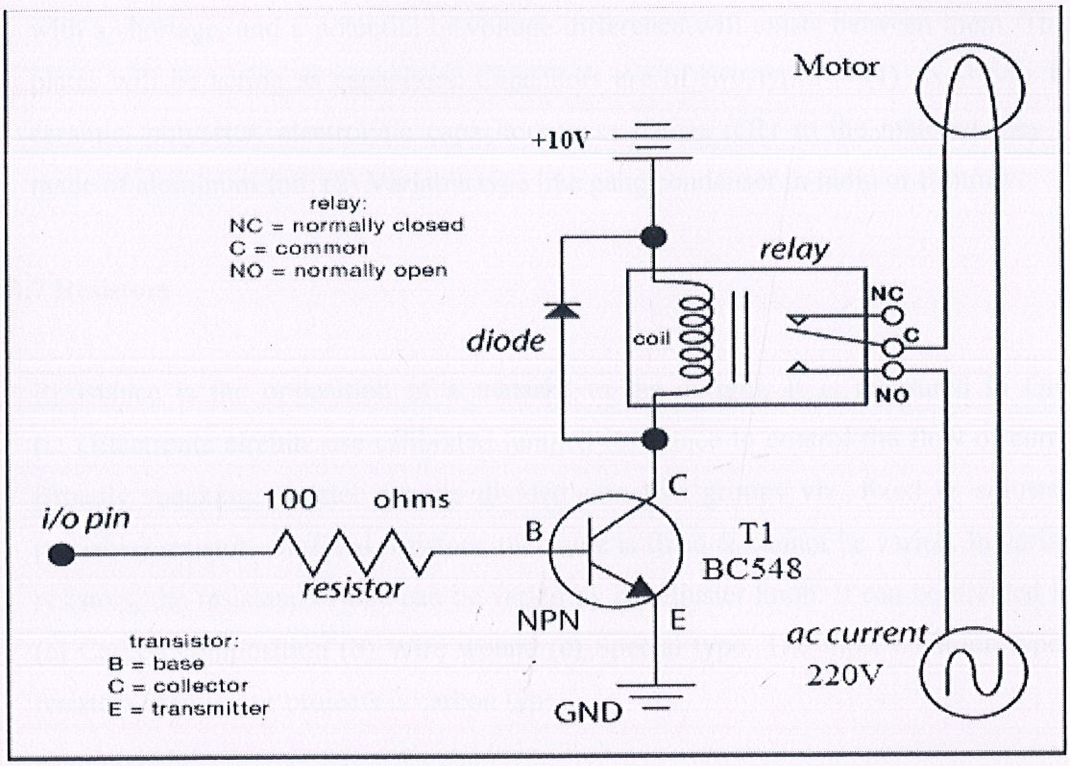


Figure 3.7: Corresponding Relay circuit

The circuit is simple NPN transistor common emitter switching circuit. The transistor T-1 is supplied through negative at emitter. The base is conducted through the port output from computer and collector gives output to energies the relay commonly connected to +ve supply. The diode prevents back emf produced by relay while working.

3.6 Capacitors

It is an electronic component whose function is to accumulate charges and then release it. To understand the concept of capacitance, consider a pair of metal plates which all are placed near to each other without touching. If a battery is connected to these plates the positive pole to one and the negative pole to the other, electrons from the battery will be attracted from the plate connected to the positive terminal of the battery. If the battery is then disconnected, one plate will be left with an excess of electrons, the other with a shortage, and a potential or voltage difference will exists between them. These plates will be acting as capacitors. Capacitors are of two types: - (1) fixed type like ceramic, polyester, electrolytic capacitors-these names refer to the material they are made of aluminum foil. (2) Variable type like gang condenser in radio or trimmer.

3.7 Resistors

Resistance is the opposition of a material to the current. It is measured in Ohms (□).Electronic circuits use calibrated lumped resistance to control the flow of current. Broadly speaking, resistor can be divided into two groups viz. fixed & adjustable (variable) resistors. In fixed resistors, the value is fixed & cannot be varied. In variable resistors, the resistance value can be varied by an adjuster knob. It can be divided into (a) Carbon composition (b) Wire wound (c) Special type. The most common type of resistors used in our projects is carbon type.

3.8 Diodes

The simplest semiconductor device is made up of a sandwich of P-type semi conducting material, with contacts provided to connect the p-and n-type layers to an external circuit. This is a junction Diode. If the positive terminal of the battery is connected to the p-type material (cathode) and the negative terminal to the N-type material (Anode), a large current will flow. This is called forward current or forward biased.

3.8.1 Rectifier diodes

Rectifier diodes are used in power supplies to convert alternating current (AC) to direct current (DC), a process called rectification. They are also used elsewhere in circuits where a large current must pass through the diode. All rectifier diodes are made from silicon and therefore have a forward voltage drop of 0.7V. The 1N4001 is suitable for most low voltage circuits with a current of less than 1A.

3.9 Light Emitting Diodes (LEDs)

LED must have a resistor connected in series to limit the current through the LED, otherwise it will burn out almost instantly.

The resistor value, R is given by:

R = (VS - VL) / I

VS = supply voltage

VL = LED voltage (2V)

I = LED current (A)

If the calculated value is not available choose the nearest standard resistor value which is greater, so that the current will be a little less than you chose.

3.10 Picture of Product

One portion of the figure shows the transponder/transmitter and the other shows the rest of the project showing the receiver, relay, transformer, buzzer, door, relay, motor and every other part. The four key controls are to act as dummy transponders for the receiver as we have built only one transmitter.

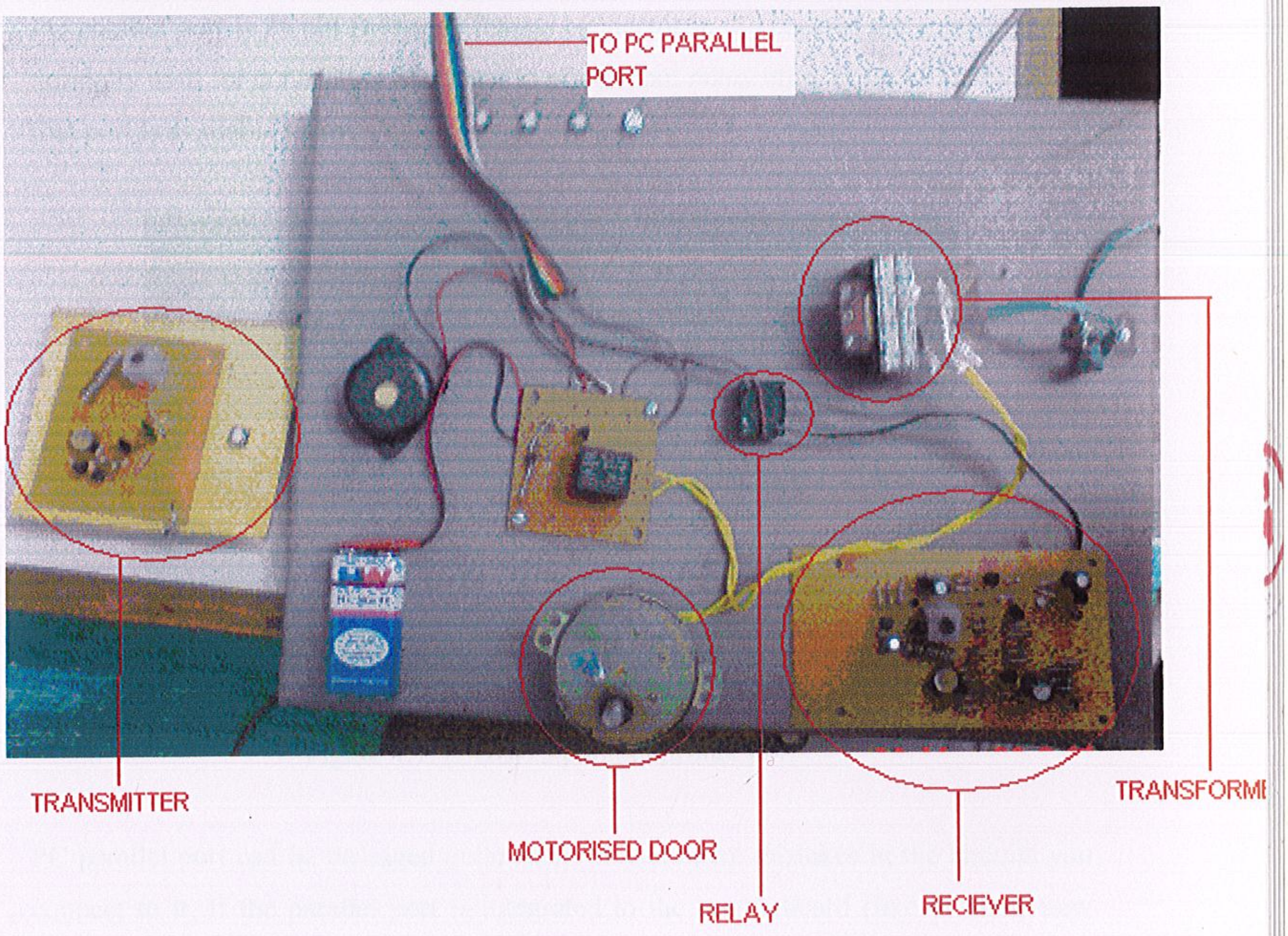


Figure 3.8: Labeled snapshot of the hardware

Chapter 4

Software Schematics

4.1 Parallel port interfacing

PC parallel port is 25 pin D-shaped female connector in the back of the computer. It is normally used for connecting computer to printer, but many other types of hardware for that port is available today.

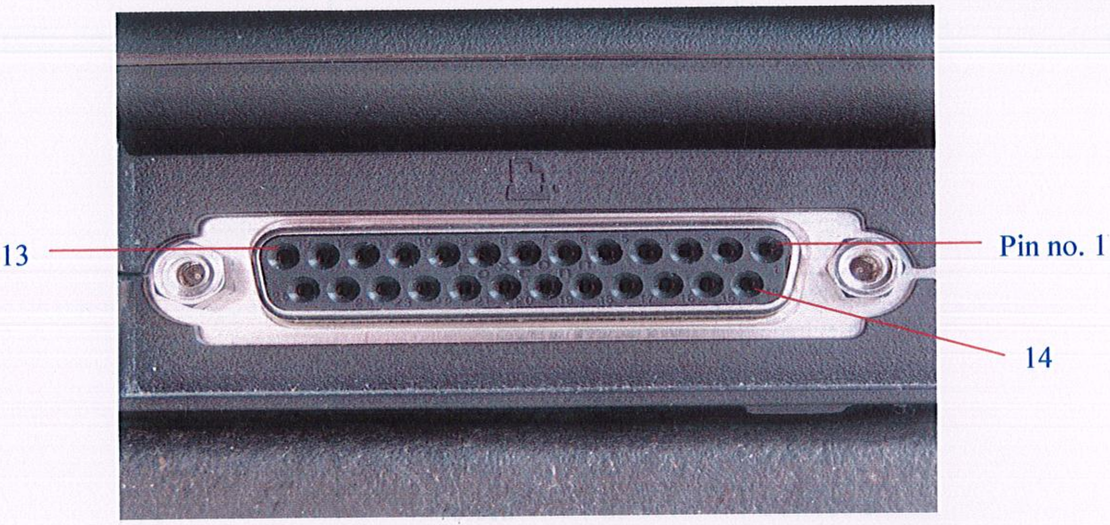


Figure 4.1: A DB-25 parallel printer port

PC parallel port can be damaged quite easily if you make mistakes in the circuits you connect to it. If the parallel port is integrated to the motherboard (like in many new computers) repairing damaged parallel port may be expensive (in many cases it is cheaper to replace the whole motherboard than repair that port).

4.1.1 Pin Structure of port

Pin no. (DB25)	Signal name	Direction	Register -bit
1	nStrobe	In/Out	Control-0
2	Data0	Out	Data-0
3	Data1	Out	Data-1
4	Data2	Out	Data-2
5	Data3	Out	Data-3
6	Data4	Out	Data-4
7	Data5	Out	Data-5
8	Data6	Out	Data-6
9	Data7	Out	Data-7
10	nAck	In	Status-6
11	Busy	In	Status-7
12	Paper-Out	In	Status-5
13	Select	In	Status-4
14	Linefeed	In/Out	Control-1
15	nError	In	Status-3
16	nInitialize	In/Out	Control-2
17	nSelect-Printer	In/Out	Control-3
18-25	Ground	-	-

Table 5.1: Pin out of DB-25

Signals with prefix 'n' are active low. That means, normally these pins will have low value. When it needs to send some indication, it will become high. Not all 25 are needed always. Usually you can easily do with only 8 output pins (data lines) and signal ground.

4.2 How to calculate your own values to send to program

You have to think the value you give to the program as a binary number. Every bit of the binary number control one output bit. The following table describes the relation of the bits, parallel port output pins and the value of those bits.

Pin	2	3	4	5	6	7	8	9
Bit	D0	D1	D2	D3	D4	D5	D6	D7
Value	1	2	4	8	16	32	64	128

For example if you want to set pins 2 and 3 to logic 1 (led on) then you have to output value 1+2=3. If you want to set on pins 3, 5 and 6 then you need to output value 2+8+16=26. In this way you can calculate the value for any bit combination you want to output.

4.3 Change in the program due to different computers

Our program includes some inport values like:

```
        ch=inportb(0x379);
        if(ch==63)
        {}
        else if(ch==255)
        {}
        else if(ch==95)
        {}
        else if(ch==111)
        {}
        else if(ch==119){}
```

The values 63, 255, 95, 111, 119 are the in port values taken by the parallel port.

In maximum computers these values are acceptable but in some computers it won't acceptable and thus we have to put new values in place of these. They are 56, 248, 88, 102, and 112.* these values are addition

*Thus you have to just subtract 7 from all the above values in the program given. The difference is due to the configuration some computers are 16 bit, some 32 bit etc.

4.4 Basics of the program

The program basically works on simple c language functions except there are certain functions which are used to take the input and give some values to the port. In Turbo C, there are following functions used for accessing the port:

- outportb(PORTID, data);
- data = inportb(PORTID);
- outport(PORTID, data);
- data = inport(PORTID);

Outport() function sends a word to port, inport() reads a word from the port. outportb() sends a byte to port and inportb() reads a byte from the port. If you include DOS.H header, these functions will be consiudered as macro, otherwise as functions. Function inport() will return a word having lower byte as data at PORTID and higher byte as data at PORTID+2. So, we can use this function to read status and control registers together. inportb() function returns byte at PORTID. outport() writes the lower byte to PORTID and higher byte to PORTID+1. So this can be used to write data and control together. outportb() function write the data to PORTID. outport() and outportb() returns nothing

Here is an example source code for C compiler:

```
#include <stdio.h>
#include <dos.h>
#include <conio.h>

/********************************************/
/* this program set the parallel port outputs*/
/********************************************/
```

```
void main (void)
{
clrscr();            /* clear screen */
outportb(0x378,0xff); /* output the data to parallel port , here 0xff is the data*/
getch();             /* wait for key press before exiting */}
```

Chapter 5

Results and Discussions

5.1 The smart card

As shown in the figure 3.3 the circuit of the transmitter unit contains a trimmer capacitor due to which it cannot be implemented on a breadboard. To make the circuit easy to mount we have used a special designed PCB. This PCB is available in the market as a remote switch PCB. While soldering the circuit must read the manual for soldering the trimmer and the IFT circuit, these can be destroyed due to over heat.

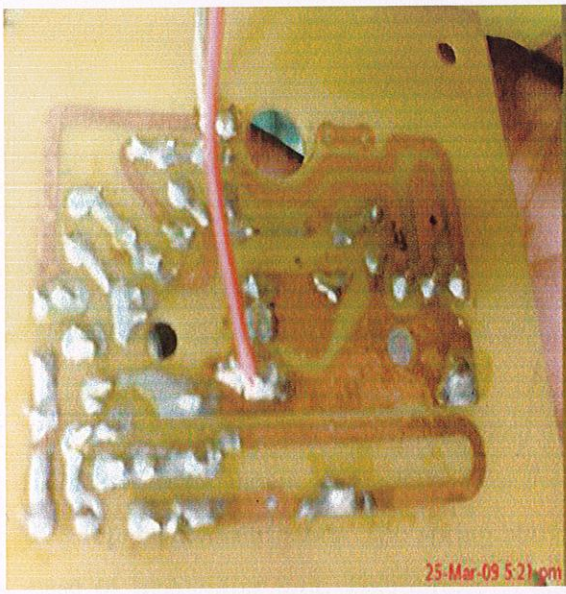


Figure 5.1a: The PCB of the transmitter unit

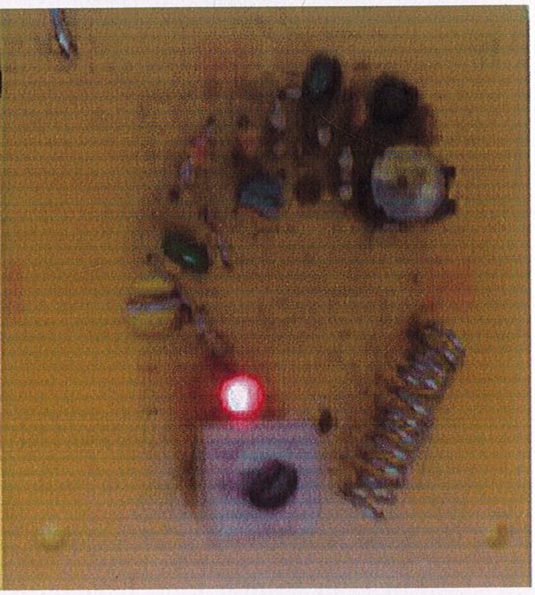


Figure 5.1b: Circuitry of the transmitter unit

Figure 5.1a shows the PCB layout of the card in including the soldered components. Figure 5.1b represents the circuit which includes a wire antenna; glowing LED proves that the circuit is in working mode and transmitting the RF signal to the receiver.

5.2 The receiver unit

The figure below shows the implemented circuit of the receiver unit which is further connected to the computer through the relay switch. Starting from left we have a bridge rectifier, a power amplification circuit and an LC tank circuit basic oscillator that receives the variable frequencies from different tags or smart cards.

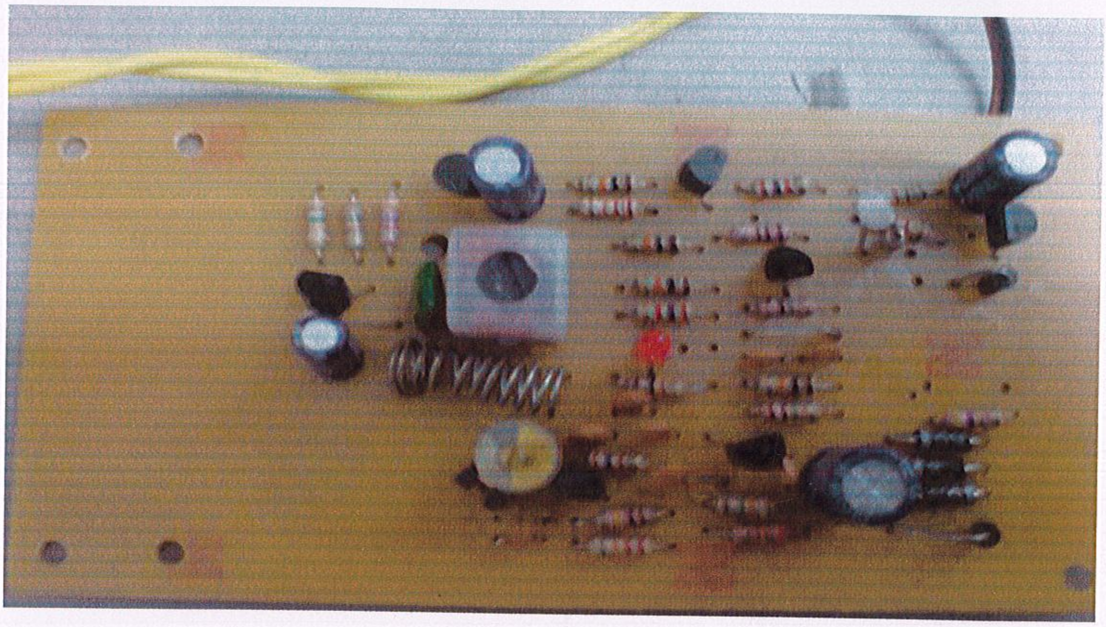


Figure 5.2: Snapshot of the receiver circuitry

. The two led's shown here are used for the power on and signal verification. Three pin ICs represents transistors. The spring shown above acts as an antenna same as in the case of transmitter unit. This circuit is also mounted on a printed PCB to make the implementation easy and to reduce the chances of error because any error in the circuit can result in damage to the interface and can even destroy the motherboard of the system.

5.3 Initializing the system

To run project we need to first install the port drivers. Then run the program and connect the wires. We will see a led glowing in the receiver unit which justifies that the connections are good and the unit is ready to operate. The monitor screen shows the options available.

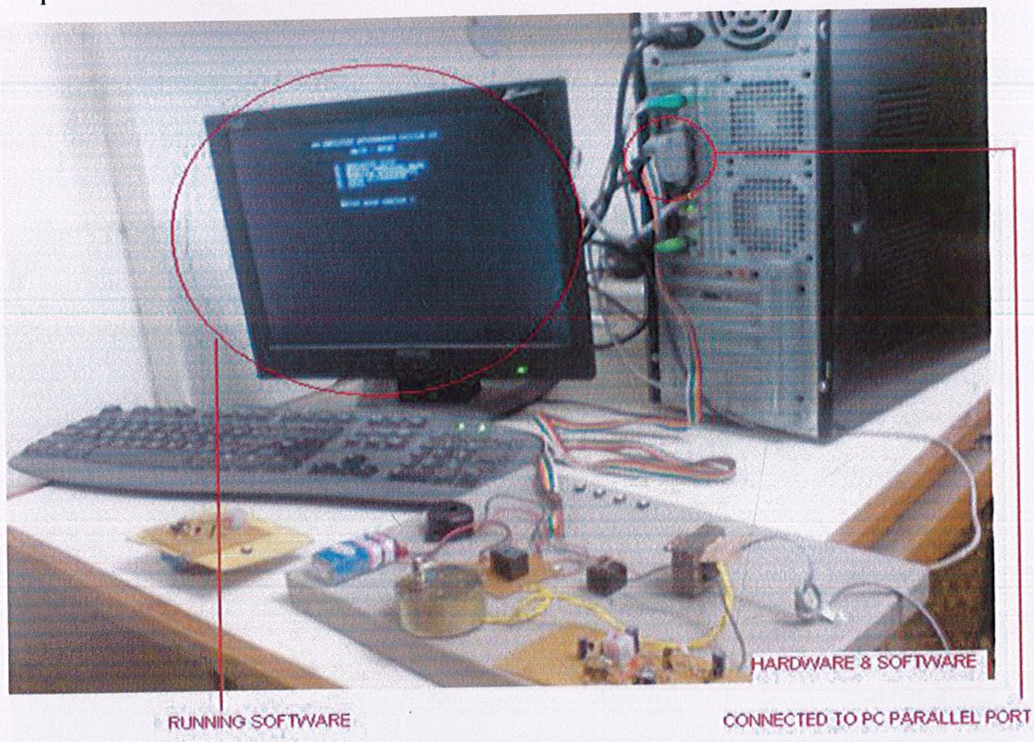
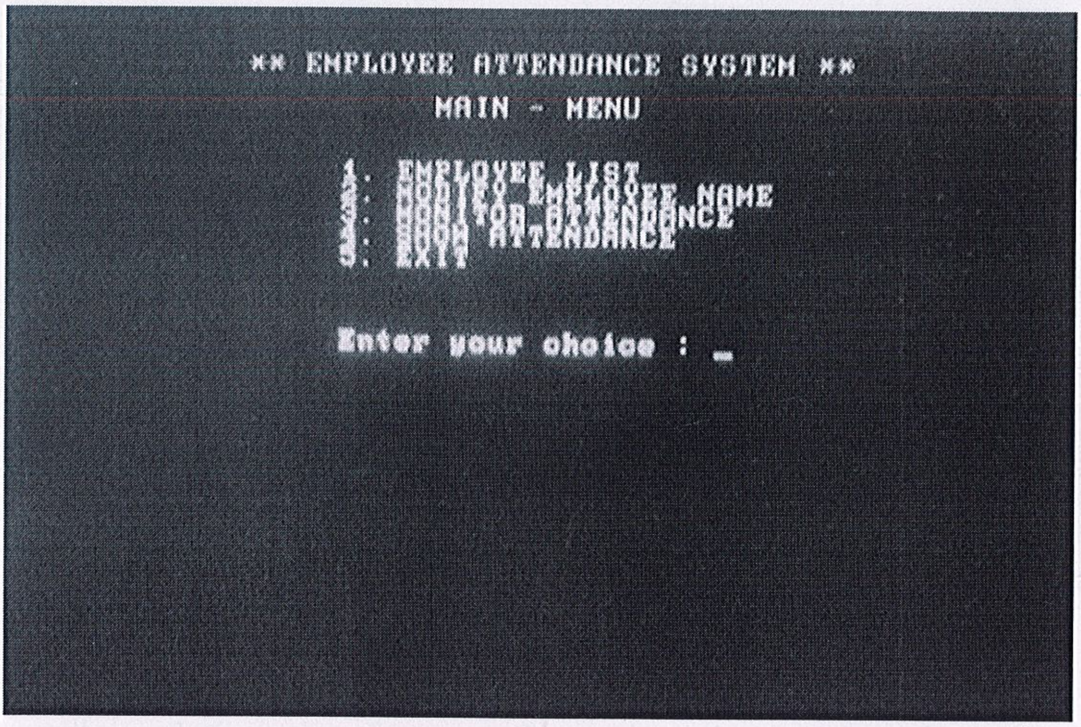


Figure 5.3: Picture of the system

5.4 Employee attendance system

The figure below is a snapshot of the project when interfaced with a computer. This picture depicts the main menu of the system. it is as introductory page to our system, form here every option can be accessed. Any option as mentioned below can be accessed by entering the number corresponding to the option. For example if the employee list has to be accessed, option 1 has to be entered by the user and the software will show the list of all the employees.



```
** EMPLOYEE ATTENDANCE SYSTEM **
          MAIN - MENU

      1: EMPLOYEE LIST
      2: MODIFY EMPLOYEE NAME
      3: MONITOR ATTENDANCE
      4: SHOW ATTENDANCE
      5: EXIT

      Enter your choice : _
```

j

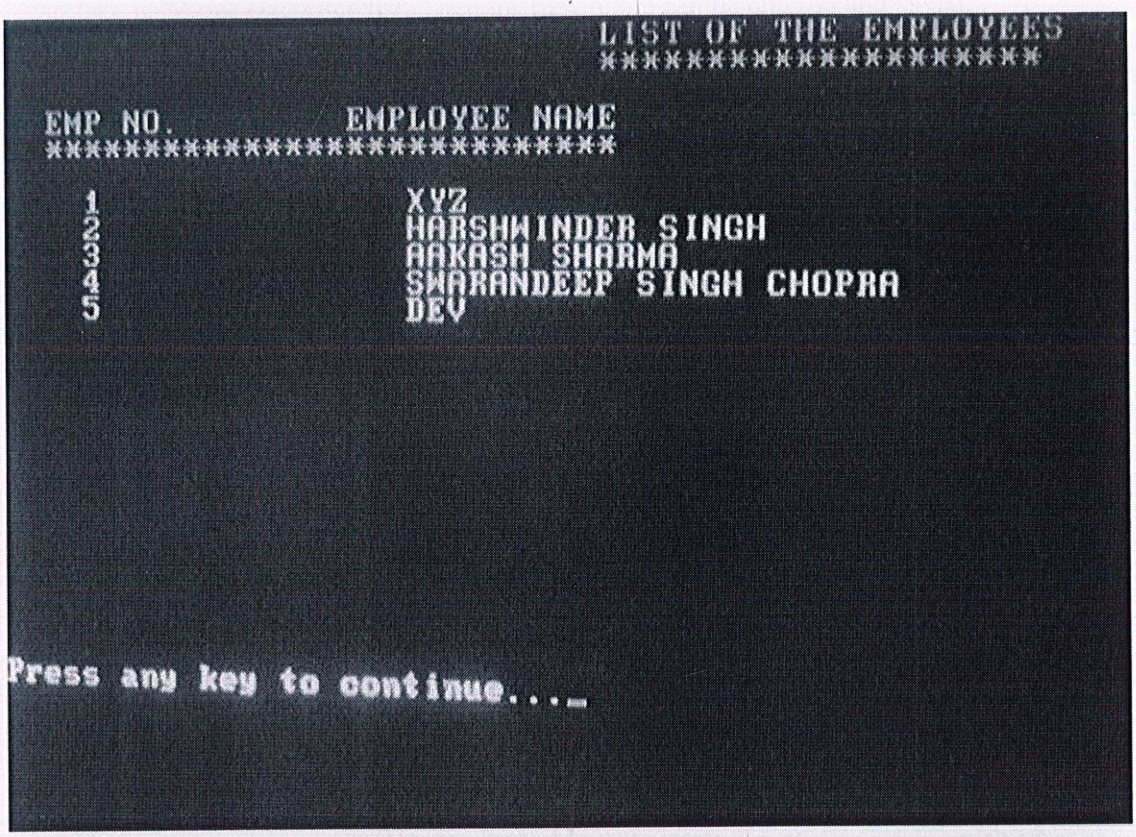
Figure 5.4: Snapshot of the main menu

The main menu of the project includes the following options:

- List of the employees working in the organization.
- Modify employee information.
- Monitoring attendance.
- Display of attendance of an employee with date and time.

5.4.1 List of employees

Employee list which for our specific example has been taken as a list of five employees only, it can extend to any number depending on the company's requirement.



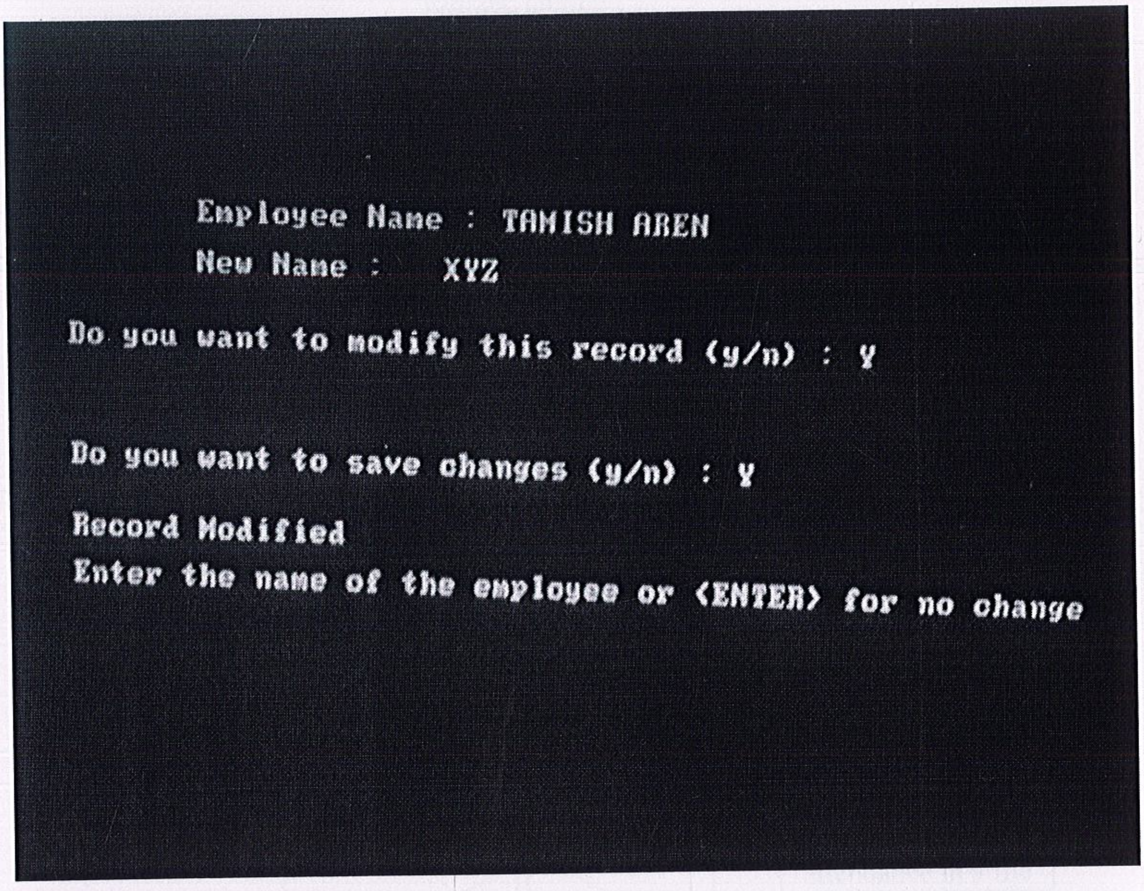
```
                                    LIST OF THE EMPLOYEES
                                    *********************

 EMP NO.          EMPLOYEE NAME
 *****************************

   1                   XYZ
   2                   HARSHWINDER SINGH
   3                   AAKASH SHARMA
   4                   SWARANDEEP SINGH CHOPRA
   5                   DEV




Press any key to continue...._
```

Figure 5.4: Results of option 1 of program

It will give a basic preview of the setup of the employees in the company, the employee list can be referred to as a help option whenever required. The list can be edited also depending on the current scenario of the company concerned.For example, if there is a resignation situation or by for any reason the setup needs to be changed or if an employee has changed, this list can be referred to and required modifications can be very easily made.

5.4.2 Modify employee information

Modification feature we have been talking about. Once the option is selected the interface asks for the code of the employee to be modified or gives a help option which can take us to our reference list. Then the new name can be entered and saved.



```
          Employee Name : TAMISH AREN
          New Name :    XYZ

   Do you want to modify this record (y/n) : y


   Do you want to save changes (y/n) : y

   Record Modified
   Enter the name of the employee or <ENTER> for no change
```

Figure 5.5: Results of option 2 of program

When we enter the option the program first asks for the new name to be entered. It also confirms the changes to avoid any mistakes once the user agrees for the changes; it overwrites in its database the new name of the employee on the old one. The other two options can only be viewed when the interface is used while a successful connection has been made between the reader and the computer in connection.

5.4.3 Attendance monitoring and verification of RF tag

The working of the project can be explained with the help of a flow chart

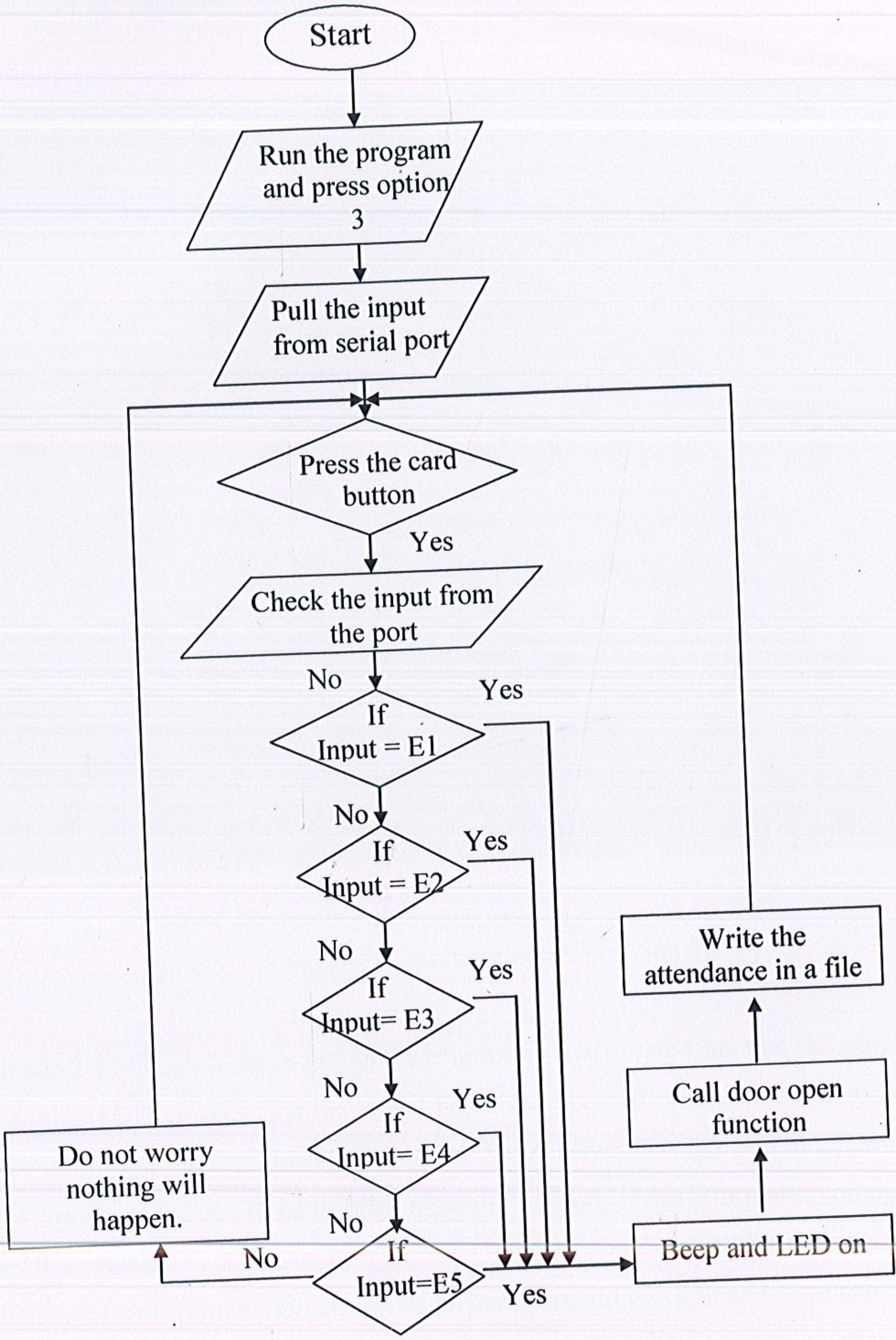

Start
Run the program and press option 3
Pull the input from serial port
Press the card button
Yes
Check the input from the port
No
Yes
If Input = E1
No
Yes
If Input = E2
No
Yes
If Input= E3
No
Yes
If Input= E4
No
If Input=E5
No
Yes
Do not worry nothing will happen.
Beep and LED on
Call door open function
Write the attendance in a file

Figure 5.6: System flow chart

Bring the card in the range of the receiver and switch on the button. The transmitter then sends a signal to the receiver and the receiver further transmits it to the computer with the help of the parallel port interface.

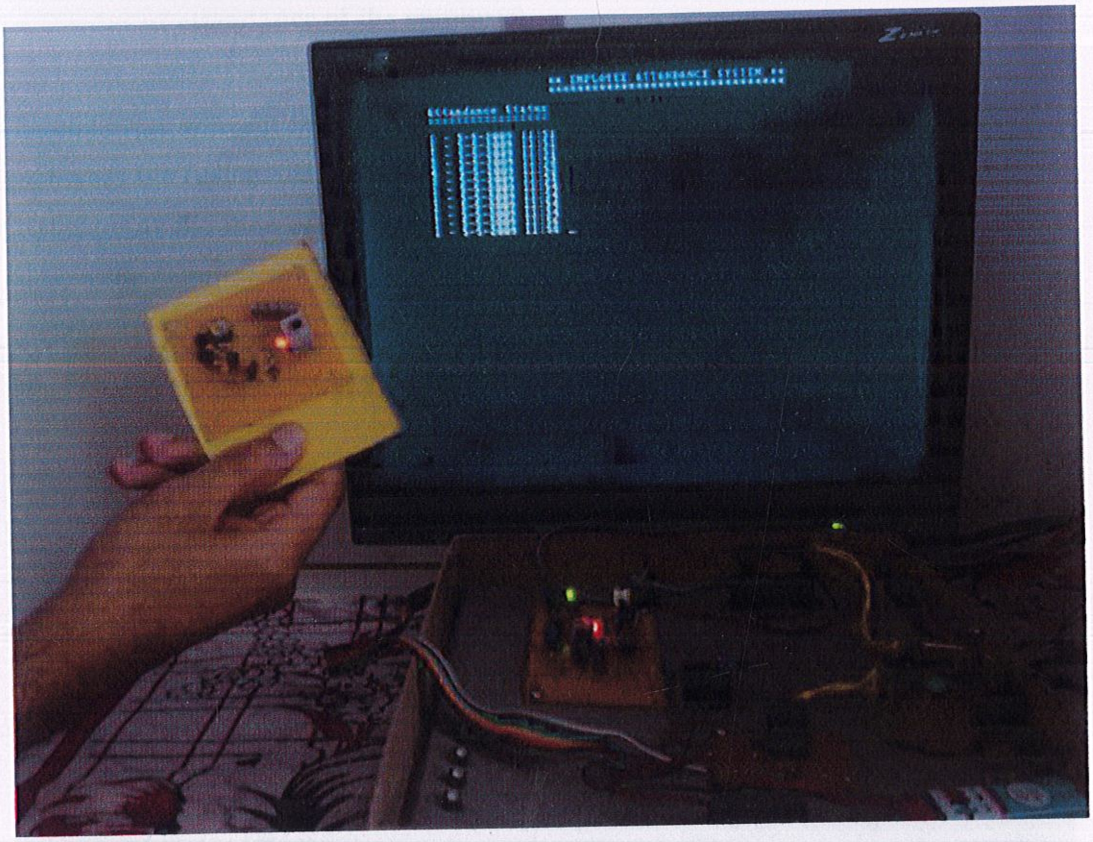
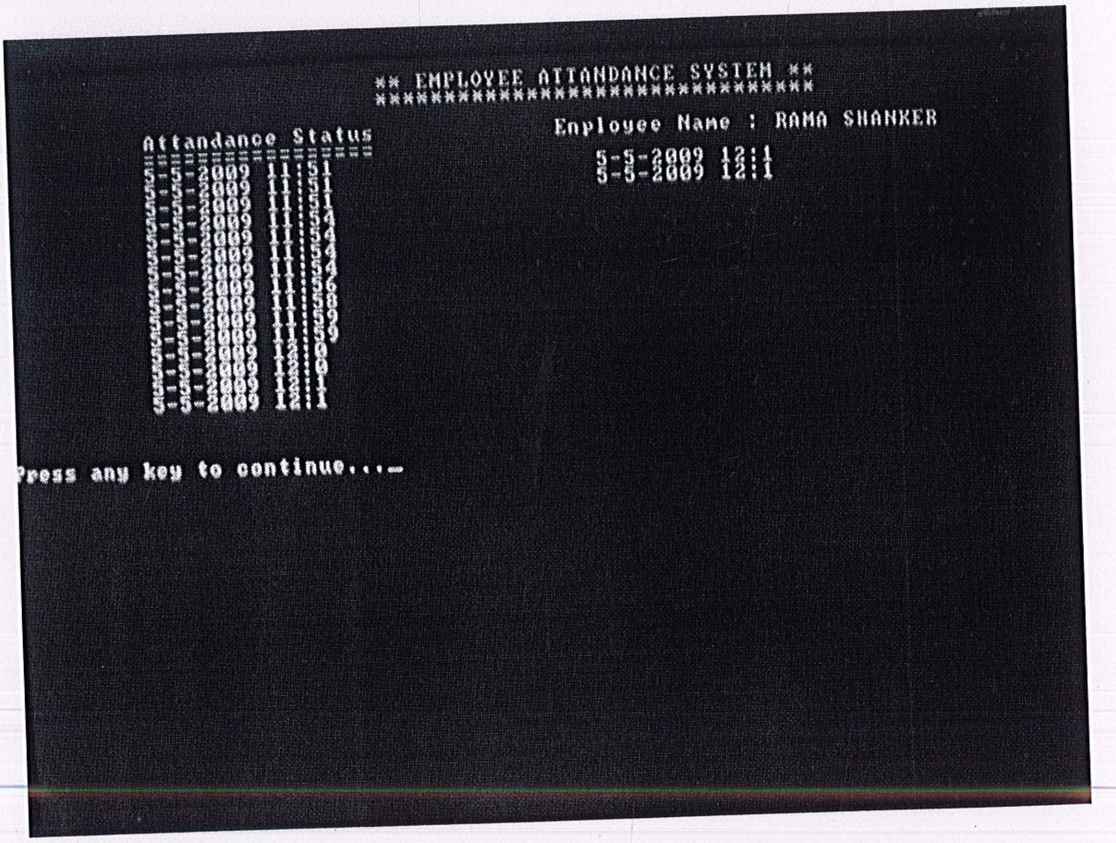


Figure 5.7: Snapshot of working project (option 3)

We can see 2 LEDs glowing in the receiver unit one (red) represents that the power is on. The other LED verifies that the signal has been received. The receiver detects the tag and the information contained by it is read. The receiver is connected to a relay unit which is further connected to pc through a parallel in-port. If the information on the tag matches the database in the pc it is programmed to open the door and the buzzer blows. The attendance status on the screen shows the employee id on right and Date and Time of entrance on the left. Besides the attendance the computer also sends a signal through the other relay to the buzzer and to the motor to which the gate is connected. The time for which the motor is revolving can be changed by the program.

5.4.4 Display of attendance of the employee

The computer with on line real time application will enter and store the data in the employees file (using. dat). Thus we have five data files handled by PC each for each employee. At the time of exit, he again does the same process to open the gate/door again. Thus one time the computer will take as entry time and other for the exit time. Anytime we can see from computer the time schedules of the specific employees out of five. For other four employees we can show with the key controls.



```
                             ** EMPLOYEE ATTANDANCE SYSTEM **
                             ********************************
                                      Enployee Name : RAMA SHANKER
       Attandance Status
       ===================                5-5-2009 12:1
       5-5-2009 11:51                     5-5-2009 12:1
       5-5-2009 11:51
       5-5-2009 11:51
       5-5-2009 11:54
       5-5-2009 11:54
       5-5-2009 11:54
       5-5-2009 11:54
       5-5-2009 11:56
       5-5-2009 11:58
       5-5-2009 11:59
       5-5-2009 11:59
       5-5-2009 12:0
       5-5-2009 12:0
       5-5-2009 12:1
       5-5-2009 12:1
       5-5-2009 12:1

Press any key to continue..._
```

Figure 5.8: Results of option 4 of program

Figure 5.8 shows the attendance of the employee" Rama Shankar" with date and time. The date and time are taken up from the computer clock. This is saved in a file and can be used for further reference. This data can also be used to calculate the working hours of that employee and can further be useful in calculating the salary if necessary. In case we are monitoring the attendance of student this can be used to calculate the percentage of classes attended by the student.

CHAPTER 6

Controversies and Future Work

6.1 Problems and concerns

The main difficulty working with RFID tags can be summarized as:

- **Card Theft**

  The main concern of the thesis is to built a secure attendance monitoring system but if the card is not in the hands of its owner it can be used for illegal purposes.

- **Global standardization**

  The frequencies used for RFID in the USA are currently incompatible with those of Europe or Japan. Furthermore, no emerging standard has yet become as universal as the barcode.

- **Security concerns**

  A primary RFID security concern is the illicit tracking of RFID tags. Tags which are world-readable pose a risk to both personal location privacy and corporate/military security. Such concerns have been raised with respect to the United States Department of Defense's recent adoption of RFID tags for supply chain management. More generally, privacy organizations have expressed concerns in the context of ongoing efforts to embed electronic product code (EPC) RFID tags in consumer products.

  The cost/power limitation has led some manufacturers to implement cryptographic tags using substantially weakened or proprietary encryption schemes, which do not necessarily resist sophisticated attack. For example, the Exxon-Mobil Speedpass uses a cryptographically-enabled tag manufactured by Texas Instruments, called the Digital Signature Transponder (DST), which incorporates a weak, proprietary encryption scheme to perform a challenge-response protocol for lower cost. Still other cryptographic protocols attempt to achieve privacy against unauthorized readers, though these protocols are largely in the research stage.

One major challenge in securing RFID tags is a shortage of computational resources within the tag. Standard cryptographic techniques require more resources than are available in most low cost RFID devices.

- **Exploits**

  Ars Technica reported in March 2006 an RFID buffer overflow bug that could infect airport terminal RFID Databases for baggage, and also Passport databases to obtain confidential information on the passport holder.

- **Passports**

  In an effort to make passports more secure, several countries have implemented RFID in passports. However, the encryption on UK chips was broken in less than 48 hours. Since that incident, further efforts have allowed researchers to clone passport data while the passport is being mailed to its owner. Where a criminal used to need to secretly open and then reseal the envelope, now it can be done without detection, adding some degree of insecurity to the passport system.

- **Shielding**

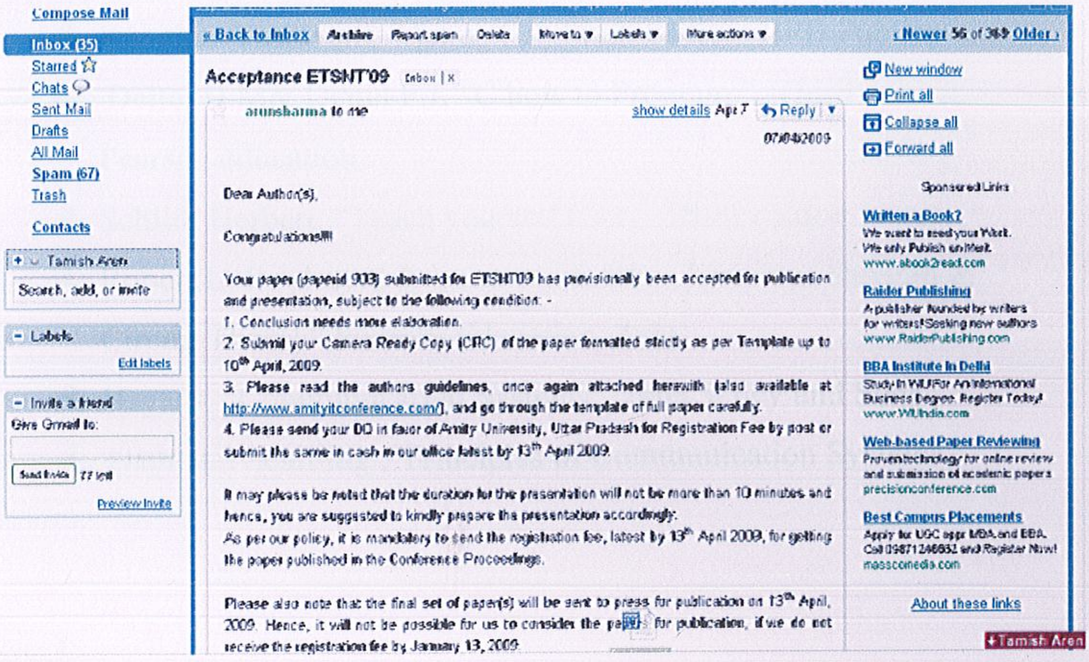
  A number of products are available on the market that will allow a concerned carrier of RFID-enabled cards or passports to shield their data. In fact the United States government requires their new employee ID cards to be delivered with an approved shielding sleeve or holder. There are contradicting opinions as to whether aluminum can prevent reading of RFID chips. Some people claim that aluminum shielding, essentially creating a Faraday cage, does work. Others claim that simply wrapping an RFID card in aluminum foil, only makes transmission more difficult, yet is not completely effective at preventing it.

6.2 Future work

To decrease the chances of misuse of the identification card we can embed the card with the facial imprints of the card holder. When the card is activated, a CTC can be used to obtain the facial imprints of the hard holder which can be matched with the computer database to confirm the identity.

Achievements

It gives us immense pleasure in writing that we got our Research paper selected **(paper ID 903)**, namely **"ATTENDANCE MONITORING USING RADIO FREQUENCY IDENTIFICATION"**, in ***National Conference on Emerging Trends in Software and Networking Technologies (ETSNT'09)*** being held at Amity Institute of Information Technology, Uttar Pradesh on April 17-18 2009.



Acceptance ETSNT'09

arunsharma to me Apr 7

07/04/2009

Dear Author(s),

Congratulations!!!

Your paper (paperid 903) submitted for ETSNT09 has provisionally been accepted for publication and presentation, subject to the following condition: -

1. Conclusion needs more elaboration.
2. Submit your Camera Ready Copy (CRC) of the paper formatted strictly as per Template up to 10th April, 2009.
3. Please read the authors guidelines, once again attached herewith (also available at http://www.amityitconference.com/), and go through the template of full paper carefully.
4. Please send your DD in favor of Amity University, Uttar Pradesh for Registration Fee by post or submit the same in cash in our office latest by 13th April 2009.

It may please be noted that the duration for the presentation will not be more than 10 minutes and hence, you are suggested to kindly prepare the presentation accordingly.
As per our policy, it is mandatory to send the registration fee, latest by 13th April 2009, for getting the paper published in the Conference Proceedings.

Please also note that the final set of paper(s) will be sent to press for publication on 13th April, 2009. Hence, it will not be possible for us to consider the papers for publication, if we do not receive the registration fee by January 13, 2009.

Snapshot of the confirmation received via email.

BIBLIOGRAPHY

- Joseph J. Carr ,"Secrets of RF circuit design"
- Davis W Alan and Aggarwal Krishna,“ Radio frequency circuit design.”, Singapore :John Wiley & sons,2001.
- Kanitkar Yashwant, “ let us C.”, Sixth edition, BPB Publications
- Deitel H.M&.Deitel P.J, “C how to Program.”, Third edition, Pearson education
- Schildt Herbert, “Teach yourself C++.” Third edition
- Robert L. Boylestad & Louis Nashelsky ,"Electron Devices & Circuit Theory",Pearson Education, Asia.
- Haykin, “Communication Systems”, John Wiley and Sons.
- Taub and Schilling ,“Principles of Communication Systems”.