MICROCONTROLLER BASED GPRS ENABLED RFID SYSTEM

By

Kashif Sharif 2003-NUST-BICSE-74

Project Report in partial fulfillment of the requirements for the award of Bacholor of Information and Communication System Engineering degree

School of Electrical Engineering and Computer Sciences
National University of Sciences and Technology
Rawalpindi, Pakistan
2008

MICROCONTROLER BASED GPRS ENABLED RFID SYSTEM

By

Kashif Sharif (2003-NUST-BICSE-74)

Project documentation submitted in partial fulfillment of the requirements for the degree of

Bachelors in Information & Communication Systems Engineering (BICSE)

NUST School of Electrical Engineering and Computer Science

National University of Sciences and Technology

Rawalpindi, Pakistan

(2008)

CERTIFICATE

It is certified that the contents and form of thesis entitled **"Microcontroller Based GPRS Enabled RFID System"** submitted by **Kashif Sharif (2003-NUST-BICSE-74)** have been found satisfactory for the requirement of the degree.

Advisor: ______________________________

(Dr. Nazar Abbas Saqib)

Co-Advisor: ______________________________

(Dr. Fauzan Mirza)

DEDICATION

To Allah the Almighty

&

To my Parents and Faculty

ACKNOWLEDGEMENTS

I am deeply thankful to my advisor and Co-Advisor, Dr. Nazar Abbas Saqib, and Dr. Fauzan Mirza for helping me throughout the course in accomplishing my final year project. Their guidance, support and motivation enabled me in achieving the objectives of the project.

I am also thankful to Mr. Mujtaba Haider and Mr. Ali Haider for their help, at the crucial stages of the project. Finally, I am extremely thankful to Mr. Jaudat Shaikh (Product Manager, LMKR), for guiding me through emails and sparing his valuable time for me.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Radio Frequency Identification Technology is used to identify the things uniquely and is widely used in a lot of applications all over the world. The RFID Readers, which are used to read RFID tags, have wired communication with computers/network devices but In many applications it is required to have wireless communication between RFID Reader and backend computer system. In local industry there is no solution to this requirement so aim of this project is to develop such an RFID system in which communication between RFID Reader and back end computer system will be wireless.

Chapter 1

INTRODUCTION

For years, visual scanning systems, such as bar code systems, have helped manufacturers and retailers keep track of inventory. Radio frequency identification (RFID) systems evolved as a way to provide all the benefits of visual scanning systems, while overcoming many of their limitations. Radio frequency (RF) describes electromagnetic waves in the 10 kHz to 10 GHz range. Electronic identification (ID) systems transfer data messages from an object to be identified to a data management system. RFID systems use radio frequency to transfer data between an item being tracked and a reader/writer. It is a fast, automatic identification technology.

Radio Frequency Identification System is especially suited for applications which require high data rate transmission, no line of sight requirement in scanning, larger data storage capacity on RFID Tags and long read range.

Radio Frequency Identification System normally contains four components

i. RFID Tag

ii. RFID Reader

iii. Middleware

iv. Back end Host System

The communication between RFID Reader and RFID Tag is wireless while the communication between RFID Reader and Backend System is wired.

1.1 Importance

The rapid growth of using RFID System in a lot of applications in the recent years demands a wireless mode of communication between RFID Reader and Back end system which is required in many applications.

1.2 Project Goal

The goal of the project was to develop:

- **A product which**
  - Receives data from RFID Reader
  - Operates a Mobile Device
  - Sends data to backend System through Mobile Device
- **A software utility which**
  - Receives data from Mobile Device
  - Stores the Data in to Database

1.3 Report Organization

The report is organized into five chapters.

***Chapter** 2 explains the RFID System Components, their working and functionality.*

***Chapter** 3 gives insight into evolution of Standards of RFID System. It also gives a detailed overview of the basic concepts and the building blocks involved in RFID System.*

Chapter 4 *gives insight into Microcontroller, RFID reader communication protocols.*

Chapter 5 *discusses the Implementation of the wireless RFID System. It involves the sequence diagrams and methodology.*

Chapter 2

RFID SYSTEM COMPONENTS

This chapter explains the functionality, working and types of the main components of the RFID System. The main topics covered in this chapter are:

- RFID Tags
- RFID Reader
- Antennas

2.1 RFID Tags

RFID tags (also called transponders) are attached to objects that you want to track. The tag transfers data to the reader using radio waves that are tuned to the same frequency as the reader and within the reading range of the reader. The tag circuitry consists of a microchip attached to an antenna. This circuitry is adhered to an insert, which is then packaged for the appropriate application. Tags come in many different form factors for different applications and for different environments. A tag can be mounted inside a carton or it can be embedded in plastic for mounting in a damp environment. A tag may be as small as a grain of rice or as large as a brick. It may be adhered under a label. Some examples of the types of tags are: container tags, windshield sticker tags, tire tag inserts, metal mount tags, and inserts [1].

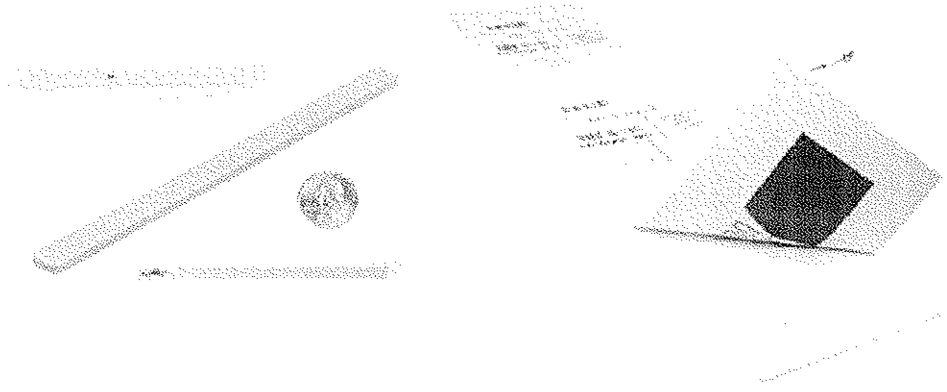


Fig 2.1 Examples of stick tags and some labels that have tags adhered under them.

Tag data is typically contained in an electrically-erasable, programmable, read-only memory circuit, or EEPROM. Tags can be programmed by the manufacturer or customer to match information on the object to be tagged, such as part number, serial number, destination, purchase order, SSCC, and so forth. Besides form factors, tags vary by their performance. They can be read-only, write-once/read many (WORM), or read/write. Tags also vary by their technologies. They can use active, active backscatter, or modulated backscatter to power their circuitry and communicate with the reader.

2.1.1 Read-Only Tags

Read-only tags are generally the least expensive. A read-only tag is pre-numbered and requires a host database. Once a read-only tag is programmed by the manufacturer, you cannot alter its data. [1]

2.1.2 Write-Once/Read-Many Tags

WORM tags are a form of read-only tags. A WORM tag is pre-numbered and requires a host database. Once a WORM tag is programmed by the manufacturer or by the customer, you cannot alter its data.

2.1.3 Read/Write Tags

Read/write tags are much more flexible than read-only tags or WORM tags. A read/write tag generally requires larger chips than the other tags; however it can hold much more information. Each IS0 18000-6B tag contains a unique serial number, but it also may have other information, such as a customer's account number. You can update or change the information as often as needed. Because the read/write tag becomes a portable database that travels with the product, you can modify its data throughout its journey along the supply chain. Depending on the individual chip capabilities, you can also permanently lock the data on a byte-by-byte basis.

2.1.4 Tag Technologies

There are three different types of RFID tag technologies that you can use: active, active backscatter (semi-passive), modulated backscatter (passive).

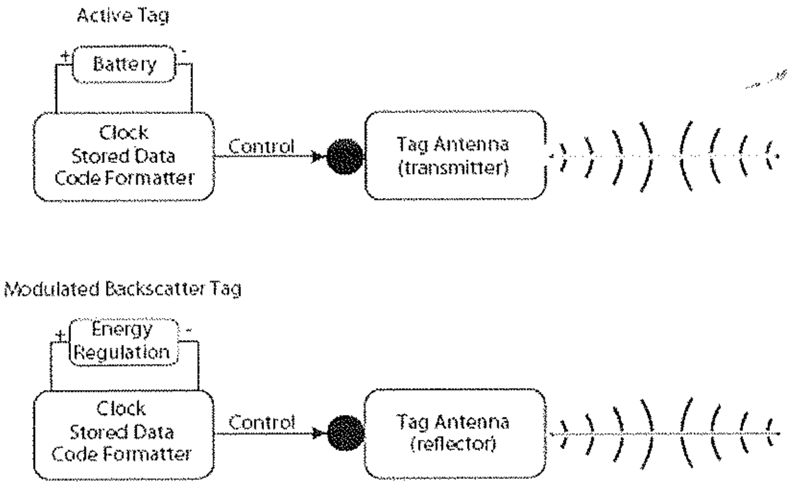


Fig 2.2 RFID Tag Block Diagrams

Active and active backscatter tags are most useful for tracking high-value goods that need to be scanned over long ranges. However, they are too expensive to put on low-cost items. Since modulated backscatter tags are the least expensive, they are best for tracking ordinary goods that are scanned over shorter ranges [2].

2.1.5 Active Tags

Active tags are the most expensive because each tag has a small lithium battery that powers its radio, circuitry, and memory. Since the active tag has an on-board power source, it has the longest reading range, which is about 91.4 m (300 ft). This tag is the best selection when your most important consideration is to be able to read tags at the greatest distance. Active tags have a limited operating life because the battery eventually loses power and replacing the battery is probably more expensive than replacing the tag. Also, active tags can only be used in certain environments because they add to the radio noise background.

2.1.6 Active Backscatter Tags

Active backscatter tags, also called battery-assisted tags, are less expensive than active tags. The tag has a medium reading range, which is between 3 and 15.2 m (10 to 50 ft). The battery in the tag powers the tag's internal circuitry, but it does not power its radio. The reader (through its antennas) transmits RF energy. When a tag enters the reader's reading range, it reflects the reader-generated RF energy to transfer data.

Like the active tags, active backscatter tags have a limited operating life because they eventually lose power and it is probably not worth the cost to replace the battery. The more the tag is read, the sooner the battery runs out [2].

2.1.7 Modulated Backscatter Tags

Modulated backscatter tags, also called passive tags, are the least expensive, the lightest, and have a virtually unlimited life time. The tag has a shorter reading range than active backscatter—between a few cm (in) to 5.5 m (18 ft). Like active backscatter technology, the reader (through its antennas) transmits RF energy. When a tag enters the reader's reading range, it reflects the reader-generated RF energy, which powers the tag. Since the tag cannot transmit its own signal (since it has no internally-supplied power), it simply reflects part of this RF energy back through its antenna to the reader's receiver. These tags do not contribute to radio noise background. Modulated backscatter tags require a reader to have much more power than a reader for active tags. They can be inductively-coupled or capacitive coupled.

2.1.8 Inductively-Coupled Tags

Inductively-coupled tags (also called radio-wave-coupled tags) are powered by magnetic energy from the reader. That is, a coil in the reader antenna and a coil in the tag antenna form an electromagnetic field. The tag draws power from the magnetic energy in the field and uses it to run its circuitry. Because the tag must be close to the reader, the reading range of inductive tags is very small.

2.1.9 Capacitively-Coupled Tags

Capacitively-coupled tags (also called propagation-coupled tags) are powered by the electromagnetic energy generated by the reader. The tag gathers the energy from the reader antenna and reflects back an altered signal. Capacitively-coupled tags are less expensive and more flexible than inductively-coupled tags. They also have a longer reading range [2].

2.1.10 How Tags Affect the Reading Range

The RFID tags used in any installation significantly affect the dimensions and performance of the reading range. Among the primary tag characteristics that influence the reading range are:

- Tag power source (battery or beam).
- Tag orientation.
- Tag speed through the reading range.
- Tag mounting surface.
- Tag sensitivity.
- Tag reflectivity.

2.1.11 Tag Power Source

Tags may be either active (powered by battery) or modulated backscatter (powered by the beam or radio signal). The active tag's performance (signal strength) declines gradually with distance, returning a progressively weaker signal. The modulated backscatter tag's reading range is limited by the need to receive adequate RF energy to energize its circuits. Their performance decline gradually until the received radio signal is insufficient to energize its circuits; beyond that point, no signal is returned. [2]

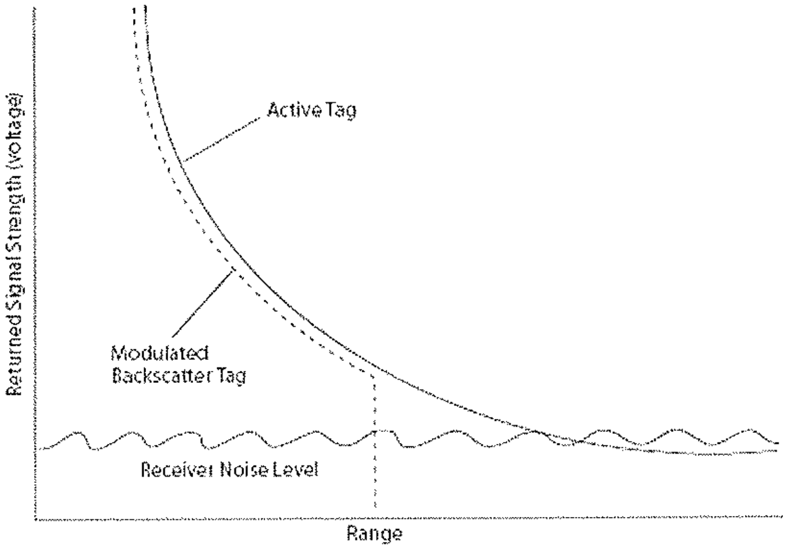


Fig 2.3 The relative decline in performance of the active tag and the modulated backscatter tag.

2.1.12 Tag Orientation and Placement

Tags are polarized just as are antennas. For optimal RFID system performance and reading range, tag polarization must be parallel with the applicable antenna's polarization. Ideal alignment of the antenna and tag is with the tag directly in front of the antenna and the tag's longer side oriented parallel with the antenna polarization. Realistically, however, it is virtually impossible to guarantee ideal alignment of all tags to be read in a normal operation. In all applications, the alignment of the tag antenna with the system antenna is important.

The orientation of the tag in direct phase with the antenna pattern returns optimal results. However as a general rule, you may misorient the tag by 15° in any direction with negligible degradation in performance. Proper system configuration can permit even greater tolerance. This tolerance to misorientation allows the system to read tags whose orientation and angle of presentation change as a function of their trajectory through the reading range.

Also, the tag reading range may be affected by pitch, roll, and yaw. These next definitions assume that antenna polarization is parallel with the tag's longer side.

2.1.13 Tag Speed

The speed at which a moving tag can be read is limited by the need to receive a little more than one complete code frame while the tag is within reading range. For example, in certain circumstances, a reading range 1.5 m (5 ft) wide may support a maximum tag speed of 152.4 m/min (500 ft/ min). The data transfer rate is different from one air interface protocol to another. For example, the EPC global Gen 2 air interface protocol lets data rates vary by tag, reader, and application. However, in general, in order for the tag to move faster, you need to have a "cleaner" environment, which means stronger signals and fewer sources of noise.

2.2 RFID Readers

In the most general terms, RFID readers identify and communicate with RFID tags. The reader, which has one or more system antennas, generates and sends out RF energy, processes data returned by the tags in its reading range, and relays the tag data to a host system. If your RFID system uses modulated backscatter (passive) tags, the reader must generate enough RF energy to energize the tags' circuitry so that the tag can reflect its data back to the reader. The reader may also write to tags. Readers come in many different forms and can be used for many different applications in many different environments. There are fixed readers, portable readers, and vehicle-mount (forklift) readers. You can mount a fixed reader so that it can read tags traveling through dock doors, conveyor belts, loading bays, gates, doorways, and many other areas. You can use portable readers to add RFID capabilities to your existing application without investing in a new mobile computing system. Portable readers can also be used to read and write to tags that are in remote locations [1].

Fig 2.4 An RFID Reader

2.2.1 How Readers Affect RFID System Performance

The reader has both active and passive influence on RFID system performance. Although inevitable, the effect of electrical noise and interference can be mitigated to an extent, through proper installation. The outer boundary of the reading range is marked by the distance from the system antenna at which a tag can no longer be reliably read. This happens when the distance between the reader and a modulated backscatter tag becomes so great that the power of the radio signal is below the tag's sensitivity level. At the outer boundary, tag data will not be read with any degree of certainty.

2.2.2 Reader Sensitivity

The reader's sensitivity is determined primarily by the electrical noise level of its internal circuitry. This noise competes (interferes) with the tag signal, and when sufficiently strong, the noise can overwhelm the tag signal in much the same way static can overwhelm a radio broadcast. Interference can be defined as any undesired electrical energy within the RFID system.

2.2.3 Electrical Noise and Interference

The reader is also vulnerable to electrical noise from external sources, such as these two broad types:

i. Sources that produce electrical noise when located in the RF field.

ii. Other sources of electrical noise.

2.2.4 Sources of Electrical Noise

Sources that produce electrical noise respond in the RF field in the same way a tag responds. When these tag-like signals return through the antenna, they may be strong enough to mask a real tag signal and prevent the reader from decoding the tag ID.

Examples of these sources commonly found in the environment are:

- Other readers.
- Fluorescent lights (AC)
- Mercury and sodium vapor lamps (AC-powered street lights).
- Camp lanterns (models which convert VDC to high-frequency AC).
- Neon lights.

2.2.5 Other Sources of Electrical Noise

Other sources of electrical noise may also be present in the environment. However, if you configure your RFID system properly, these sources will have little or no effect on system performance.

Examples of other sources of electrical noise are:

- High-speed fans with metal blades.
- High-speed trains.

- Digital noise.
- Cellular telephones (when switching on and off).
- Microphonics caused by system vibrations or motions.

Some of these sources of electrical noise are not always easy to locate, since they often generate noise intermittently. The system designer or installer must be aware of such possible sources of noise and be prepared to compensate for them [2].

2.2.6 Solving Electrical Noise and Interference Problems

The best way to compensate for sources of electrical noise is to remove the source from the RF field. Or, you can remove the source a sufficient distance from the antenna so that its signal level is far below that of the weakest expected tag signal. When it is not practical to move either the source of the noise or the RFID system components, the source must be shielded with wire screen or other suitable material.

The type and length of cables used to connect system components can affect noise levels in the system and power output through the antenna. Long cable runs generally require heavier cable and a higher level of EMI (electromagnetic interference) shielding [2].

2.2.7 Frequencies and Bandwidth

All RFID systems must operate within national and international laws and regulatory guidelines with respect to frequency and bandwidth use. Depending on the country, several frequency bands may be available. Choose a frequency for your RFID equipment, including the readers, that matches your application and performance requirements.

2.3 RFID Antennas

Every RFID tag has an antenna and every RFID reader has either an integrated antenna or an external system antenna. An RFID antenna has two functions:

i. Transmit the radio signal.

ii. Receive the coded signal transmitted or reflected by the tag.

Antennas come in many different forms and can be used for many different applications in many different environments. Here is an example of what an antenna may look like.

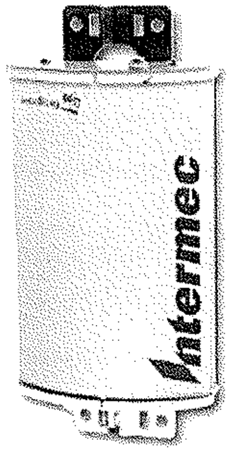


Fig 2.5 RFID Reader Antenna

The radio signal that is transmitted from the reader through the antennas to modulated backscatter (passive) tags must be strong enough to energize (turn on) the tag's electronic circuitry. The radio signal must also be able to reflect off the tag and return an adequate number of complete tag messages to the antenna. [1]

2.3.1 Affect of Antennas the Reading Range

Each antenna broadcasts RF energy in a characteristic radiation pattern. This pattern is the most influential factor determining the shape of the reading range. It radiates primarily in front of the antenna and is relatively symmetrical. When it is strong enough to communicate with a tag, the RF energy contained within the pattern is considered the "active" region. Beyond the active region, the antenna radio signal is too weak to reliably maintain a communications link between the tag and reader.

2.3.2 Antenna Radiation Patterns

The antenna radiation pattern shows the antenna gain (a measure of antenna directivity), which determines the relative strength of the RF field within the antenna's pattern. In general, gain is expressed in dB (decibels) as the ratio of the maximum (forward) power density to the power density of an isotropic radiator emitting the same total amount of power. Its units are designated dBi, where the third letter ("i") means "over an isotropic."

An isotropic radiator is an imaginary source that emits radiation uniformly in all directions. Its radiation pattern is perfectly spherical in space. Note that the gain of an isotropic radiator that is radiating in a uniform spherical pattern is one (0 dB). By directing the radiator's energy, an antenna's power density may be concentrated along a preferred direction. This concentration of energy results in a power density gain in the designated direction.

A typical medium gain antenna has a gain of 10 dBi or more. This antenna pattern can be fan- or cone-shaped, with beam widths of 20 to 40 degrees. The field in front of an antenna varies gradually, so that the edges of the reading range are "soft."

2.3.3 How to Choose the Right Antennas

When you are choosing antennas for your application, you need to consider these factors:

- Application type
- Frequencies and bandwidth
- Reading range performance
- Environment
- Cost

All RFID systems must operate within national and international laws and regulatory guidelines with respect to frequency and bandwidth use. Depending on the country, several frequency bands may be available. Choose a frequency for your RFID equipment, including the antennas, that matches your application and performance requirements. Most antenna radiation graphs only show the antenna's far-field performance. However, if you want your RFID system to have good coverage, you must address far-field performance and near-field performance.

2.4 RFID Standards

RFID technology standards are being worked on by two major organizations: ISO (International Organization for Standardization) and EPCglobal. There are three different types of standards:

i. Air interface protocols, which describe the way readers and tags, communicate with each other.

ii. Data content, which describe how the data is organized.

iii. Applications, which explain how applications are used in an RFID system.

ISO has created many standards for RFID technology that deal with both the air interface protocol and the applications for RFID. The air interface protocol standard that describes how readers communicate with ultra-high frequency (UHF) RFID tags is called ISO 18000-6. There are two versions of 18000-6: 18000-6A and 18000-6B. EPCglobal created the electronic product code (EPC) and they are responsible for its technology. EPCglobal is creating standards that govern how EPC data is shared among companies and other organizations. Thus, they have written air interface protocol standards that describe how readers communicate with EPC tags. The first standards were classified as EPCglobal Gen 1 and they addressed class 0 and class 1 tags. Now, EPCglobal has developed a second generation air interface protocol called EPCglobal Gen 2, which is designed to communicate with tags that are a higher class and that will work internationally [1].

2.5 RF Spectrum

The RF spectrum is regulated by government regulatory agencies, such as the FCC, who establish guidelines for its use. Depending on the region and country where you are installing your RFID system, you must follow those agencies' guidelines. Typically, the guidelines specify how you can use these features:

- Frequency and bandwidth size
- Channel use (primary or secondary)
- Power level (in milli watts or watts)
- Duty cycle (percent of time allowed to output power)

2.5.1 Frequencies and Bandwidth

All RFID systems must operate within national and international laws and regulatory guidelines with respect to frequency and bandwidth use. Depending on the country, several frequency bands may be available. However, operating outside the more common bands has disadvantages. RFID systems can be classified according to the frequency band in which they operate:

- Low frequency (10 to 500 kHz), near-field system using modulated backscatter, inductively-coupled tags.
- High frequency (10 to 15 MHz), near-field system using modulated backscatter, inductively-coupled tags.
- Ultra-high frequency (860-960 MHz), far-field system using modulated backscatter, capacitively-coupled tags or active tags.
- Microwave frequency (2.4-5.0 GHz), far-field system using modulated backscatter, capacitively-coupled tags or active tags.

Each frequency band has advantages and disadvantages that you need to understand when designing your RFID system. Depending on which frequency band your RFID system uses, certain characteristics of the RFID system can be affected, such as reading range,[2].

For low and high frequency systems:

- Higher frequency = shorter radio wavelength = longer reading range

For ultra-high frequency and microwave systems:

- Higher frequency = shorter radio wavelength = shorter reading range

Low Frequency Systems

Low frequency systems usually operate in the 125 to 135 kHz range. They use modulated backscatter, inductively-coupled tags. In this frequency range, you get small amounts of data at slow speeds, short reading ranges, and large tags due to large looping antennas. Typically, the reading range is half the longest dimension of the antenna loop. However, the tags are inexpensive. This frequency range is relatively free from regulatory limitations. Although it does not penetrate metals very well, it does penetrate other materials, such as tissue (people, animals, etc.), wood, and water. It is often used for animal identification and access control.

2.5.2 High Frequency Systems

High frequency systems usually operate at 13.56 MHz. They also use modulated backscatter, inductively-coupled tags. Since these tags have a simpler antenna design, they are even more inexpensive than the tags used in low frequency systems. Like the low frequency systems, this system is good at reading small amounts of data at slow speeds. However, it transmits data at slightly higher speeds than low frequency systems and has a slightly larger reading range (0.7 m or 2.3 ft). This frequency band is a government-regulated frequency. Like the low frequency systems, it does not penetrate metals very well, but it does penetrate tissue and water. It is typically used for access control, inventory control, and smart cards [1].

2.5.3 UHF Systems

Ultra-high frequency (UHF) systems usually operate in the 865 to 928 MHz range. They use modulated backscatter, capacitive-coupled tags or active tags and have antennas that allow them to have reading ranges much larger than the antenna dimensions. Because these tags have smaller antennas than high frequency systems, they are smaller than the tags used in high frequency systems. UHF systems have a reading range that is from a few to many wavelengths long. They are good at reading large amounts of data at high speeds. The 865 to 928 MHz range is the best range for distances between 1 m (3.3 ft) and 10 m (33 ft). UHF frequency ranges are government-regulated. They are not very effective frequencies in environments that have a lot of tissue or water. However, they are effective around metals. This system is best for supply chain management applications [1].

2.5.4 Microwave Systems

Microwave systems usually operate at the 2.4 GHz range. They use modulated backscatter, capacitive-coupled tags or active tags. Because these tags have the smallest antennas, they are the smallest tags. Microwave systems have a longer reading range than low or high frequency systems, but a much shorter range than UHF systems. 2.4 GHz has a reading range of about 1 m (3.28 ft). Microwave systems are government regulated and are more susceptible to noise (such as noise generated by wireless LANs and microwave ovens) than UHF systems. However, if you are not concerned about reading range, this frequency has a lot of bandwidth available to it and has more channels to hop between.

2.5.5 About Channel Use

All RFID systems must operate within national and international laws and regulatory guidelines with respect to channel use. Depending on the country, the operating frequency for RFID may be a primary or secondary service. Primary services let you broadcast radio waves however, secondary service or out-of channel emissions must be kept low to provide efficient use of the overall band. Primary services must not jam or decrease performance for any other devices that use frequencies outside the allowed RFID frequency bands. If the operating frequency is a primary service, it can claim interference from a secondary service. However, a secondary service cannot claim interference from a primary service.

2.5.6 Power Levels and Duty Cycle

All RFID systems must operate within national and international laws and regulatory guidelines with respect to power levels and duty cycle. Power levels are defined as the maximum wattage (W) allowed at EIRP (Effective Isotropic Radiated Power). EIRP is the apparent power transmitted towards the antenna, if it is assumed that the signal is radiated equally in all directions. In the U.S.A., RFID equipment can only radiate a maximum power of 4 W. In Europe (according to ETSI 300 220), the maximum power output is 0.5 W or 2 W, depending on the frequency. Duty cycle is defined as the percent of time the RFID equipment is outputting power. For example, in Europe at 869 MHz, each reader can only radiate a maximum of 0.5 W at a 10% duty cycle per hour. That is, the reader can only transmit for six minutes out of every hour. [2]

2.6 Radio Signals

In RFID systems, the readers and active tags generate the radio signal and broadcast them into the environment through antennas.

2.6.1 Types of Radio Signals Used in RFID Systems

Radio signals are sent out as waves. All waves can be described in reference to their amplitude or strength. In RFID systems, there are three main types of radio signals that are used:

- Continuous-wave
- Pulsed
- Swept frequency

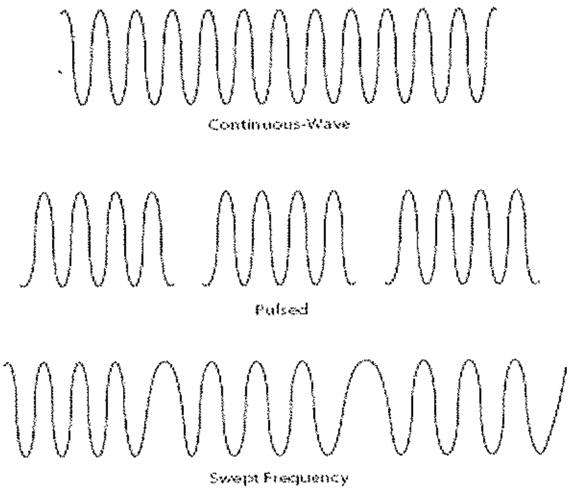


Fig 2.6 The three types of radio signals that are used in RFID systems.

When you design your RFID system, you need to consider what type of radio signals you will use. The reader-to-tag signal can be the same as or it can be different from the tag-to-reader signal [2].

2.6.2 What Affects the Radio Signal?

The most significant factors that influence the radio signal is overall signal strength and noise on the signal.

2.6.3 Overall Signal Strength

The overall signal strength is influenced by three factors: power density, field strength, and antenna gain. Power density is the amount of energy flowing from an antenna through a unit area that is normal to the direction of propagation in a unit time. It is measured in watts per square meter. Field strength is the intensity of a radio signal measured at a certain distance from the transmitting antenna. Field strength is usually expressed in volts per meter. Antenna gain is the ratio of the signal, usually expressed in dB, received or transmitted by an antenna as compared to an isotropic antenna. You can only achieve antenna gain by making an antenna directional, that is, with better performance in one direction than in others. As a radio signal propagates out from the source (antenna), the total RF energy radiated from the source (antenna gain) remains the same, but the overall signal strength decreases as the distance from the source increases. In other words, as the radio signal (tag) moves away from the source (antenna), the antenna gain remains the same, but its field strength and power density decreases. Doubling the antenna gain will double the field strength. The field strength decreases as the inverse of the distance from the antenna. For example, the field strength at 3 m (10 ft) from the antenna is twice the strength at 6 m (20 ft) from the antenna. The power density of the radio signal follows the inverse square law, which means it decreases as the inverse square of the distance from the antenna. For example, if the power density at 3 m (10 ft) from the antenna is 1 watt per square meter, the power density at 6 m (20 ft) from the antenna is 0.25 watts per square meter [1].

2.6.4 Electrical Noise on the Signal

The electrical noise on the radio signal is influenced by:

- Noise within the reader.
- Noise within the tags.
- Other RF transmitters.
- Other sources that produce low frequency noise (keys jingling).
- Fluorescent lighting.
- Interaction with nearby objects.

2.7 Radio Waves

Since radio signals (RF energy) are sent out as waves, an RFID system is influenced by many fundamental properties of radio waves. In many ways, radio waves behave like light waves or water waves. Radio waves can:

- Travel in straight lines.
- Undergo reflections.
- Be refracted (the bending of a wave as it passes in or out of a medium, like light passing through water).
- Bend around certain objects (diffraction).

When radio waves are normal, such as those broadcast from an RFID system antenna, they travel in a straight line. When a radio wave is added to or subtracted from reflected or refracted radio waves from the same source, it causes an effect called "multipath." Multipath is the existence of multiple routes for a single beam of RF energy. How the multipath is formed is determined by the location of the peaks and valleys of the radio waves when they converge [2].

2.7.1 RF Reflection

Radio waves are reflected from metallic surfaces as well as dielectric (non conducting) surfaces. RF reflectors can allow tags outside the antenna's line of sight to be read and can cause multipath effects. Metallic surfaces are the most common and most effective RF reflectors. However to a lesser extent, radio waves are also reflected by dielectric materials, such as dirt, wood, ice, asphalt, and cured concrete. When dielectric materials in the system environment become wet, they reflect radio waves more effectively, thus behaving more like metallic surfaces. Note that whether coarse or smooth, the surface texture of an RF reflector has negligible effect on its reflectivity. When designing an RFID system, you must make sure to factor in RF reflectors in the environment. To control RF reflections, use careful antenna placement and aiming and RF power reduction. Where these factors alone cannot adequately control RF reflections, you may need to use other techniques (shielding, absorbing, range sensitivity adjustment, handshake counts, or barriers).

2.7.2 RF Refraction

Any material that the radio signal can pass through refracts the signal to some extent. When a radio signal enters a dielectric at an angle, its direction of travel is altered by a small degree. RF refraction rarely affects RFID system performance, except when tags are mounted on or under surfaces where dielectric materials are placed (or may accumulate) over the tag (between tag and system antenna).

2.7.3 RF Diffraction

RF diffraction may affect RFID system performance. RF diffraction occurs when radio waves are bent around objects in the environment, allowing them into "shadow" areas normally expected to have little or no signal. Metal poles, corners of buildings, and coin collection boxes in toll plazas often create diffraction.

How Multipath Affects the Reading Range

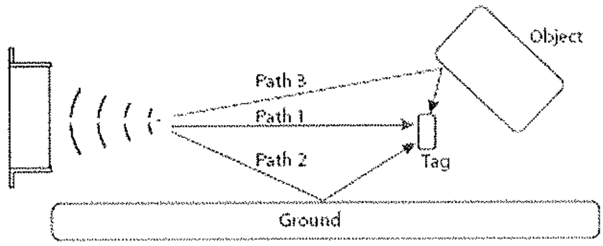


Fig 2.7 When two or more favorable radio paths exist between the tag and the antenna.

Multipath occurs when two or more favorable radio paths exist between the tag and the antenna. Multipath signals can add at their intersection, creating an area of field enhancement beyond the normally expected reading range, or they can subtract, creating unexpected null regions within the antenna's reading range.

2.7.4 Using Multipath to Extend the Reading Range

The constructive interference of multipath signals can be used to create field enhancement, which extends the reading range. Constructive interference describes the combined, positive effect of a main radio signal intersecting in phase with one or more reflected radio signals. Although the reflected radio signals are considered to be interference, the net result is a constructive one. [2]

Chapter 3

MICROCONTROLLER COMMUNICATION PROTOCOLS

3.1 Introduction to Serial Communications

A serial port sends and receives data one bit at a time over one wire. While it takes eight times as long to transfer each byte of data this way, only a few wires are required. In fact, two-way (full duplex) communications is possible with only three separate wires - one to send, one to receive, and a common signal ground wire.

3.1.1 Bi-Directional Communications

The serial port on a PC is a full-duplex device meaning that it can send and receive data at the same time. In order to be able to do this, it uses separate lines for transmitting and receiving data. Some types of serial devices support only one-way communications and therefore use only two wires in the cable - the transmit line and the signal ground [4].

3.1.2 Communicating by Bits y Bits

Once the start bit has been sent the transmitter sends the actual data bits. There may either be 5, 6, 7, or 8 data bits, depending on the number one have selected. Both receiver and the transmitter must agree on the number of data bits, as well as the baud rate. Almost all devices transmit data using either 7 or 8 data bits.

Notice that when only 7 data bits are employed, you cannot send ASCII values greater than 127. Likewise, using 5 bits limits the highest possible value to 31. After the data has been transmitted, a stop bit is sent. A stop bit has a value of 1 - or a mark state - and it can be detected correctly even if the previous data bit also had a value of 1. This is accomplished by the stop bit's duration. Stop bits can be 1, 1.5, or 2 bit periods in length.

3.1.3 The Parity Bit

Besides the synchronization provided by the use of start and stop bits, an additional bit called a parity bit may optionally be transmitted along with the data. A parity bit affords a small amount of error checking, to help detect data corruption that might occur during transmission. One can choose either even parity, odd parity, mark parity, space parity or none at all. When even or odd parity is being used, the number of marks (logical 1 bits) in each data byte are counted, and a single bit is transmitted following the data bits to indicate whether the number of 1 bits just sent is even or odd. For example, when even parity is chosen, the parity bit is transmitted with a value of 0 if the number of preceding marks is an even number. For the binary value of 0110 0011 the parity bit would be 0. If even parity were in effect and the binary number 1101 0110 were sent, then the parity bit would be 1. Odd parity is just the opposite, and the parity bit is 0 when the number of mark bits in the preceding word is an odd number. Parity error checking is very rudimentary. While it will tell you if there is a single bit error in the character, it doesn't show which bit was received in error. Also, if even numbers of bits are in error then the parity bit would not reflect any error at all. Mark parity means that the parity bit is always set to the mark signal condition and likewise space parity always sends the parity bit in the space signal condition. Since these two parity options serve no useful purpose whatsoever, they are almost never used.

3.1.4 RS- 232C

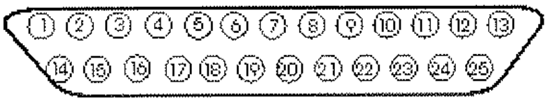
RS-232 stands for Recommend Standard number 232 and C is the latest revision of the standard. The serial ports on most computers use a subset of the RS-232C standard. The full RS-232C standard specifies a 25-pin "D" connector of which 22 pins are used. Most of these pins are not needed for normal PC communications, and indeed, most new PCs are equipped with male D type connectors having only 9 pins [5].

3.1.5 DCE and DTE Devices

Two terms you should be familiar with are DTE and DCE. DTE stands for Data Terminal Equipment, and DCE stands for Data Communications Equipment. These terms are used to indicate the pin-out for the connectors on a device and the direction of the signals on the pins. Your computer is a DTE device, while most other devices are usually DCE devices. If you have trouble keeping the two straight then replace the term "DTE device" with "your PC" and the term "DCE device" with "remote device" in the following discussion. The RS-232 standard states that DTE devices use a 25-pin male connector, and DCE devices use a 25-pin female connector. You can therefore connect a DTE device to a DCE using a straight pin-for-pin connection. However, to connect two like devices, you must instead use a null modem cable. The Null modem cable cross transmit and receive lines in the cable, and are discussed later in this chapter. The listings below show the connections and signal directions for both 25 and 9-pin connectors.

25 Pin Connector on a DTE device (PC connection)

Male
RS232 DB25

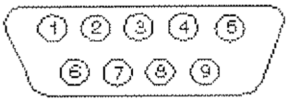


Pin Number	**Direction of signal:**
1	Protective Ground
2	Transmitted Data (TD) Outgoing Data (from a DTE to a DCE)
3	Received Data (RD) Incoming Data (from a DCE to a DTE)
4	Request To Send (RTS) Outgoing flow control signal controlled by DTE
5	Clear To Send (CTS) Incoming flow control signal controlled by DCE

6	Data Set Ready (DSR) Incoming handshaking signal controlled by DCE
7	Signal Ground Common reference voltage
8	Carrier Detect (CD) Incoming signal from a modem
20	Data Terminal Ready (DTR) Outgoing handshaking signal controlled by DTE
22	Ring Indicator (RI) Incoming signal from a modem

9 Pin Connector on a DTE device (PC connection)

Male RS232 DB9



Pin Number	**Direction of signal:**
1	Carrier Detect (CD) (from DCE) Incoming signal from a modem
2	Received Data (RD) Incoming Data from a DCE
3	Transmitted Data (TD) Outgoing Data to a DCE
4	Data Terminal Ready (DTR) Outgoing handshaking signal
5	Signal Ground Common reference voltage
6	Data Set Ready (DSR) Incoming handshaking signal
7	Request To Send (RTS) Outgoing flow control signal
8	Clear To Send (CTS) Incoming flow control signal
9	Ring Indicator (RI) (from DCE) Incoming signal from a modem

The TD (transmit data) wire is the one through which data from a DTE device is transmitted to a DCE device. This name can be deceiving, because this wire is used by a DCE device to receive its data. The TD line is kept in a mark condition by the DTE device when it is idle. The RD (receive data) wire is the one on which data is received by a DTE device, and the DCE device keeps this line in a mark condition when idle. RTS stands for Request To Send.

This line and the CTS line are used when "hardware flow control" is enabled in both the DTE and DCE devices. The DTE device puts this line in a mark condition to tell the remote device that it is ready and able to receive data. If the DTE device is not able to receive data (typically because its receive buffer is almost full), it will put this line in the space condition as a signal to the DCE to stop sending data. When the DTE device is ready to receive more data (i.e. after data has been removed from it's receive buffer), it will place this line back in the mark condition. The complement of the RTS wire is CTS, which stands for Clear to Send. The DCE device puts this line in a mark condition to tell the DTE device that it is ready to receive the data. Likewise, if the DCE device is unable to receive data, it will place this line in the space condition. Together, these two lines make up what is called RTS/CTS or "hardware" flow control.

The Software Wedge supports this type of flow control, as well as Xon/XOff or "software" flow control. Software flow control uses special control characters transmitted from one device to another to tell the other device to stop or start sending data. With software flow control the RTS and CTS lines are not used. DTR stands for Data Terminal Ready. Its intended function is very similar to the RTS line. DSR (Data Set Ready) is the companion to DTR in the same way that CTS is to RTS. Some serial devices use DTR and DSR as signals to simply confirm that a device is connected and is turned on. The Software Wedge sets DTR to the mark state when the serial port is opened and leaves it in that state until the port is closed. The DTR and DSR lines were originally designed to provide an alternate method of hardware handshaking. It would be pointless to use both RTS/CTS and DTR/DSR for flow control signals at the same time. Because of this, DTR and DSR are rarely used for flow control. CD stands for Carrier Detect. Carrier Detect is used by a modem to signal that it has a made a connection with another modem, or has detected a carrier tone. The last remaining line is RI or Ring Indicator.

The Carrier Detect (CD) and the Ring Indicator (RI) lines are only available in connections to a modem. Because most modems transmit status information to a PC when either a carrier signal is detected (i.e. when a connection is made to another modem) or when the line is ringing, these two lines are rarely used. 9 to 25 Pin Adapters

The following table shows the connections inside a standard 9 pin to 25 pin adapter [5].

9-Pin Connector	**25 Pin Connector**
Pin 1 DCD	Pin 8 DCD
Pin 2 RD	Pin 3 RD
Pin 3 TD	Pin 2 TD
Pin 4 DTR	Pin 20 DTR
Pin 5 GND	Pin 7 GND
Pin 6 DSR	Pin 6 DSR
Pin 7 RTS	Pin 4 RTS
Pin 8 CTS	Pin 5 CTS
Pin 9 RI	Pin 22 RI

3.1.6 Baud Vs Bits per Second

The baud unit is named after Jean Maurice Emile Baudot, who was an officer in the French Telegraph Service. He is credited with devising the first uniform-length 5-bit code for characters of the alphabet in the late 19th century. What baud really refers to is modulation rate or the number of times per second that a line changes state. This is not always the same as bits per second (BPS). If you connect two serial devices together using direct cables then baud and BPS are in fact the same. Thus, if you are running at 19200 BPS, then the line is also changing states 19200 times per second. But when considering modems, this isn't the case. Because modems transfer signals over a telephone line, the baud rate is actually limited to a maximum of 2400 baud. This is a physical restriction of the lines provided by the phone company. The increased data throughput achieved with 9600 or higher baud modems is accomplished by using sophisticated phase modulation, and data compression techniques.

In a perfect world, all serial ports on every computer would be DTE devices with 25-pin male "D" connectors. All other devices to would be DCE devices with 25-pin female connectors. This would allow you to use a cable in which each pin on one end of the cable is connected to the same pin on the other end. Unfortunately, we don't live in a perfect world. Serial ports use both 9 and 25 pins, many devices can be configured as either DTE or DCE, and - as in the case of many data collection devices - may use completely non standard or proprietary pin-outs. Because of this lack of standardization, special cables called null modem cables, gender changers and custom made cables are often required.

3.1.7 Cables Lengths

The RS-232C standard imposes a cable length limit of 50 feet. You can usually ignore this "standard", since a cable can be as long as 10000 feet at baud rates up to 19200 if you use a high quality, well shielded cable. The external environment has a large effect on lengths for unshielded cables. In electrically noisy environments, even very short cables can pick up stray signals. The following chart offers some reasonable guidelines for 24 gauge wire under typical conditions. You can greatly extend the cable length by using additional devices like optical isolators and signal boosters. Optical isolators use LEDs and Photo Diodes to isolate each line in a serial cable including the signal ground. Any electrical noise affects all lines in the optically isolated cable equally - including the signal ground line. This causes the voltages on the signal lines relative to the signal ground line to reflect the true voltage of the signal and thus canceling out the effect of any noise signals.

3.1.8 Gender Changers

A problem may be encounter is having two connectors of the same gender that must be connected.

3.1.9 Null Modem Cables and Null Modem Adaptors

If you connect two DTE devices (or two DCE devices) using a straight RS232 cable, then the transmit line on each device will be connected to the transmit line on the other device and the receive lines will likewise be connected to each other. A Null Modem cable or Null Modem adapter simply crosses the receive and transmit lines so that transmit on one end is connected to receive on the other end and vice versa. In addition to transmit and receive, DTR & DSR, as well as RTS & CTS are also crossed in a Null modem connection.

3.1.10 Synchronous and Asynchronous Communications

There are two basic types of serial communications, synchronous and asynchronous. With Synchronous communications, the two devices initially synchronize themselves to each other, and then continually send characters to stay in sync. Even when data is not really being sent, a constant flow of bits allows each device to know where the other is at any given time. That is, each character that is sent is either actual data or an idle character. Synchronous communications allows faster data transfer rates than asynchronous methods, because additional bits to mark the beginning and end of each data byte are not required.

The serial ports on PCs are asynchronous devices and therefore only support asynchronous serial communications. Asynchronous means "no synchronization", and thus does not require sending and receiving idle characters. However, the beginning and end of each byte of data must be identified by start and stop bits. The start bit indicate when the data byte is about to begin and the stop bit signals when it ends. The requirement to send these additional two bits cause asynchronous communications to be slightly slower than synchronous however it has the advantage that the processor does not have to deal with the additional idle characters. An asynchronous line that is idle is identified with a value of 1, (also called a mark state). By using this value to indicate that no data is currently being sent, the devices are able to distinguish between an idle state and a disconnected line. When a character is about to be transmitted, a start bit is sent. A start bit has a value of 0, (also called a space state). Thus, when the line switches from a value of 1 to a value of 0, the receiver is alerted that a data character is about to come down the line.

3.2 Wiegand Interface

Wiegand interface is a defacto industry standard used for interfacing card readers to control panels. So basically the wiegand format is used for security card data encoding. There is a lot of confusion regarding the 'Wiegand Format', when the term WIEGAND is used it basically means a 26-bit data format with a specific arrangement of binary data. This 26-bit data format is a widely used industry standard. Almost all access control systems accept the standard 26-bit data format. 26-bit originated with true Wiegand swipe card technology. There are other data format like the 34-bit & 37-bit format which use the same signaling standard as that of wiegand but have different data formatting standard.

3.2.1 Wiegand Data Format Standard

The wiegand format consists of a parity bit, 8-bit facility code, 16-bit user ID, and another parity bit. A parity bit is used as a very simple quality check for the accuracy of the transmitted binary data. In the above example, the leading parity bit (even) is linked to the first 12 data bits. If the 12 data bits result in an odd number, the parity bit is set to one to make the 13-bit total come out even. The final 13 bits are similarly set to an odd total.

3.2.2 Wiegand Signaling Standard

For communication with the microcontroller the Wiegand interface uses two wires for carrying the card data to the controller these wires are called as DATA0 & DATA1. Normally both these lines are high i.e. when no data is being sent. A '0' is sent by making DATA0 line LOW & DATA1 line HIGH. Whereas a '1' is sent by making DATA1 line LOW & keeping DATA0 line HIGH. This signal is at TTL level & not an open collector signal so can be directly connected to the Microcontroller.

A typical pulse width is 50 μs with an inter-spacing of 1ms but the actual timing values & output circuitry (open collector/TTL) are determined by the card reader manufacturer.

Chapter 4

IMPLEMENTATION

In this chapter the methodology of the implementation of individual module of the project is discussed. This chapter covers the following main topics:

- Interface of Microcontroller with RFID Reader
- Interface of Microcontroller with Mobile Device
- Interface of Mobile Device with Computer

4.1 Interface of Microcontroller with RFID Reader

As the aim of the project is to establish wireless communication between RFID Reader and backend computer system so for this we need some intelligent device which can get data from RFID Reader and send it to the backend Computer system. For this purpose Atmel 89c52 Microcontroller is used.

4.1.1 Atmel 89c52 Microcontroller

The AT89c52 is a low-power, high-performance CMOS 8-bit microcontroller with 4K bytes of In-System Programmable Flash memory. The device is manufactured using Atmel's high-density nonvolatile memory technology and is compatible with the industry- standard 80C51 instruction set and pinout. The on-chip Flash allows the program memory to be reprogrammed in-system or by a conventional nonvolatile memory programmer. By combining a versatile 8-bit CPU with In System Programmable Flash on a monolithic chip, the Atmel AT89c52 is a powerful microcontroller which provides a highly-flexible and cost-effective solution to many embedded control applications. The AT89S51 provides the following standard features: 8K bytes of Flash, 128 bytes of RAM, 32 I/O lines, Watchdog timer, two data pointers, two 16-bit timer/counters, a five-vector two level interrupt architecture, a full duplex serial port, on-chip oscillator, and clock circuitry. In addition, the AT89c52 is designed with static logic for operation down to zero frequency and supports two software selectable power saving modes. The Idle Mode stops the CPU while allowing the RAM, timer/counters, serial port, and interrupt system to continue functioning. The Power-down mode saves the RAM contents but freezes the oscillator, disabling all other chip functions until the next external interrupt or hardware reset [6].

4.1.2 RFID Reader and Microcontroller Communication

After reading data from the RFID Tag the RFID Reader transmits the data to the main controlling device the microcontroller through wiegand protocol. The data on the RFID Tag is 26 bits unique ID which is received by the microcontroller from the RFID Reader through Interrupts at its interrupt pins. The interrupts are handled by an interrupt handler. For each interrupt pin of the microcontroller there is an interrupt routine which is called automatically when an interrupt is generated by the RFID reader at the interrupt pin of the microcontroller. The interrupt routine0, which is called when interrupt is generated at interupt0 pin of the microcontroller, adds bit 0 into the interrupt handler and the interrupt routine1, which is called when interrupt is generated at interupt1 pin of the microcontroller, adds bit 1 into the interrupt handler. The interrupt handler can handle 26 interrupts.

4.1.3 Data Manipulation

After reading 26 bits data from the RFID Reader the microcontroller converts this binary data into the decimal format for simplicity and better user readability. The binary data is converted into the decimal format by left shift operator which applies on a variable after taking applying xor operation on the variable and 26 1s.

4.1.4 Microcontroller and LCD interface

After binary to decimal conversion the data is printed on the LCD. The pins number 32, 33,34,35,38 and 39 of the microcontroller are connected to the 4, 5,11,12,13 and 14 number pins of the LCD. The size of the LCD is 2X16 i,e two rows and 16 columns.

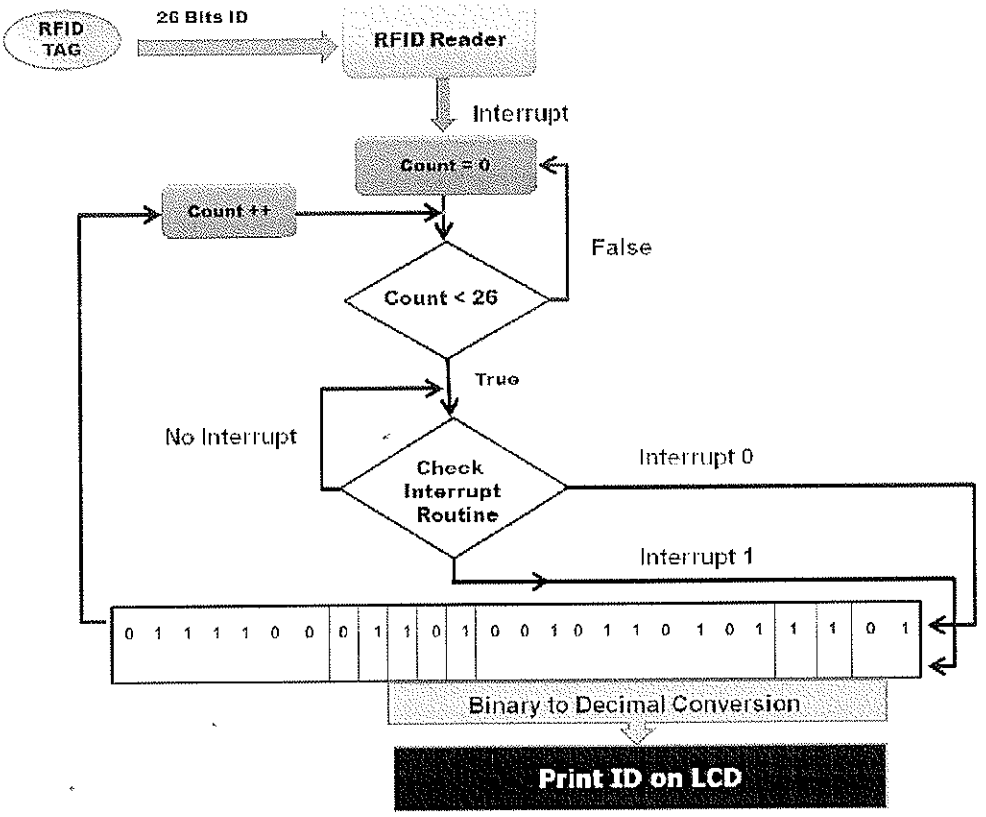


Fig 4.1 Tag data flow in interface of RFID Reader and Microcontroller

4.2 Microcontroller and Mobile device interface

The microcontroller and mobile device have communication through RS-232 serial interface with the mobile device. The microcontroller communicates with the mobile device through AT commands.

After reading data from the RFID reader the microcontroller sends it to the mobile device through the AT Commands. The microcontroller configures the mobile device to send the data through SMS and GPRS. The microcontroller for SMS tells the microcontroller the number of the SIM which is inserted into another mobile device that is attached to the backend server. To send the data through GPRS the microcontroller embeds the data into the URL of the web page hosted on the backend server and sends it to the serial port of the mobile device. The mobile device opens this URL and on page load the data is entered into the backend database.

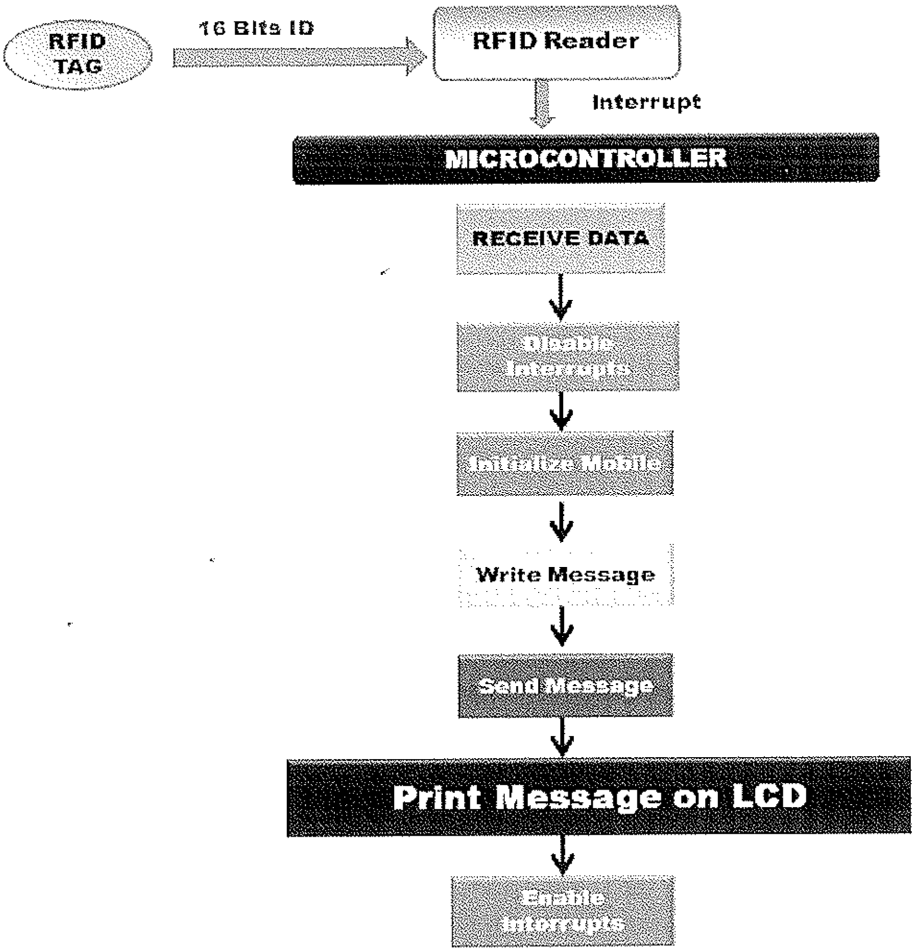


Fig 4.2 Microcontroller and Mobile device interface to send SMS

While sending the data to Mobile device the microcontroller disables its interrupt pins and after sending the data it again enable its interrupt pins.

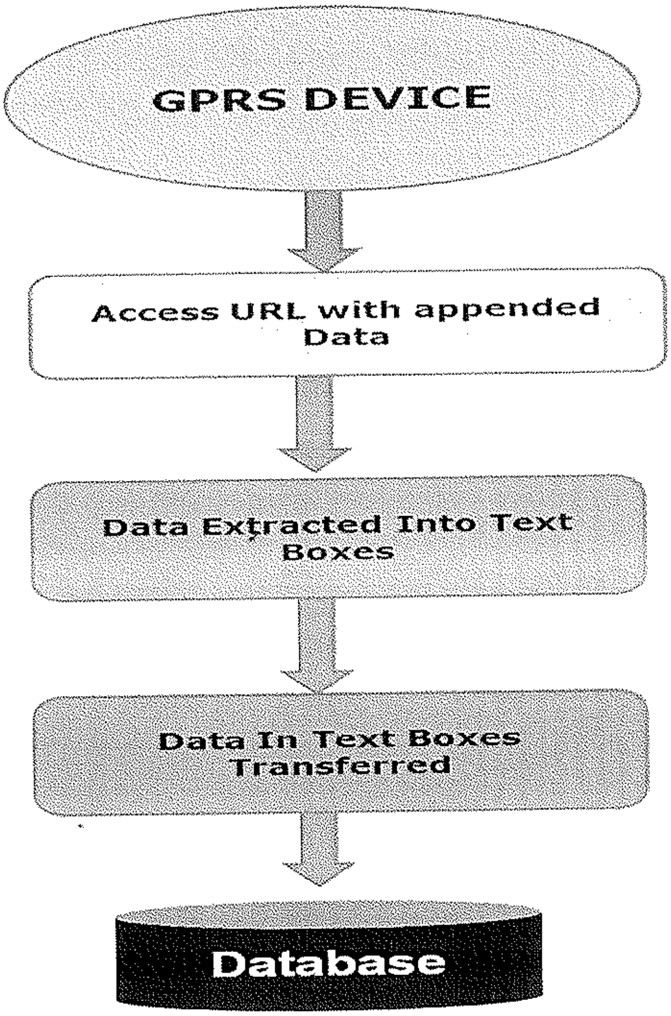

GPRS DEVICE
Access URL with appended Data
Data Extracted Into Text Boxes
Data In Text Boxes Transferred
Database

Fig 4.3 Steps to send the data through GPRS

4.3 Mobile device and Computer Interface

To receive the data from the RFID Reader through SMS there is another mobile device which receives the SMS. This mobile device is attached to the serial port of the computer. To read the SMS from the mobile device a software utility is developed into the Visual Basic 6 which receives the SMS from the mobile device by AT commands and stores the data into the data base. There is an active control in the software utility which performs the functionality of reading data from the buffer of the serial port of the computer. This software utility can also search the data from the mobile device by entering anyone of Tag ID, Reader ID, Time and Date.To communicate with the mobile device the software utility first configure the settings to Baud rate equal to 115200 bits/sec, data bits equal to 7, start bit equal to 1 and parity bit equal to 0.

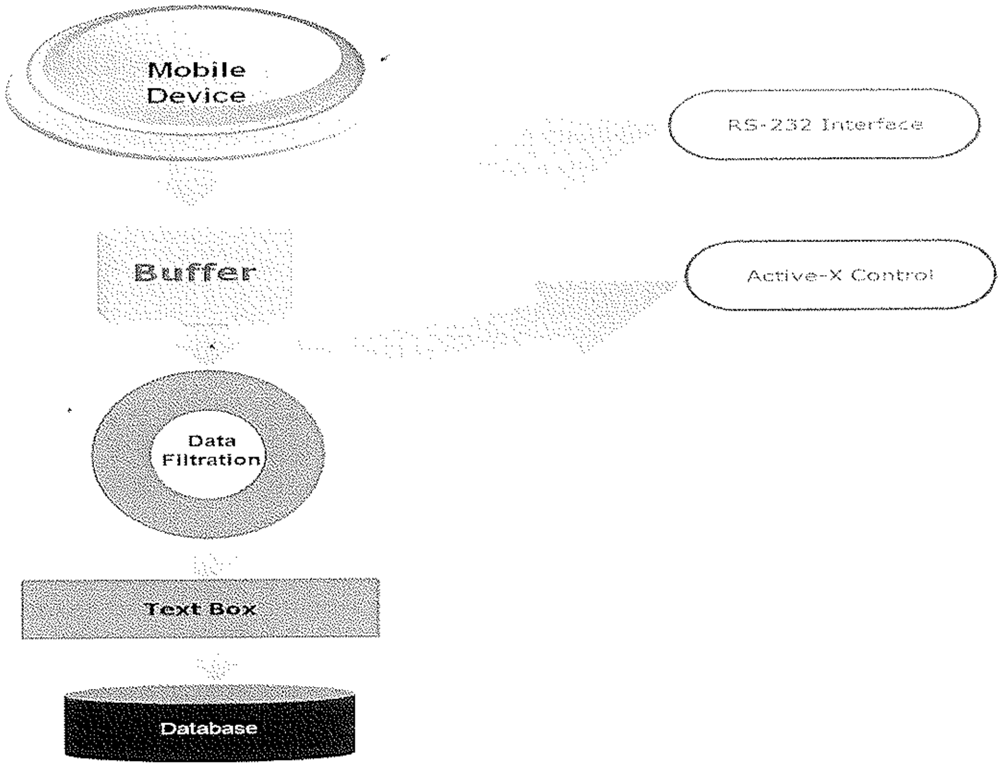
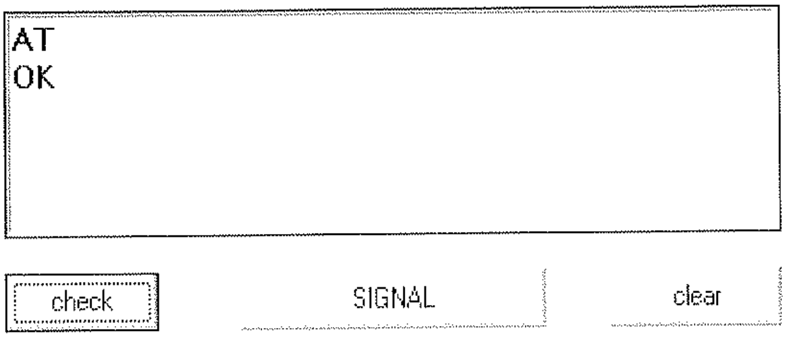


Fig 4.4 How the Mobile device interacts with computer and the data flow

Chapter 5

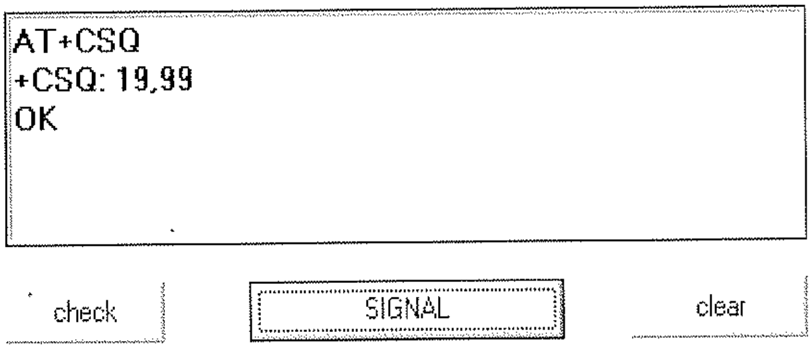
RESULTS

This chapter shows the results of the software utility, which is to handle the SMS and searching of data, and the web page which handles the GPRS data.



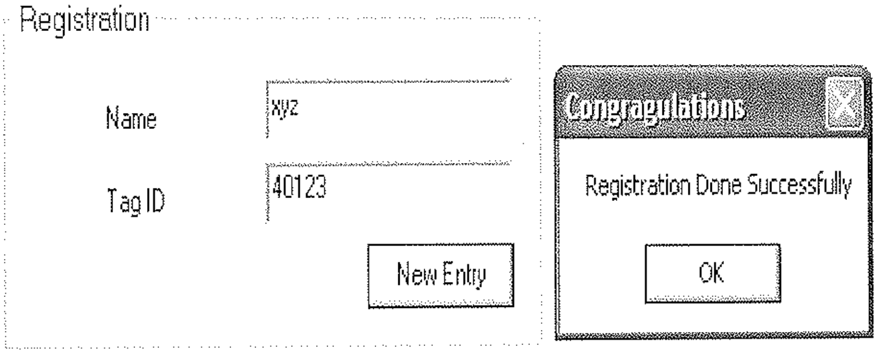
```
AT
OK
```

Fig 5.1 *The response of the mobile device through AT command*



```
AT+CSQ
+CSQ: 19,99
OK
```

Fig 5.2 *Signal level of the mobile device through AT command*



Registration

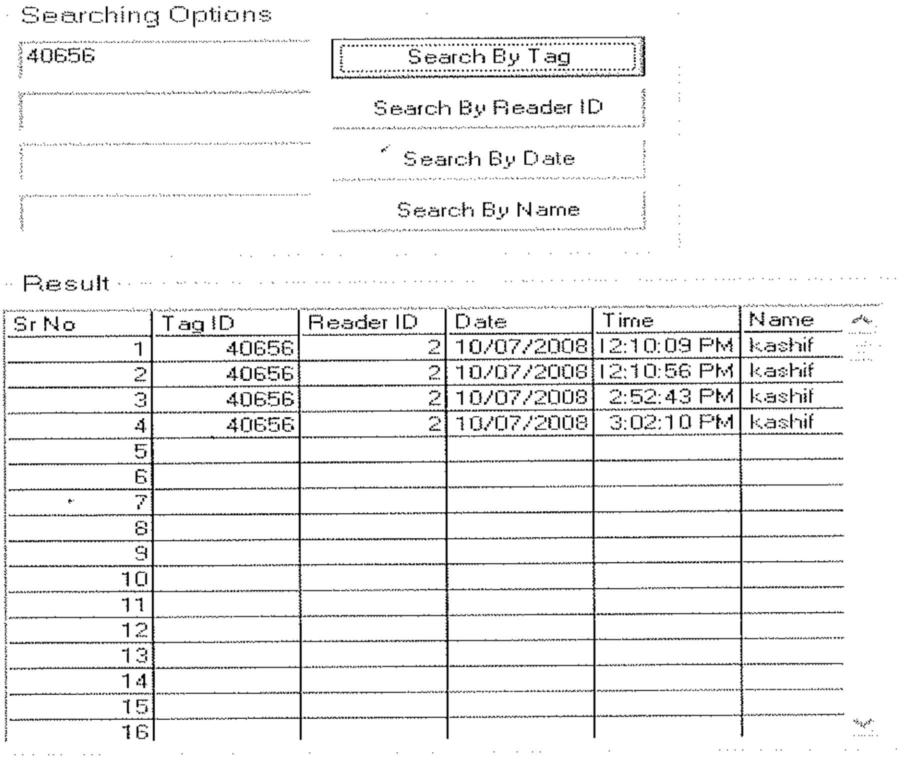
Name: xyz

Tag ID: 40123

Congragulations

Registration Done Successfully

Fig 5.3 Registration of an RFID Tag into the Database.



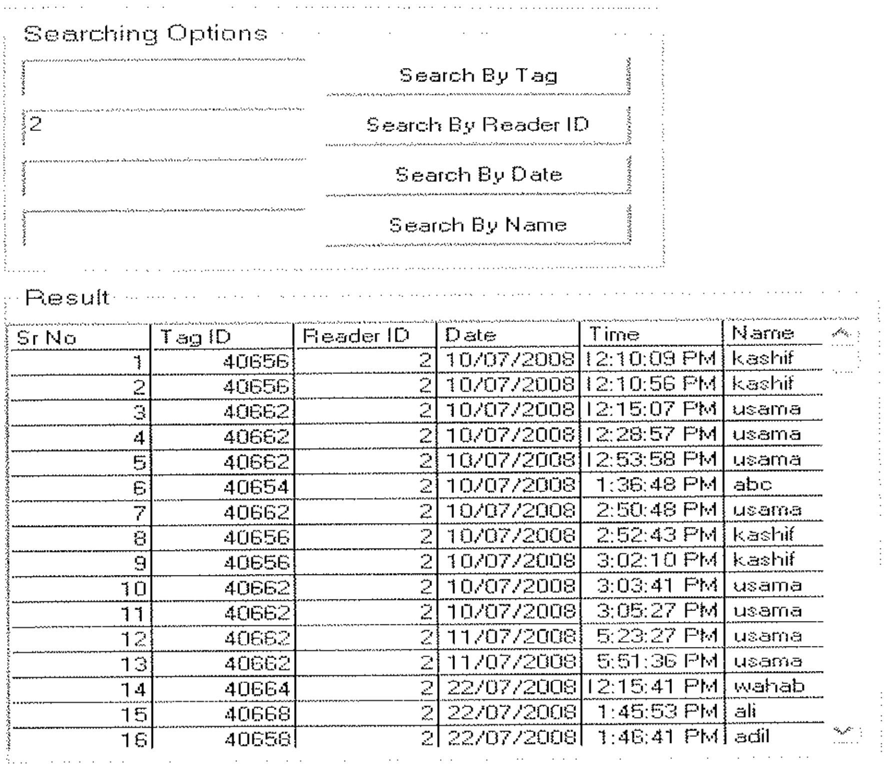
Searching Options

40656

Result

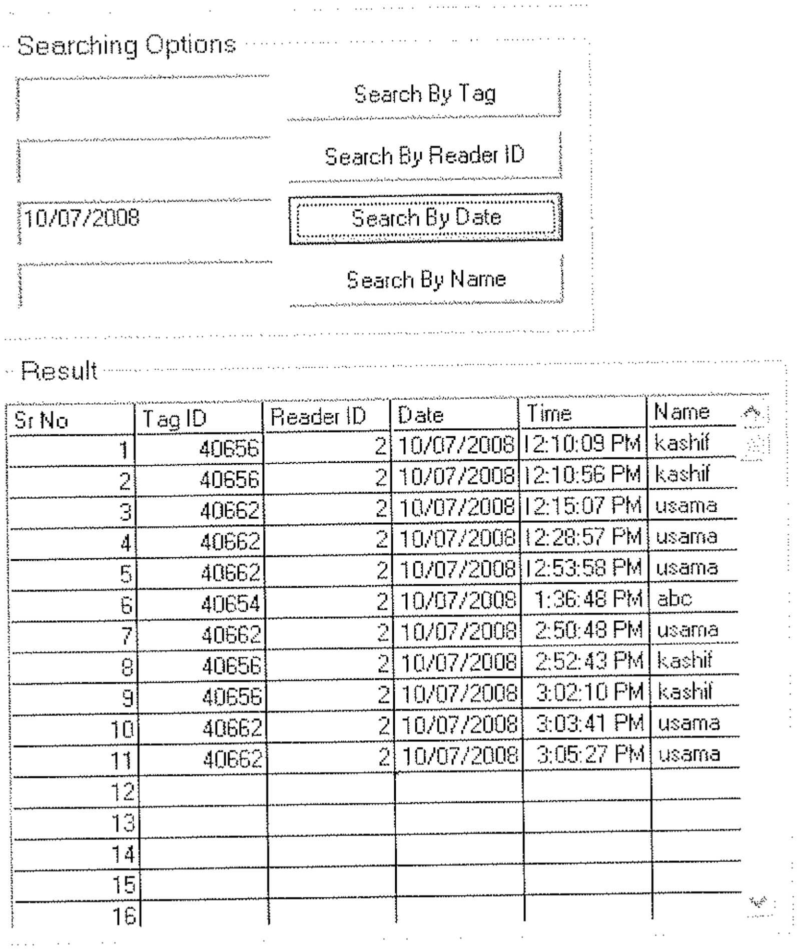
Sr No	Tag ID	Reader ID	Date	Time	Name
1	40656	2	10/07/2008	12:10:09 PM	kashif
2	40656	2	10/07/2008	12:10:56 PM	kashif
3	40656	2	10/07/2008	2:52:43 PM	kashif
4	40656	2	10/07/2008	3:02:10 PM	kashif
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					

Fig 5.4 Searching of the information from Database through Tag ID.



Sr No	Tag ID	Reader ID	Date	Time	Name
1	40656	2	10/07/2008	12:10:09 PM	kashif
2	40656	2	10/07/2008	12:10:56 PM	kashif
3	40662	2	10/07/2008	12:15:07 PM	usama
4	40662	2	10/07/2008	12:28:57 PM	usama
5	40662	2	10/07/2008	12:53:58 PM	usama
6	40654	2	10/07/2008	1:36:48 PM	abc
7	40662	2	10/07/2008	2:50:48 PM	usama
8	40656	2	10/07/2008	2:52:43 PM	kashif
9	40656	2	10/07/2008	3:02:10 PM	kashif
10	40662	2	10/07/2008	3:03:41 PM	usama
11	40662	2	10/07/2008	3:05:27 PM	usama
12	40662	2	11/07/2008	5:23:27 PM	usama
13	40662	2	11/07/2008	5:51:36 PM	usama
14	40664	2	22/07/2008	12:15:41 PM	wahab
15	40668	2	22/07/2008	1:45:53 PM	ali
16	40658	2	22/07/2008	1:46:41 PM	adil

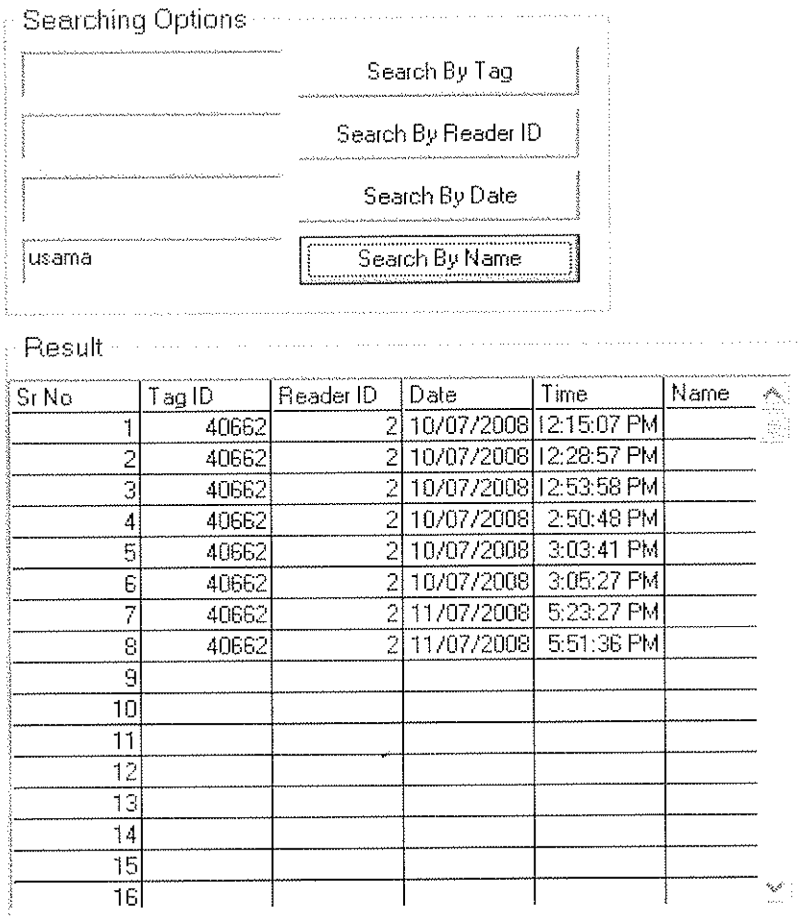
Fig 5.5 *Searching of the information from Database through Reader ID*



10/07/2008

Sr No	Tag ID	Reader ID	Date	Time	Name
1	40656	2	10/07/2008	12:10:09 PM	kashif
2	40656	2	10/07/2008	12:10:56 PM	kashif
3	40662	2	10/07/2008	12:15:07 PM	usama
4	40662	2	10/07/2008	12:28:57 PM	usama
5	40662	2	10/07/2008	12:53:58 PM	usama
6	40654	2	10/07/2008	1:36:48 PM	abc
7	40662	2	10/07/2008	2:50:48 PM	usama
8	40656	2	10/07/2008	2:52:43 PM	kashif
9	40656	2	10/07/2008	3:02:10 PM	kashif
10	40662	2	10/07/2008	3:03:41 PM	usama
11	40662	2	10/07/2008	3:05:27 PM	usama
12					
13					
14					
15					
16					

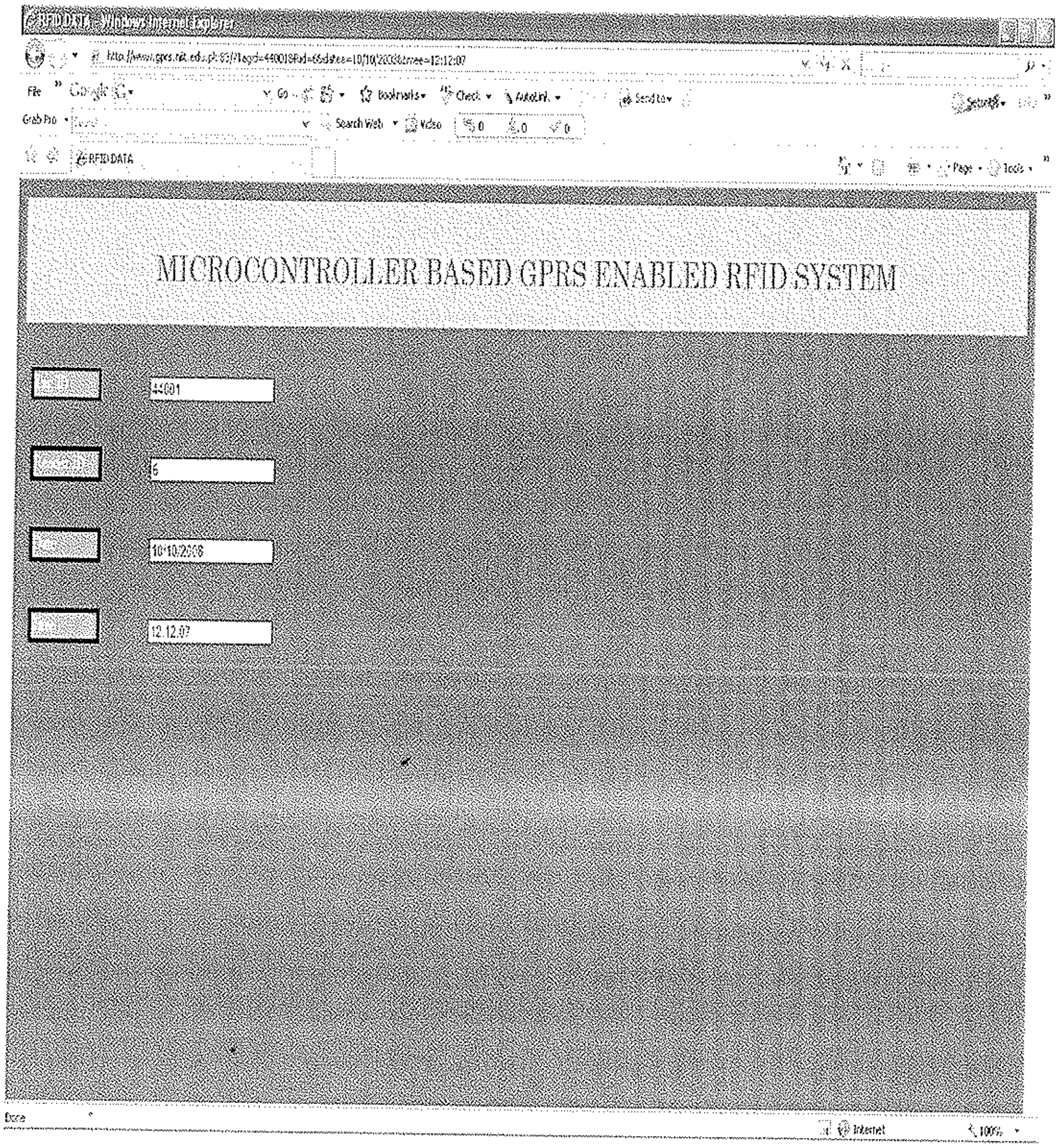
***Fig 5.6** Searching of the information from Database through date.*



usama

Sr No	Tag ID	Reader ID	Date	Time	Name
1	40662	2	10/07/2008	12:15:07 PM	
2	40662	2	10/07/2008	12:28:57 PM	
3	40662	2	10/07/2008	12:53:58 PM	
4	40662	2	10/07/2008	2:50:48 PM	
5	40662	2	10/07/2008	3:03:41 PM	
6	40662	2	10/07/2008	3:05:27 PM	
7	40662	2	11/07/2008	5:23:27 PM	
8	40662	2	11/07/2008	5:51:36 PM	
9					
10					
11					
12					
13					
14					
15					
16					

Fig 5.7 *The searching of the information from Database through Time.*



http://www.gprs.nit.edu.pk:85/?tagid=44001&id=6&dates=10/10/2008&time=12:12:07

MICROCONTROLLER BASED GPRS ENABLED RFID SYSTEM

44001

6

10/10/2008

12.12.07

Fig 5.8 *The webpage which receives Data through GPRS and save it into database on every page load.*

Chapter 6

CONCLUSION

Radio frequency Identification system is widely used all over the world in a lot of applications. The wired communication between RFID Reader and Backend System, is an issue in a lot of applications, restricts this superb technology to adopt for automation, authentication, inventory management and a lot more application.

This project addressed this issue and gives a solution for wireless communication between RFID Reader and Backend System. It makes the RFID system simple and easy to implementable. This wireless RFID System can make RFID technology feasible in a lot of applications where it is hard to use it.

Chapter 7

RECOMMENDATIONS

This project is based on AT89C52 microcontroller which has small memory and low processing so to enhance the systems efficiency it is recommended to use some microcontroller with more internal memory and greater processing power.

Future work may be based on this project by developing some useful application of this product.

The project can be implemented on FPGA chip but the high prices of FPGA chips is an issue

One of the disadvantages of RFID System is that there is a great security threat in it. The RFID tags can be cloned so a duplicate RFID Tag can be used by any one. Also RFID tags can be read by any reader so the sensitive data stored on the tag can be disclosed which is a great threat.

REFERENCES

[1] RFID Essentials, By Bill Glover, Himanshu Bhatt January 2006 Series: Theory in Practice ISBN 10: 0-596-00944-5

[2] Intermec System Manual

[3] http://www.dnatechindia.com/index.php/Tutorials/8051 Tutorial/Wiegand.html

[4] http://www.beyondlogic.org/serial/serial.htm

[5] http://www.camiresearch.com/Data_Com_Basics/RS232_standard.html

[6] AT89c52 System Manual

APPENDIX A

ActiveX

A set of technologies that allow software components to interact with one another in a networked environment, regardless of the language in which the components were created

Bandwidth

The difference between the highest and lowest frequencies in a given range. For example, an analog telephone line accommodates a bandwidth of 3,000 hertz (Hz), the difference between the lowest (300 Hz) and highest (3,300 Hz) frequencies it can carry. In digital communications, bandwidth is expressed in bits per second (bps).

Baud rate

The speed at which a modem communicates. Baud rate refers to the number of times the condition of the line changes. This is equal to bits per second only if each signal corresponds to one bit of transmitted data.

Modems must operate at the same baud rate in order to communicate with each other. If the baud rate of one modem is set higher than that of the other, the faster modem usually alters its baud rate to match that of the slower modem.

GPRS

GPRS stands for General Packet Radio System. GPRS provides packet radio access for mobile Global System for Mobile Communications (GSM) and time-division multiple access (TDMA) users.

GPRS is important as a migration step toward third-generation (3G) networks and allows network operators to implement an IP-based core architecture for data applications, which will continue to be used and expanded for 3G services for integrated voice and data applications.

GPRS is a new bearer service for GSM that greatly improves and simplifies wireless access to packet data networks, e.g., to the Internet. It applies a packet radio principle to transfer user data packets in an efficient way between GSM mobile stations and external packet data networks. Packets can be directly routed from the GPRS mobile stations to packet switched networks.

Virtual IP address

An IP address that is shared among the hosts of a Network Load Balancing cluster. A Network Load Balancing cluster might also use multiple virtual IP addresses, for example, in a cluster of multi homed Web servers.

Interrupt

A request for attention from the processor. When the processor receives an interrupt, it suspends its current operations, saves the status of its work, and transfers control to a special routine known as an interrupt handler, which contains the instructions for dealing with the particular situation that caused the interrupt.

Server

In general, a computer that provides shared resources to network users.

Packet

An Open Systems Interconnection (OSI) network layer transmission unit that consists of binary information representing both data and a header containing an identification number, source and destination addresses, and error-control data.