Q

SP3078

DEVELOPMENT OF ACCESS CARD USING MICROCONTROLLER

A DISSERTATION

Submitted in partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY
in
ELECTRONICS AND COMMUNICATION ENGINEERING

By

Shitij Chopra (031006)

Himanshu (031024)

Rohan Gupta(031103)

विद्या तत्व ज्योतिसम:
JAYPEE UNIVERSITY OF
INFORMATION TECHNOLOGY

Department of Electronics and Communication Engineering,
Jaypee University of Information Technology, Waknaghat,
Solan - 173215, Himachal Pradesh, INDIA.

MAY 2007

CERTIFICATE

This is to certify that the work entitled, "Microcontroller Based Access Card" submitted by Himanshu, Shitij Chopra & Rohan Gupta in partial fulfillment 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.

Vivek

Name of Supervisor: - Mr Vivek Sehgal.

ACKNOWLEDGMENT

First of all, we would like to thank our project supervisor Mr. Vivek Sehgal , for his able guidance and support in the conception and development of this project. His suggestions in visualizing the project and sustained interest to attain the objective envisaged in the project are gratefully acknowledged.

A special thanks to Mr. Rohit Shrama , Faculty (Department Of Electronics & Communication) for his constant guiding vision and motivation that went a long way in materializing this project.

TABLE OF CONTENTS

1. INTRODUCTION

2. LITERATURE SURVEY AND RELEVANT THEORY

3. HARDWARE DESCRIPTION

4. SOFTWARE DESCRIPTION

5. RESULTs, CONCLUSION AND FUTURE SCOPE

LIST OF FIGURES

Chapter 1:- INTRODUCTION

Chapter 2: - LITERATURE, SURVEY AND RELEVANT THEORY

Chapter 3: - HARDWARE DESCRIPTION

Chapter 4: - SOFTWARE DESCRIPTION

LIST OF TABLES

Chapter 2: - LITERATURE, SURVEY AND RELEVANT THEORY

Chapter 3: - HARDWARE DESCRIPTION

Chapter 5: - RESULTS, CONCLUSION AND FUTURE SCOPE

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 cardholder. 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.) and time restrictions. All 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 frame work and supporting interoperability frame work 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 & privilege are verified in a truly reliable way, that identification is authoritative .

1.2 Access Control

Access control is a matter of who, where and when. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Mechanical locks and keys generally do not allow restriction of the key holder to specific times or dates. . Mechanical locks and keys do not provide records of the key used on any specific door and the key can be easily copied transferred to an unauthorized 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 limitation 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 system is the credential reader. A reader reflects the technology of the credential. The reader for a magnetic stripe, bar code, or Wig and card is typically called a swipe reader and is in common use in retail stores and ATMS.Some swipe readers requires 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. When infrareds used for data transmission it become smart IR reader. To the user, an access control system is composed of.

- A card that is presented to a door reader,
- The reader, that responds with a signal indicating a valid card, and
- The door or gate, that is unlocked if entry is authorized.

1.3 Types of Access Systems

Systems can be grouped into three different categories: Stand-Alone, Simple On-Line, and PC host based. Each group has different features, capabilities, and cost that must be matched to your needs. A description of each group follows.

1.3.1 Stand Alone Systems

Stand-Alone card access systems consist of one or two card readers operating independent of computers. These types of systems generally have limited card capacities and features. Stand-Alone systems are often selected by businesses having only a few doors to control and a limited number of people requiring a few cards. Owners of these systems are not interested in recording system use or in restricting access by time of day, day of week. The advantages of stand-alone systems are low cost and ease of operation.

1.3.2 On –Line Systems

In an on-line system, the readers are interconnected to each other, allowing communication with a controller and computer terminal. It is common for the readers to rely on the computer to make the access control decisions. The card readers get information from the card and send it to the computer for processing. The computer compares the information received from the card reader against information contained in its memory. If the proper information is found, the computer signals the card reader to unlock the door. Event recording is a primary advantage of on-line systems, which can print events on a printer or store the information electronically in a computer.

On-line systems can control a larger number of doors and have memory for a larger number of cards. They also feature more access levels and schedules. These two features allow the operators to specify what doors an individual can use, the time of day each door can be used, as well as the days of the week each door can be used.

1.3.3 PC-Host Based Systems

These are enhanced or expanded versions of the on-line systems described previously. They have expanded reader and card capacities and more refined and sophisticated features. Complex on-line systems generally have extensive alarm point monitoring capabilities and can display graphic representations of the facility, aiding in the identification and location of alarms. They can control gates, lights, and other security related equipment such as video surveillance cameras. Complex on-line systems can control several hundred doors, tens of thousands of cards, and monitor thousands of alarm points. They are capable of being controlled or operated from several locations.

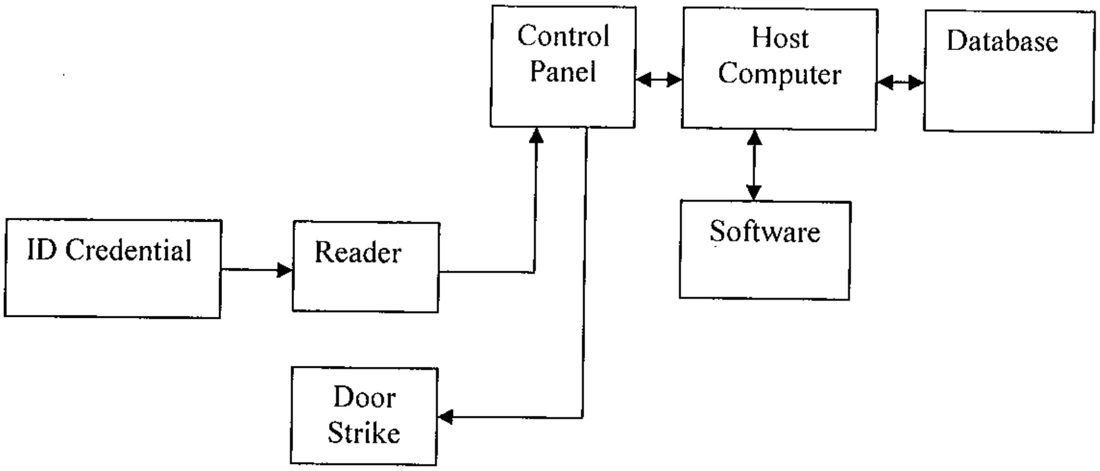


Fig 1.1: Access Control System Schematic

For example, the security director of a facility may have a terminal in his or her office for administering the system, and a guard station may have a terminal for acknowledging and responding to alarms and other events.

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 protected in such a fashion that data cannot be directly accessible without going through certain security mechanism contained with in the card.

1.5 Need of the Work to Be Done

Security is highly demand today. The growing possibilities of theft & fraud need the special means of security. This is to design a cheep & more secure system. Already exist 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 card are secure but they are costly. On the other hand there are some systems, which are more secure as they are on the data code bases but they are also very costly. In existing system hardware is increased as no. of user increases. But in this thesis, hardware is not depending on no. of users. By using this system it can make your device to be work in the presence of a particular person. In existing systems, everyone can access the any device. So there is a need to design a security system which on the one hand is cheep & one the other hand provide the security of access to particular person having particular card.

1.6 Objective of Thesis

Electronic access control generally refers to the substitution of keys with electronically encoded cards. Biometric identification is more reliable and capable than the traditional knowledge based techniques differentiating between an authorized person and a fraudulent imposter. In this technology distinguishing traits such as fingerprint, face, and voice or hand geometry recognizes each 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 access system and to minimize power loss. This electronic access system will allow convenient and efficient access to all card-related services. Smart cards allow elimination of inefficiencies that have characterized public service systems in the past paper based cards. Also, storage and transmission of sensitive personal information will be handled securely. Users should gain confidence in these systems as everyone will benefit from their efficiencies and reduced cost. Thus, bringing maximum security to the overall system.

1.7 Block Diagram

This system has two parts- one is contact less card and another is card reader. Card reader is ideal for applications such as access control, attendance monitoring etc.

1.7.1 About Card

There are predefined codes for every card. Codes are stored in the micro controller's memory. Micro controller has inbuilt EEPROM so it uses inbuilt EEPROM to store the code for a user. EEPROM technology features low voltage capability, an EEPROM endurance of 100,000 write/erase cycles, a ten year EEPROM data retention and over 5000V of ESD protection, thereby ensuring safe storage of the card data throughout the lifetime of the card. Each micro controller is programmed for a specific predefined code thus each user will have a unique code. Whenever a user attempt card &press the switch present on card, in front of card reader at 6 inches of distance, code stored in the memory is transmitted serially from the micro controller to power amplifier. And power amplifier makes it capable to be fed to the IR transmitting LED.

1.7.2 About Card Reader

Card reader, from the card at baud rate of 9600bps receives codes. Infrared receiver works in positive logic i.e. when the IR light falls on it, its output goes high and when the IR light doesn't fall on it, its output goes low. Receiver passes these codes to the PC .MAX 232 will make it compatible with PC. The software will check and compare the code received. If the code is present in the database then it will switch on the electromagnetic relay circuitry using parallel port. Otherwise it will give a message on screen or make a sound buzzer on. If the code matches as there in database, then it will open the door using stepper motor. Make the power supply on for a particular cabin. And make the attendance record on the basis of time.

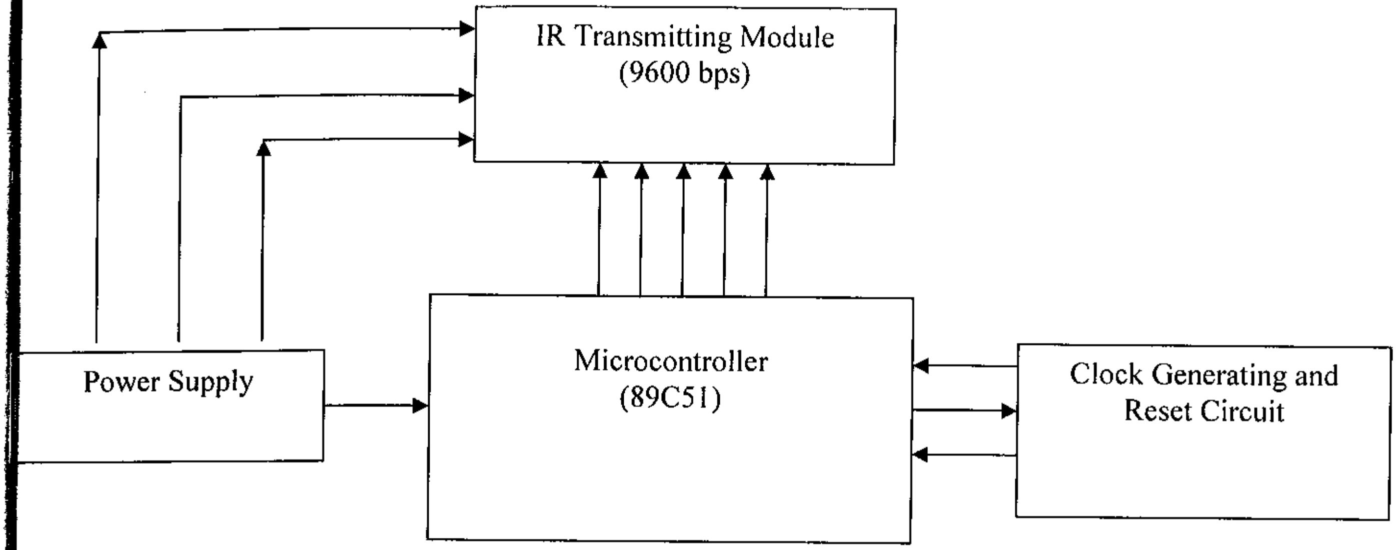


Fig 1.2: Block Diagram of Card

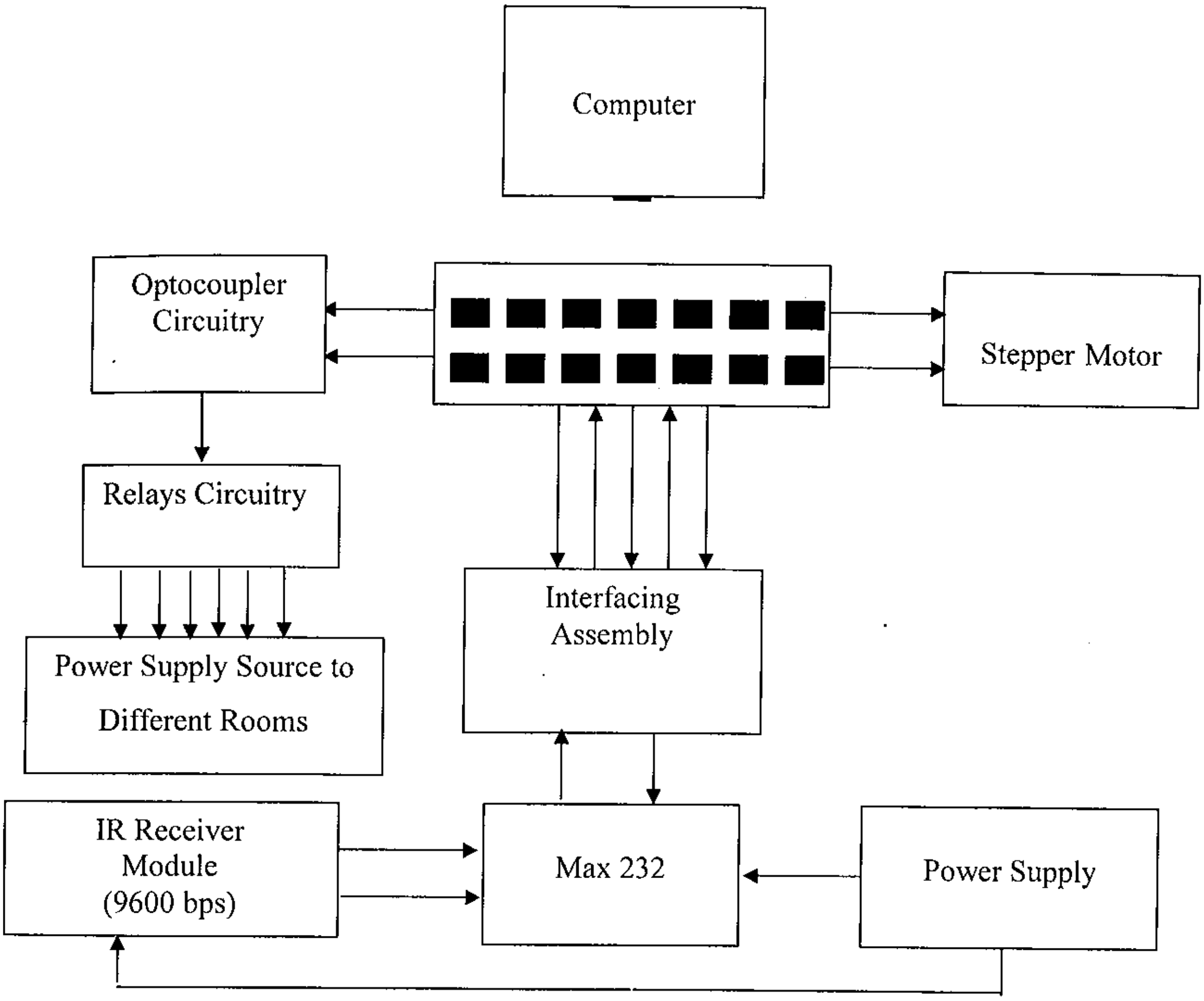


Fig 1.3: Block Diagram of Card Reader

1.8 Organization of the Thesis

Chapter 1: Describes the objectives of the study and definition of the topic

Chapter 2: Describes the literature review and methods used to conduct the study and dedicate to relevant theory.

Chapter 3: Describes the different hardware components which are used

Chapter 4: Describe the software.

Chapter 5: Conclusion and future work.

CHAPTER 2
LITERATURE SURVEY AND RELEVANT THEORY

2.1 Literature Survey

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

Smart card technology has been around for more than 20 years. Since its first introduction into the market, its main application is for the payphone system. As card manufacturing cost decreased, smart card usage has expanded. Its use in Asia is expected to be growing at a much faster pace than in Europe. According to a survey performed by Ovum Ltd., the numbers of smart card units have reached 2.7 billion by 2003. The largest markets will be in prepayment applications, followed by access control, and electronic cash applications. According to a study by Dataquest, the overall market for memory and microprocessor-based cards has grown from 544 million units in 1995 to 3.4 billion units by 2001 .

In May 1996, several companies including Microsoft, Hewlett-Packet and Schlumberger formed a PC/SC workgroup which aimed at integrating the smart card with personal computer (PC). This workgroup mainly concentrates on producing a common smart card and PC interface standards for the smart card and PC software producers. Many of the interface standards and hierarchy have already been established. Some of these prototype products are now available on the market .

The smart card is expected to be used in many applications and especially in personal security related applications such as access control, computer logon, secure email sending and retrieving services. The reason for this growth lies in the smart card's portability and security characteristics

The security requirements of smart cards in personal communication system are two folds; they are authentication & protection of information. This paper deals with matter pertaining to the application of IC cards (or smart cards) in the security of personal communication system.

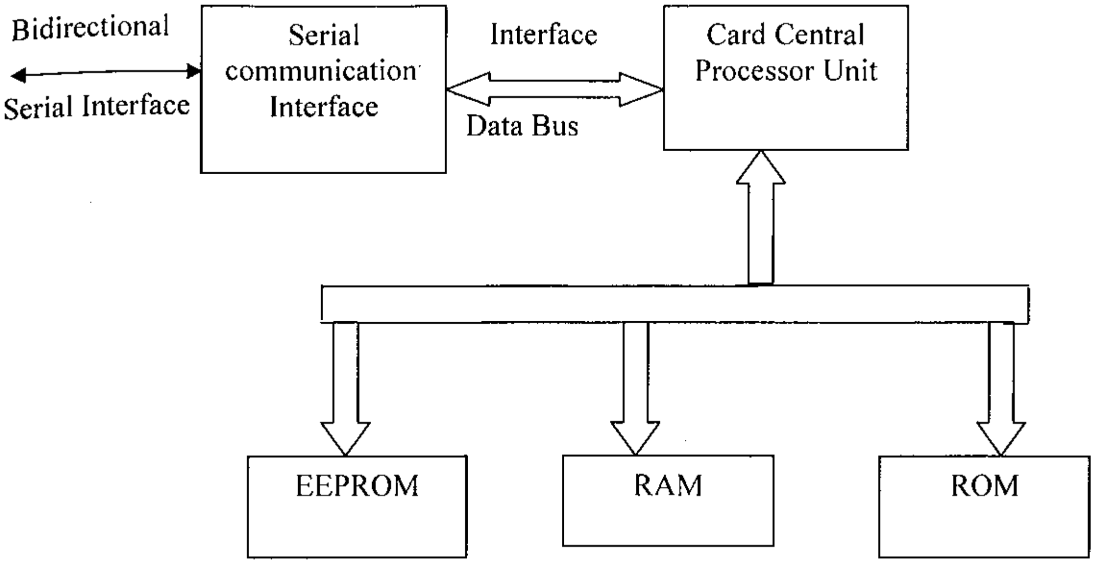


Fig 2.1: Smart Card Internal Architecture

Security advantages achieved by the use of smart cards in security system are discussed. Smart card is required to perform three fundamental functions -

(1) To communicate with a host device

(2) To store data

(3) And to process data received by and stored in the card.

In general smart cards conform to a standard architecture. The key element in this architecture is a microcontroller, ROM, RAM, EEPROM & a communication interface.

A pc based smart card reader is designed and fabricated for contact smart cards that conform to the ISO 7816 standard is described. Reader developed will be able to accept both synchronous & asynchronous cards. Built to be interfaced to standard PC via the parallel port. Software portion is to conform to ISO 7816-3.reader will generate the appropriate clock & VCC input signal on board, support 5-volt cards, and provide bidirectional data line of the card .

2.1.1 Active IR Sensors

These are free standing line sensors that consist of IR transmitters, photo detectors, and application specific lenses.

2.1.2 Passive IR Sensors

Every person, aimed, or object emits IR energy as a function of its surface temperature and size. Such radiated energy is in the wavelength region of 10micron for normal ambient temperature. Passive IR (PIR) sensors detect changes in thermal infrared radiation with in a specific field of view, responding to both changes of scene (including desired target) and change in illumination. PIR systems are widely used for interior application, and are now being used for exterior freestanding and wide area applications .

The user authentication scheme enables the receiver to distinguish between the intruders and the legitimate users. Access control protects the objects from attaching by the unauthorized users. Integrating these two mechanisms in to a single module benefits security, communication overheads, and computation cost .

In order to send command signal to and collect data from a wheelchair during propulsion, an IR data communication system was designed. The digital data from the smart wheel goes to the transmitter attached to the wheel and is transmitted at a data rate of 38.4Kbps.the receiver gets the data at a distance of 6m & then the data is transmitted to the RS-232 serial port of a PC. The infrared chip set acts as a transceiver, so the command signal can also be sent to the smart wheel. as a medium for short range, indoor communication , infrared radiation offers several advantages over Radio IR emitter and detectors capable of high speed operations are available at low cost. Infrared devices cannot penetrate through walls or other opaque barriers, so that infrared transmission is restricted to line-of-site with in the area in which they are originated. This aspect or IR communication prevents interference between links operating in different room, so transmission in different rooms need not be coordinated. Even in the same room, IR radiation does not interfere with other systems which do not use IR. To reduce interference from the wheel chair user's hand moving between the IR transceivers, we mount the IR transceiver as close as possible to the center of smart wheel .

The recent growth of high performance portable computers and computer network has promoted strong demands for low power interconnection facilities between mobile terminals and networks. The wireless communication offers flexible connections among mobile terminals, and innovates today's computers and communication technologies. There are two alternatives for the wireless communication, radio and infrared. The communication based on the infrared has many advantages over that on the radio. Infrared wireless communication system is proposed dedicated to mobile communication. Specification of infrared communication system for this system is as follows.

Peak wavelength	850nm
Modulation	4PPM
Output power	100mw/sr(pulse peak)
Sensitivity	10micro w/cm^2
Data rate	4 Mbps
Link length	1 cm-100cm,30 degree
Bit error rate	Less than 10^{-8}
Channel	Line-of-sight

Table 2.1: IR Specifications

2.2 Relevant Theory

The smart card is one of the latest additions to the world of information technology. A smart card, simply speaking, is a credit card-sized plastic card with an embedded computer chip and some memory. It is this embedded chip in the smart card that makes the card actually "Smart". The chip can store information (memory cards) or store and process information (microprocessor cards). The 'memory cards' can be viewed as minuscule removable read/write disks with optional security; and the 'processor cards' can be viewed as miniature computers with an input and output port. Latest chip used is microcontroller.

A smart card is like an "electronic wallet". Imagine the power of a computer, the speed and security of electronic data, and the freedom to carry that information anywhere on earth. Imagine a computer so small it fits inside a plastic card like the credit card you carry in your wallet. Imagine the Smart Card. The driving factors of the growing interest in smart cards include the declining cost of smart cards and the growing concern that magnetic stripe cards cannot provide the protections necessary to stop fraud and security breaches. This security issue alone may propel smart card technology to the forefront of business transactions. Historically smart cards were simply memory chips set up to store user information for example phone cards and store cards. Now, smart cards exist which contain processing capacity through the use of computer embedded chips. These still store user information but significantly can carry out transactions without the user data ever leaving the card. This means they are more secure. Smart cards require smart card readers to be able to process transactions with them .

2.2.1 Types of Smart Cards

Smart cards are defined according to the type of chip implanted in the card and its capabilities.There is a wide range of options to choose from when designing a particular system.

2.2.1.1 Memory Cards

Memory cards have no sophisticated processing power and cannot manage files dynamically. All memories communicate to readers through synchronous protocols. There are three primary types of memory cards:

Straight Memory Cards

These cards just store data and have no data processing capabilities. These cards are the lowest cost per bit for user memory. They should be regarded as floppy disks of varying sizes without the lock mechanism. These cards cannot identify themselves to the reader, so your host system has to know what type of card is being inserted into a reader.

Protected/Segmented Memory Cards

These cards have built-in logic to control the access to the memory of the card. Sometimes referred to as the Intelligent Memory Cards, these devices can be set to write protect some or all of the memory array. Some of these cards can be configured to restrict access to both reading and writing. This is usually done with a password or system key. Segmented memory cards can be divided into logical sections for planned multi-functionality.

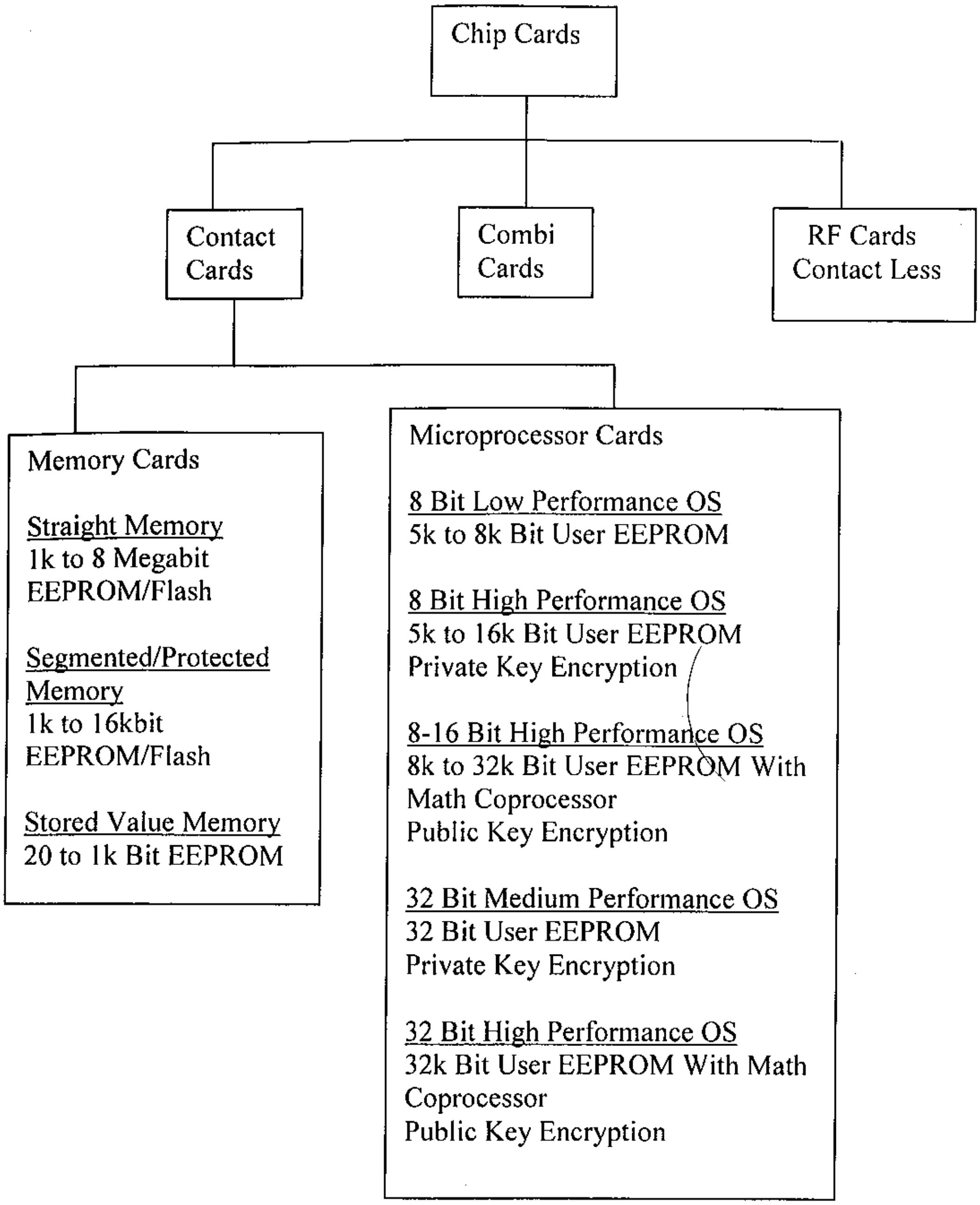

Chip Cards
Contact Cards
Combi Cards
RF Cards Contact Less
Memory Cards
Straight Memory
1k to 8 Megabit EEPROM/Flash
Segmented/Protected Memory
1k to 16kbit EEPROM/Flash
Stored Value Memory
20 to 1k Bit EEPROM
Microprocessor Cards
8 Bit Low Performance OS
5k to 8k Bit User EEPROM
8 Bit High Performance OS
5k to 16k Bit User EEPROM
Private Key Encryption
8-16 Bit High Performance OS
8k to 32k Bit User EEPROM With Math Coprocessor
Public Key Encryption
32 Bit Medium Performance OS
32 Bit User EEPROM
Private Key Encryption
32 Bit High Performance OS
32k Bit User EEPROM With Math Coprocessor
Public Key Encryption

Fig 2.2: Types of Smart Cards

Stored Value Memory Cards

These cards are designed for the specific purpose of storing value or tokens. The cards are either disposable or rechargeable. Most cards of this type incorporate permanent security measures at the point of manufacture. These measures can include password keys and logic that are hard-coded into the chip by the manufacturer. The memory arrays on these devices are set-up as decrements or counters. There is little or no memory left for any other function. For simple applications such as the telephone card, the chip has 60 or 12 memory cells, one for each telephone unit. A memory cell is cleared each time a telephone unit is used. Once all the memory units are used, the card becomes useless and is thrown away. This process can be reversed in the case of rechargeable cards.

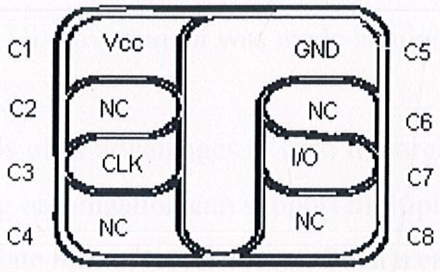


Fig 2.3: Contact Card Module

2.2.1.2 CPU/MPU Microprocessor Multifunction Cards

These cards have on-card dynamic data processing capabilities. Multifunction smart cards allocate card memory into independent sections assigned to a specific function or application. Within the card is a microprocessor or micro-controller chip that manages this memory allocation and file access. This type of chip is similar to those found inside all personal computers and when implanted in a smart card, manages data in organized file structures, via a Card Operating System (COS). Unlike other operating systems, this software controls access to the on-card user memory. This capability permits different and multiple functions and/or different applications to reside on the card, allowing businesses to issue and maintain a diversity of 'products' through the card. One example of this is a debit card that also enables building access on a college campus. Multifunction cards benefit issuers by enabling them to market their products and services via state-of-the-art transaction technology. Specifically, the technology permits information updates without replacement of the installed base of cards, greatly simplifying program changes and reducing costs.

2.2.2 Contact and Contactless Cards

There are two types of smart cards – contact or contact less. A contact smart card has to be inserted into a smart card reader for access. The micro module has connectors that are accessed by the reader for data transfer. These are typically gold plated.

A contact less card doesn't need physical contact with a reader. Contact less card requires only close proximity (a few inches) of a reader. Contact less technology was first developed by the British during world war 2nd as a means of identifying aircraft returning from mainland Europe. This system, the IFF (identity: friend or foe) system, was the first general use of radio frequency identification (RFID). In about 1977, contact less technology developed by the U.S. government was made available to the public sector by loss Alamos national laboratory.

Contact less smart cards offer advantages to both the organization issuing the card and the cardholder. The issuing organization can support multiple applications on a single card, consolidating an appropriate mix of technologies. Such a card transmits and receives data via radio frequency (RF) technology at distances ranging from a few millimeters to several inches – no physical contact is required. Both sides have antennae that are used for communication. The antenna is typically three to five turns of very thin wire connected to the chip. You have to place the card about 2”-3” from the reader for data access. Here, the card doesn't need an additional power source for data transfer.

Two additional categories, derived from the contact and contact less cards, are Combi cards and Hybrid cards. A Hybrid card has two chips, each with its respective contact and contactless interface. The combi card (Dual –interface card) is an emerging technology, which has a single chip with a contact and contact less interface.After using paper tickets, then magnetic technology, the 3rd generation widely developed now a day is based on smart cards using contact less technology.

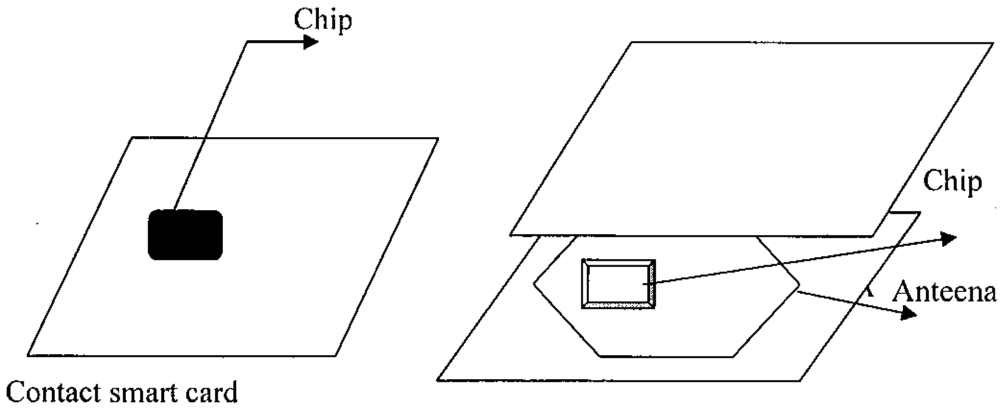


Fig 2.4: Contact & Contact less Smart Card

2.2.3 Advantages of Contactless Technology

Contact cards have certain limitations: with age, these contacts get worn out. Electrostatic discharges, due to improper contact may damage the circuits. Cardholders some times pull out the cards from the reader before the transaction is completed, leading to what is known as card tearing. Rough handling and stresses during card insertion lead to damage of the card.

Contact less technology brings many benefits to secure ID systems when factors such as high throughput and usage, harsh environments, and reader maintenance and reliability are important. Because the contact less card chip and the reader communicate using infrared waves, there is no need to physically make an electrical connection. Maintenance of reader is minimized while reliability is improved since there are no worn contacts to be replaced or openings to be unblocked. Cards also last longer because removing them from their regular carrying place is not necessary for use.

The key benefits of using contact less smart card technology for physical access are summarized below.

- High speed of access and high throughput
- Useable in harsh or dirty environments
- User friendly
    - Less intrusive
    - Does not require insertion of the card into the reader
    - No issues with orientation of the card
    - May be kept in wallet or purse for personal security during use

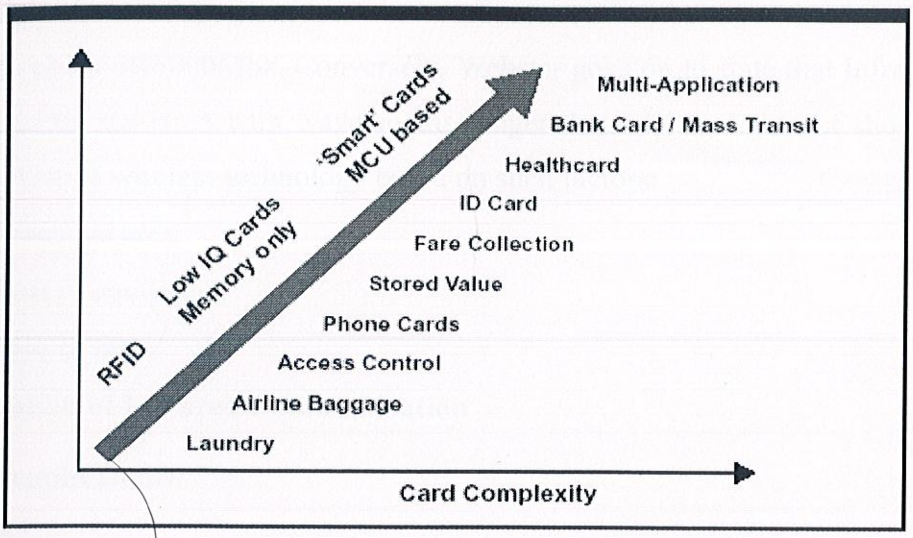


Fig 2.5: Contact less Technology Evolution

2.2.4 Drawbacks of Radio Frequency Identification

For all the applications of RFID, no standardization has been done as of now. All major RFID vendors offer proprietary systems not compatible with each other. Another drawback is the cost. RFID Readers and tags are fairly expensive. There is also the collision of signal from one reader with signal of another reader which is called Reader collision. Like Reader collision, there can also be Tag collision in which more than one tag reflects back the signal of the reader at the same time, confusing the reader .

2.2.5 Wireless Communication

The emergence of portable information terminals in work and living environments is accelerating the introduction of wireless digital links and local-area networks (LANs). Portable terminals should have access to all of the services that are available on high-speed wired networks. Unlike their wired counterparts, portable devices are subject to severe limitations on power consumption, size and weight. The desire for inexpensive, high-speed links satisfying these requirements has motivated recent interest in infrared wireless communication.

Wireless data communication may be through infrared, radio frequency or Bluetooth technology. Webster's Unabridged Dictionary tells us that Radio Frequency (RF) is a frequency in the range within which radio waves may be transmitted, from about 3 kilohertz to about 300,000Mhz, Conversely, Webster goes on to state that Infrared (IR) is electromagnetic radiation with wavelengths longer than visible light but shorter than radio waves. Use of wireless technology based on such factors:

- Coverage area
- Cost of equipment
- Ease of use

Characterization of Infrared Communication

(A) By the Applications

1. The primary commercial applications are as follows:
2. Short-term cable-less connectivity for information exchange (business cards, schedules, file sharing) between two users. The primary example is IrDA systems.
3. Wireless local area networks (WLANs) provide network connectivity inside buildings. The primary example is the IEEE802.11 standard.
4. Building-to building connections for high-speed network access or metropolitan- or campus-area networks.
5. Wireless input and control devices, such as wireless mice, remote controls, wireless game controllers, and remote electronic keys.

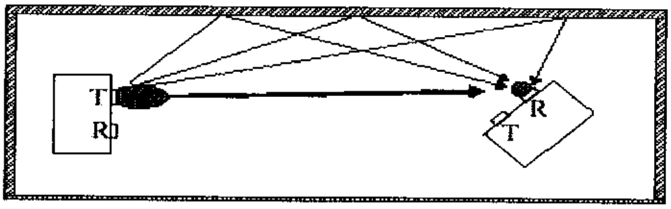


Fig 2.6: A Typical Wireless Infrared Communication System

(B) By the Link Type

Another important way to characterize a wireless infrared communication system is by the "link type", which means the typical or required arrangement of receiver and transmitter.fig.depicts the two most common configurations: the point –to-point system and the diffuse system.

In point to point system, the transmitter and receiver must be pointed at each other to establish a link. The line of sight (LOS) path from the transmitter to the receiver must be clear of obstructions, and most of the transmitted light is directed toward the receiver. The link can be created for a data exchange session between two users.

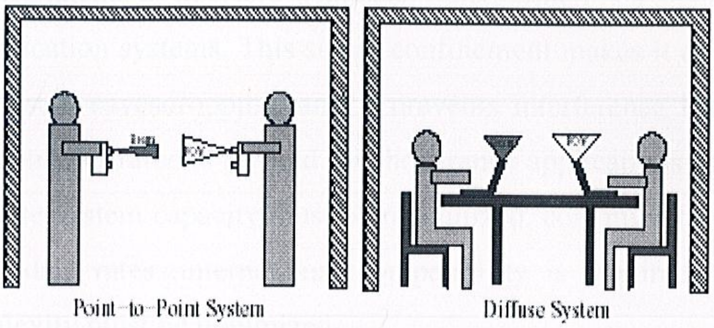


Fig 2.7: Common Types of Infrared Communication Systems

In diffuse systems, the link is always maintained between any transmitter and any receiver in the same vicinity by reflecting or "bouncing" the transmitted information-bearing light off reflecting surfaces such as ceilings, walls, and furniture. These systems are well suited to the wireless LAN application [28].

2.2.5.1 Radio Frequency

Radio frequency is used for broadcast in large spaces (outside). On multiple channels, RF is best. RF receivers consume more electrical power than IR .It provides strong and reliable signal, which is able to pass through walls and opaque objects. It even works well in the open air.

2.2.6 Comparison to Radio

Wireless infrared communication systems enjoy significant advantages over radio systems in certain environments.first, there is abundance unregulated optical spectrum available. This advantage is shrinking somewhat as the spectrum available for licensed and unlicensed radio systems increase due to modernization of spectrum allocation policies.

Radio systems must make great efforts to overcome or avoid the effects of multipath fading, typically through the use of diversity. Infrared systems do not suffer from time-varying fades due to the inherent diversity in the receiver. This simplifies design and increases operational reliability.

Infrared system provides a natural resistance to eavesdropping, as the signals are confined within the walls of the room. This also reduces the potential for neighboring wireless communication systems to interfere with each other, which is a significant issue for radio-based communication systems. This signal confinement makes it easy to secure transmissions against casual eavesdropping, and it prevents interference between links operating in different rooms. Infrared is favored for short-range applications in which per-link bit rate and aggregate system capacity must be maximized, cost must be minimized, light weight, moderate data rates ,international compatibility is required, or receiver signal-processing complexity must be minimized.

Comparison of Infrared and Other Wireless Technology

	Infrared	**Other Wireless Technology**
Typical range	Short range wireless point-n-shoot data exchange and network access	Long range wireless data exchange and network access
Interference	None	Other RF devices, building material, equipment
Security	Very secure due to short range and line of sight.	Less secure
Power consumption	Low	High
Real-time network access application	Requires user to walk up to an access point.	User does not have to be near an access point.
Range	1 meter	10 meter,1oo meter
Line of sight	Yes	No
Component cost	Low	High
Ckt design	Simple	Complicated
Portability	portable	No

Table 2.2: Comparison of Wireless Technologies

CHAPTER 3

HARDWARE DESCRIPTION

3.1 Block Diagram of System

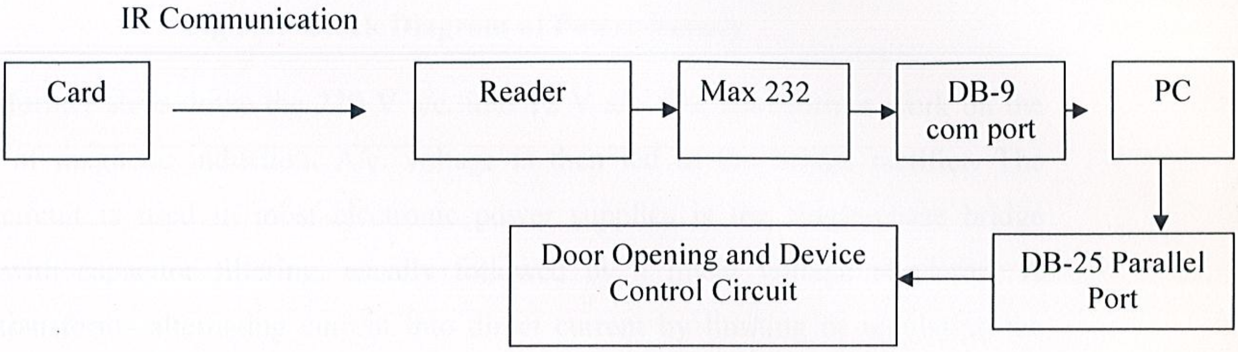


Fig 3.1: System Block Diagram

Basic components used for designing of "IR Based Secure Electronic Access System Using Microcontroller" are:

- Power supply source
- Microcontroller (8051)
- Max 232
- Infrared emitting diode
- Infrared photodiode
- Optocoupler (MCT-2E)
- Electromagnetic relay (SPDT)

3.2 Power Supply Description

The power supply circuit comprises of four basic parts –

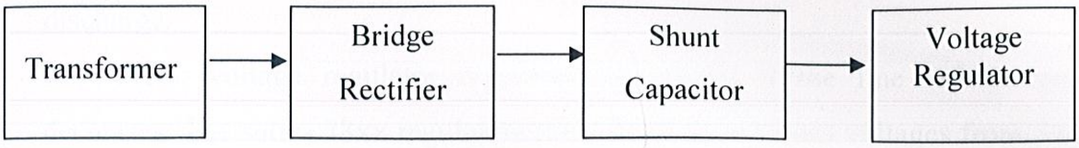


Fig 3.2: Block Diagram of Power Supply

The transformer steps down the 220 V a/c. into 12 V a/c. The transformer work on the principle of magnetic induction, A/c. voltage is then fed to the bridge rectifier. The rectifier circuit is used in most electronic power supplies is the single-phase bridge rectifier with capacitor filtering, usually followed by a linear voltage regulator.. A rectifier transforms alternating current into direct current by limiting or regulating the direction of flow of current. The output resulting from a rectifier is a pulsating D.C. voltage. This voltage is not appropriate for the components that are going to work through it.

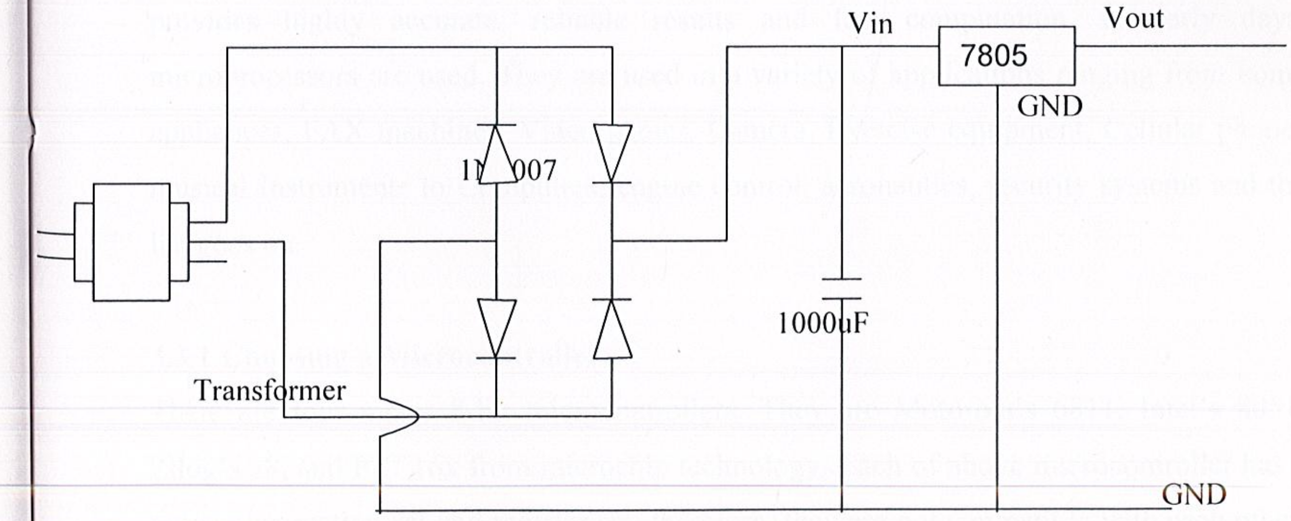


Fig 3.3 Schematic for Power Supply

The ripple of the D.C. voltage is smoothened using a filter capacitor of 1000 microF 25V. A filter capacitor is connected at the rectifier output and the d.c voltage is obtained across the capacitor. The capacitor must charge up fast, preferably with no discharge.

The voltage regulator regulates the supply if the line voltage increases or decreases. The series 78xx regulators provide fixed regulated voltages from 5 to 24 volts. An unregulated input voltage is applied at the IC Input pin i.e. pin 1 which is filtered by capacitor. The out terminal of the IC i.e. pin 2 provides a regular output. The third terminal is connected to ground.

These voltage regulators are integrated circuits designed as fixed voltage regulators for a wide variety of applications. These regulators employ current limiting, thermal shutdown and safe area compensation

3.3 Microcontroller

In our day-to-day life the role of micro-controllers has been immense. The Microcontroller has significant impact on the design of control instruments. More computing power and memory are being squeezed into fewer IC'S, to make system low cost, light weight, portable, Microcontroller are used in the system. Microcontroller provides highly accurate, reliable results and fast computation. In early days, microprocessors are used. They are used in a variety of applications ranging from home appliances, FAX machines, Video games, Camera, Exercise equipment, Cellular phones musical Instruments to Computers, engine control, aeronautics, security systems and the list goes on.

3.3.1 Choosing a Microcontroller

There are four major 8-bit microcontrollers. They are Motorola's 6811, Intel's 8051, Zilog's z8, and PIC 16x from microchip technology. Each of above microcontroller has a unique instruction set and register set; therefore, they are not compatible with each other. Two criteria in choosing microcontrollers are as:

1. Meeting the computing needs of the task at hand efficiently and cost effectively.
2. Availability of software development tools such as compilers, assemblers, and debuggers.

Following are the criteria for selecting a microcontroller:

1. The first and the foremost criteria in choosing a microcontroller is that it must meet the task at hand effectively. Among other considerations in this category are:
   - Speed-It should be highest one that the microcontroller supports.
   - Packaging-Check whether comes in 40 pin dual in line package or quad flat package or some other packing format. This is important in terms of space assembling technique and prototyping the end product.
   - Power consumption- This is especially critical for battery powered products.
   - The amount of RAM and ROM available on the chip.
   - The number of I/O pins and the timers available on the chip.

2. The second criterion in choosing a microcontroller is how easy it is in developing products around it. Key considerations include the availability of an assembler, debugger code efficient C language compiler, emulator, technical support and both in house and outside expertise.

S No.	**Feature**	**8051**	**8052**	**8031**
1	ROM(on chip program space in bytes)	4K	8K	0K
2	RAM(bytes)	128	256	128
3	Timers	2	3	2
4	I/O pins	32	32	32
5	Serial ports	1	1	1
6	Interrupt source	6	8	6

Table 3.1: Comparison of 8051 Family Members

3. The third criterion in choosing a microcontroller is its ready availability in needed quantities both at present and in future. For some designers this is even more important then first two criteria.

3.3.2 Microcontroller (8051)

The AT89C51 is a low power, high performance CMOS 8-bit microcontroller with 4Kbytes of Flash programmable and erasable read only memory (PEROM). The device is manufactured using Atmel's high density non volatile memory technology. This device is compatible with the industry standard 8051 instruction set and pin out. The on-chip Flash allows the program memory to be quickly reprogrammed using a nonvolatile memory programmer such as the PG302 (with the ADT87 adapter). By combining an industry standard 8-bit CPU with Flash on a monolithic chip, the 8951 is a powerful microcomputer which provides a highly flexible and cost effective solution to many embedded control applications. The 8951 provides the following features:

- 4 Kbytes of Flash
- 128 bytes of RAM
- 32 I/O lines
- two16-bit timer/counters
- five vector, two-level interrupt architecture
- full duplex serial port
- on chip oscillator and clock circuitry

In addition, the 8951 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 hardware reset.

3.3.3 89C51 Architecture

Eight bit CPU registers A and B, Sixteen-bit PC and DPTR, Eight-bit program status word register, Eight-bit stack pointer, Internal ROM of 4k, Internal RAM of 128 bytes, Thirty-two input/output pins arranged as four eight bit ports, Two sixteen bit timer/counter: T0 – T1, Full duplex serial data receiver/transmitter: SBUF, Control registers: TCON, TMOD, SCON, PCON, IP, and IE, Two external and three internal interrupt sources, Oscillator and clock circuits.

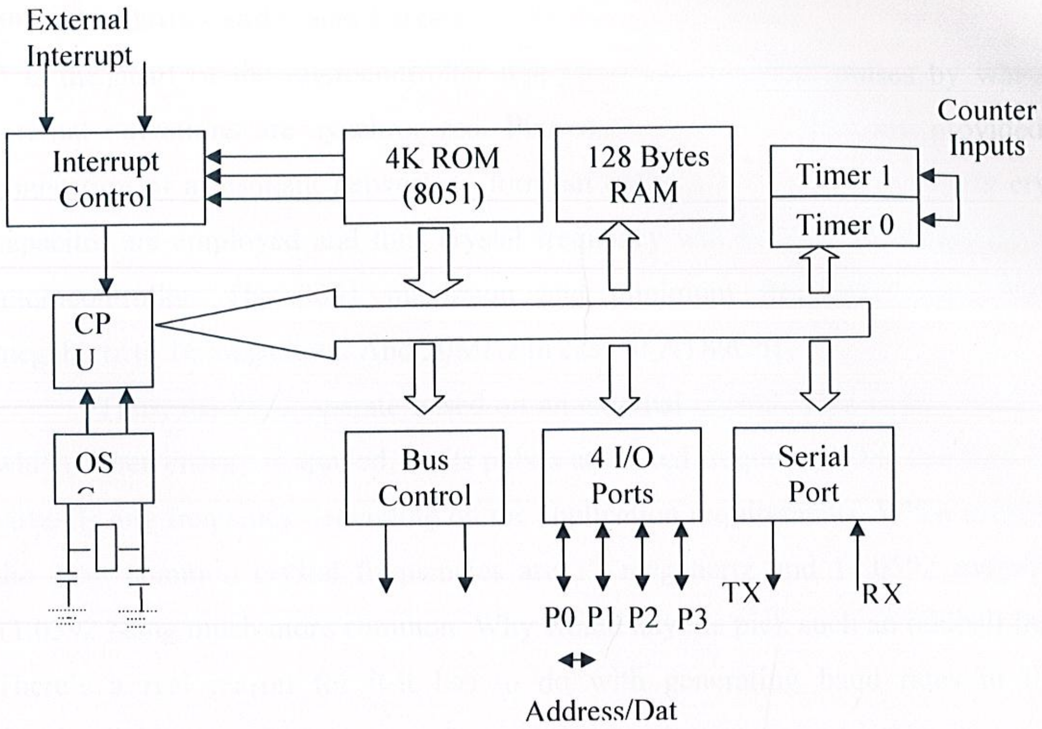


Fig 3.4: 8051 Microcontroller Block Diagram

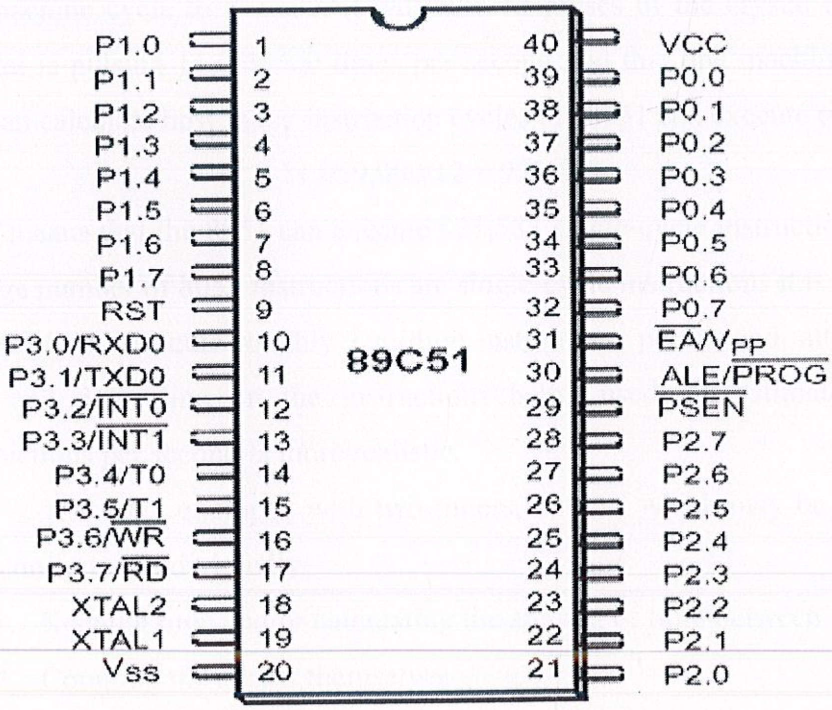


Fig 3.5: 8051 Pin Diagram

8051 Oscillators and Clock Circuit

It is the heart of the microcontroller that generates the clock pulses by which all the internal operations are synchronized. Pins XTAL1 and XTAL2 are provided for the connection of a resonant network to form an oscillator. Typically, a quartz crystal and capacitor are employed and thus crystal frequency will become the clock frequency of microcontroller. The 8051 maximum and minimum frequency range between 1 megahertz to 16 megahertz. And 20MHz in case of AT89C51.

Thus, the 8051 operate based on an external crystal. This is an electrical device which, when energy is applied, emits pulses at a fixed frequency. One can find crystals of virtually any frequency depending on the application requirements. When using on 8051, the most common crystal frequencies are 12 megahertz and 11.0592 megahertz-with 11.0592 being much more common. Why would anyone pick such an oddball frequency? There's a real reason for it-it has to do with generating baud rates in the Serial Communication.

A cycle is, in reality, 12 pulses of the crystal. That is to say, if an instruction takes on machine cycle to execute, it will take 12 pulses of the crystal to execute. Since the crystal is pulsing 11,059,000 times per second and that one machine cycle is 12 pulses, we can calculate how many instruction cycles the 8051 can execute per second:

$$11{,}059{,}000/12 = 921{,}583$$

This means that the 8051 can execute 921,583 single-cycle instructions per second. Since a large number of 8051 instructions are single-cycle instructions it is often considered that the 8051 can execute roughly 1 million instructions per second, although in reality it is less and depending on the instructions being used, an estimate of about 600,000 instructions per second is more realistic.

The 8051 equipped with two timers, both of which may be controlled, set, read, and configured individually.

1. Keeping time and/or calculating the amount of time between events
2. Counting the events themselves
3. Generating baud rates for the serial port

Input/Output Pins and Ports

One of the major features of a microcontroller is the versatility built into the input/output circuits that connect the 8051 to the outside world. The microprocessor designs add the additional chips to the interface with the external circuitry, but this ability is built into the microcontroller.

Given this pin flexibility the 8051 may be applied simply as a single component with the I/O only or it may be expanded to include the additional memory, parallel ports and serial data communication by using the alternate pin assignments.

P0 (Port 0, Bit-Addressable)

This is input/output port 0. Each bit of this SFR corresponds to one of the pins on the microcontroller. For example, bit 0 of port 0 is pin P0. 0, bit 7 is pin P0. 7. Writing a value of 1 to a bit of this SFR will send a high level on the corresponding I/O pin whereas a value of 0 will bring it to a low level.

Port 0 pins may serve as inputs, outputs, or when used together as a bidirectional low order address and data bus for the external memory.

P1 (Port 1, Bit-Addressable)

Port 1 pins have no dual functions. Therefore, it can just be either used as input or output.

P2 (Port 2, Bit-Addressable)

This is input/output port 2. Each bi of this SFR corresponds to one of the pins on he microcontroller. For example, bit 0 of port 2 is pin P2.0, bit 7 is pin P2.7. Writing a value of 1 to bit of this SFR will send a high level on the corresponding I/O pin whereas a value of 0 will bring it to a low level.

It has functions similar to the port 1. The alternate use of port 2 is to supply a high order address byte in conjunction with the port 0 low order byte to address external memory. Port 2 pins are momentarily changed by the address control signals when supplying the high order byte of 16-bit address.

P3 (Port 3, Bit-Addressable)

This is input/output port 3. Each bit of this SFR corresponds to on of the pins on the microcontroller. For example, bit0 of port 3 is pin P3.0, bit 7 is pin P3.7. Writing a value of 1 to a bit of this SFR will send a high level on the corresponding I/O pin whereas a value of 0 will bring to a low level. Thus the input/ output functions can be programmed under the control of various other special function registers.

Memory Organization

There are two types of memory in microprocessor devices.

- Program Memory
- Data Memory

Each memory type has different addressing mechanism, different control signals and different function. The Program Memory (ROM or EPROM) is extremely large, read only and non-volatile. This has a 16-bit address bus, whose elements are accessed by program counter or instructions that generates 16-bit address.

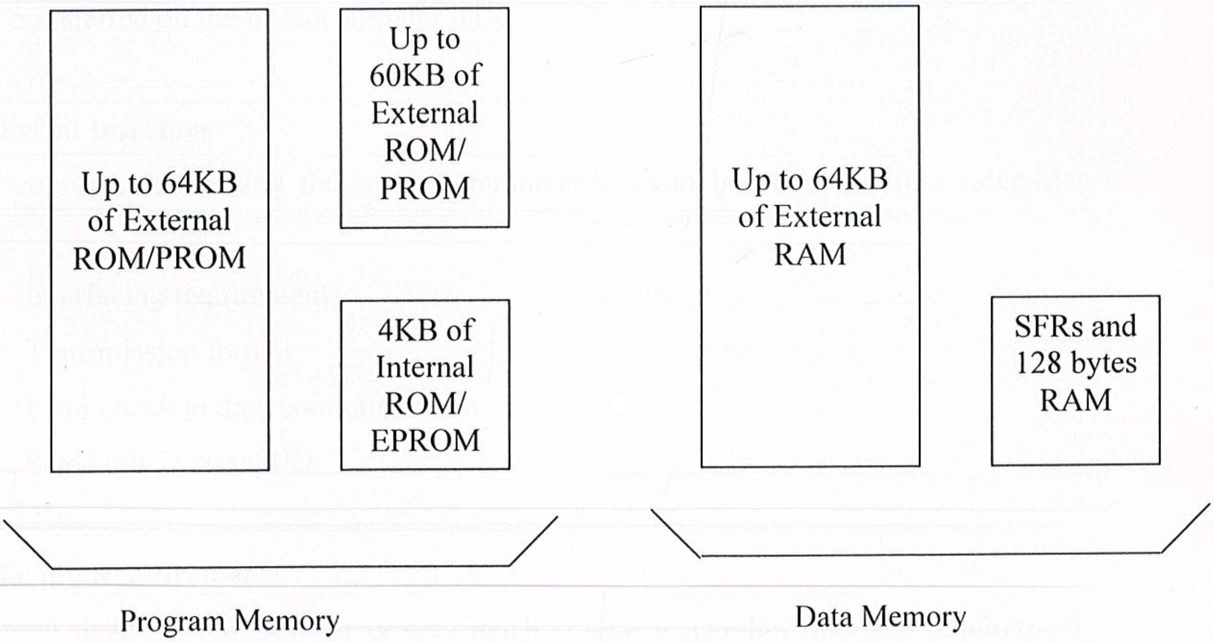

Up to 64KB of External ROM/PROM
Up to 60KB of External ROM/ PROM
4KB of Internal ROM/ EPROM
Up to 64KB of External RAM
SFRs and 128 bytes RAM
Program Memory
Data Memory

Fig 3.6: Memory Mapping

EEPROM (Electrically Erasable Programmable Rom)

EEPROM has several advantages over EPROM, such as the fact that its method of erasure is electrical and therefore instant, as opposed to the 20-minute erasure time required for UV-EPROM. In addition, in EEPROM one can select which byte to be erased, in contrast to UV-EPROM, in which the entire contents of ROM are erased. however, the main advantage of EEPROM is the fact that one can program and erased its contents while it is still in the system board. It does not require physical removal of the memory chip from its socket. In other words, unlike UV-EPROM, EEPROM does not require an external erasure and programming device [31].

3.4 Data Communication Concepts

Within a microcomputer data is transferred in parallel, because that is the fastest way to do it. For transferring data over long distances, however, parallel data transmission requires too many wires. Therefore, data to be sent long distances is usually converted from parallel form to serial form so that it can be sent on a single wire or pair of wires. Serial data received from a distant source is converted to parallel form so that it can be easily transferred on the microcomputer buses.

3.4.1 Serial Interface

Basic concepts concerning the serial communication can be classified into categories below:

- Interfacing requirements
- Transmission format
- Error check in data communication
- Standards in serial I/O

Interfacing Requirements

The serial interface requirement is very much similar to parallel interface requirement. Computer identifies the peripheral through port address and enable if using the read and write signals. The primary difference between the parallel I/O and serial I/O is the number of lines used for data transfer. Parallel I/O requires the entire bus while the serial I/O requires only one or pair of data lines for communication.

Transmission Format

Transmission format for communication is concerned with the issues such as synchronization, direction of data flow, speed, errors and medium of transmission. Serial data can be sent synchronously or asynchronously.

Serial Transmission Methods

Serial Communication, like any data transfer, requires coordination between the sender and receiver. For example, when to start the transmission and when to end it, when one particular bit or byte ends and another begins, when the receiver's capacity has been exceeded, and so on. A protocol defines the specific methods of coordinating transmission between a sender and receiver.

Two serial transmission methods are used that correct serial bit errors. The first one is synchronous communication, the sending and receiving ends of the communication are synchronized using a clock that precisely times the period separating each bit. By checking the clock the receiving end can determine if a bit is missing or if an extra bit (usually electrically induced) has been introduced in the stream. Here is an example of this method of communication, lets say that on a conveyor belt a product is passing through a sensing device every 5 seconds, if the sensing device senses something in between the 5 second lap it assumes that whatever is passing is a foreign object of some sorts and sounds an alarm, if on the 5 second lap nothing goes by it assumes that the product is missing and sounds an alarm. One important aspect of this method is that if either end of the communication loses its clock signal, the communication is terminated.

The alternative method (used in PCs) is to add markers within the bit stream to help track each data bit. By introducing a start bit which indicates the start of a short data stream, the position of each bit can be determined by timing the bits at regular intervals, by sending start bits in front of each 8 bit streams, the two systems don't have to be synchronized by a clock signal, the only important issue is that both systems must be set at the same port speed. When the receiving end of the communication receives the start bit it starts a short term timer. By keeping streams short, there's not enough time for the timer to get out of sync. This method is known as asynchronous communication because the sending and receiving end of the communication are not precisely synchronized by the means of a signal line.Each stream of bits are broke up in 5 to 8 bits called words. Usually in the PC environment you will find 7 or 8 bit words, the first is to accommodate all upper and lower case text characters in ASCII codes (the 127characters) the latter one is used to exactly correspond to one byte.

This is often referred to as a data frame. Five different parity bits can be used, the mark parity bit is always set at a logical 1, the space parity bit is always set at a logical 0, the even parity bit is set to logical 1 by counting the number of bits in the word and determining if the result is even, in the odd parity bit, the parity bit is set to logical 1 if the result is odd. The later two methods offer a means of detecting bit level transmission errors. Note that you don't have to use parity bits, thus eliminating 1 bit in each frame, this is often referred to as non parity bit frame.

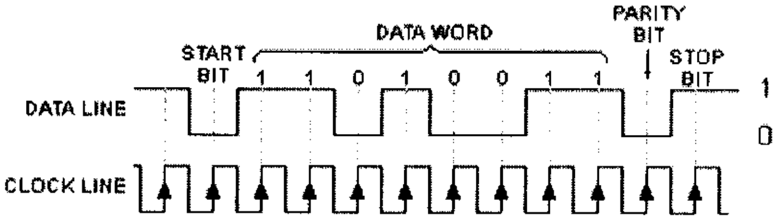


Fig 3.7: Asynchronous Serial Data Frame (8E1)

In the example above you can see how the data frame is composed of and synchronized with the clock signal. This example uses an 8 bit word with even parity and 1 stop bit also referred to as an 8E1 setting.

Bit Rates

Another important part of every asynchronous serial signal is the bit rate at which the data is transmitted. The rates at which the data is sent is based on the minimum speed of 300 bps (bits per second), you may find some slower speeds of 50, 100 and 150 bps, but these are not used in today's technologies. Faster speeds are all based on the 300 bps rate, you merely double the preceding rate, so the rates are as follows, 600, 1200, 2400, 4800, 9600, 19200 and 38400 which is the fastest speed supported by today's BIOS's.

3.5 MAX 232 (Communication Interface)

RS-232 was created for one purpose, to interface between Data Terminal Equipment (DTE) and Data Communications Equipment (DCE) employing serial binary data interchange. So as stated the DTE is the terminal or computer and the DCE is the modem or other communications device. RS 232 is the most widely used serial I/O interfacing standard. In RS 232, a 1 is represented by -3 to -25 v. while a 0 bit is +3 to + 25 v, making -3 to +3 undefined. For this reason, to connect any RS 232 to a microcontroller system we must use voltage converters such as MAX 232 to convert the TTL logic levels to the RS 232 voltage level, and vice versa.

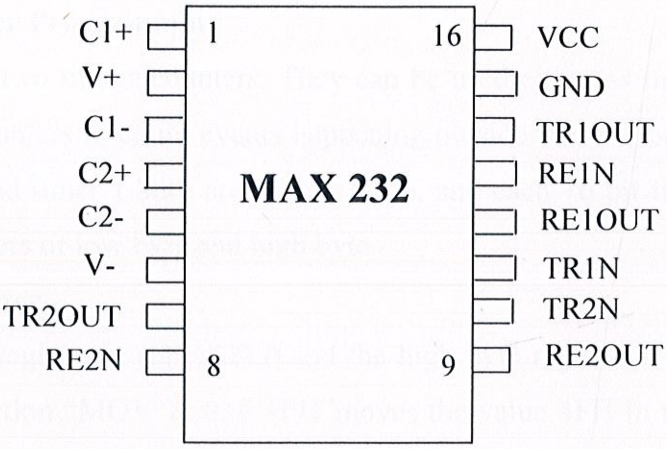


Fig 3.8: MAX 232 Pin Diagram

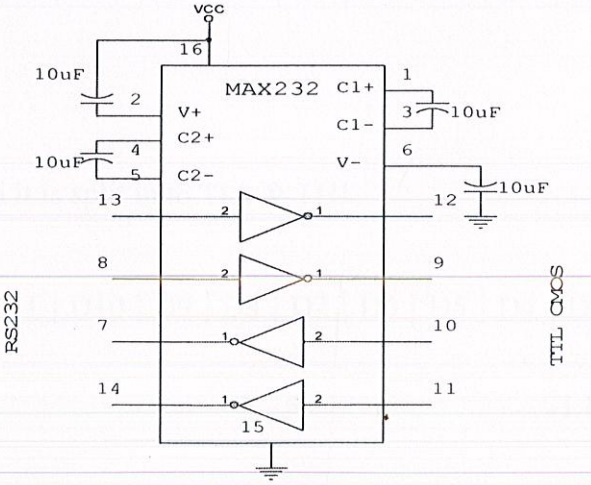


Fig 3.9: Operating Circuit of MAX 232

3.6 8051 Serial Communication Programming

Baud Rate in The 8051

The 8051 transfers and receives data serially at many different baud rates. The baud rate in the 8051 is programmable. This is done with the help of timer 1

Frequency of XTAL = 11.0592 MHZ

Machine cycle frequency =11.0592/12=921.6 KHZ.

The 8051's serial communication UART circuitry divides the machine cycle frequency of 921.6 kHz by 32 once more before it is used by timer1 to set the baud rate .result is 28,800 HZ. This value is used to find the timer 1 value to set the bad rate. When timer 1 is used to set the baud rate it must be programmed in mode 2, that is 8 bit, auto-reload.

Counter/Timer Programming

The 8051 has two timers/counters. They can be used either as timers to generate a time delay or as counters to count events happening outside the microcontroller. These timers are, timer 0 and timer 1.both are 16 bits wide, and each 16 bit timer is accessed as two separate registers of low byte and high byte.

Timer 0 Register

The low byte register is called TL0 and the high byte register is referred to as TH0.For ex., the instruction "MOV TL0, # 4FH"moves the value 4FH in to TL0, the low byte of timer 0.

D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0

Timer 1 Register

Timer 1 is also 16 bits, and it is split in to TL1 & TH1.

D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0

← TH1 → ← TL1 →

TMOD (Timer Mode) Register (20h)

Both timers 0 & 1 use the same register, called TMOD,to set the various timer operation modes.TMOD is an 8-bit register in which the lower 4 bits are set aside for timer 0 and the upper 4 bits are set aside for timer 1. In each case, the lower 2 bits are used to set the timer mode and upper 2 bits to specify the operation [31].

(MSB) (LSB)

GATE	C/T	M1	M0	GATE	C/T	M1	M0

← .Timer 1 → ← Timer 0 →

				Mode	Operating Mode
M1	Mode bit 1	1	2		8-bit auto reload
M0	Mode bit 0	0			

C/T = 0 for Timer
= 1 for Counter
GATE = 0 When on/off is done by software
= 1 when additional hardware is needed for on/off.

SBUF Register

SBUF is an 8 bit register used solely for special communication in the 8051.for a byte of data to be transferred via the TxD line; it must be placed in the SBUF register. Similarly, SBUF holds the byte of data when it is received by the 8051's RxD line.SBUF can be accessed like any other register in the 8051.

SCON (Serial Control) Register (50 H)

The SCON register is an 8 bit register used to program the start bit, stop bit, and data bits of data framing, among other things. The following describes various bits of the SCON register.

SM0	SM1	SM2	REN	TB8	RB8	T1	R1

SM0	Serial port mode spécifier.
SM1	Serial port mode spécifier.
SM2	Used for multiprocessor communication.
REN	Set/cleared by software to enable/disable reception.
TB8	Not widely used.
RB8	Not widely used.
T1	Transmit interrupt flag.
R1	Receive interrupt flag.

		Mode
SM0	0	Serial mode 1, 8 bit data, 1 stop bit, 1 start bit.
SM1	1	

3.7 Optocoupler (MCT-2E)

The MCT2XXX series optoisolators consist of a gallium arsenide infrared emitting diode driving a silicon phototransistor in a 6-pin dual in-line package. There is no electrical connection between the two, just a beam of light. The light emitter is nearly always an LED. The light sensitive device may be a photodiode, phototransistor, or more esoteric devices such as thyristors, triacs etc. To carry a signal across the isolation barrier, optocouplers are operated in linear mode.

Pin Description of MCT2E

Fig shows the six-pin IC package for an optocoupler and the electronic diagram of its pin outline. The IC package may also be called an IC or a chip. It is important to note that each type of optocoupler may use different pin assignments .

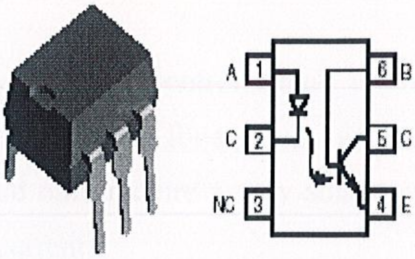


Fig 3.10: MCT-2E Pin Diagram

Pin no.	Function
1	Anode
2	Cathode
3	NC
4	Emitter
5	Collector
6	Base

Table 3.2: MCT-2E Pins

3.7.1Optocoupler Operation

Optocouplers are good devices for conveying analog information across a power supply isolation barrier, they operate over a wide temperature range and are often safety agency approved they do, however, have many unique operating considerations.

Optocouplers are current input and current output devices. The input LED is excited by changes in drive current and maintains a relatively constant forward voltage. The output is a current which is proportional to the input current. The output current can easily be converted to a voltage through a pull-up or load resistor:

Applications

- AC mains detection
- Reed relay driving
- Switch mode power supply feedback

3.8 Power Switching Devices

The switching device employed in a power control circuit is crucial to the successful operation of the circuit. The basic requirements for a power switching device are:

a. The switching device should only require a very small input current in order to control a very much larger current.

b. The switching device should operate very rapidly (i.e. the time between 'on' and 'off' states should be negligible).

c. During conduction, the switching device should be capable of continuously carrying the rated load current. It should also be capable of handling momentary surge currents.

d. There should be minimal power dissipation with in the switching device.

e. In the con- conducting state, the switching device should be capable of continuously sustaining the peak value of rated supply voltage. It should also be capable of coping with momentary surge voltages.

3.8.1 Electromagnetic Relay

A relay is simply an electrically operated on/off switch. The relay used in this hardware ckt is SPDT (single pole double throw) relay. Short circuit and other abnormal conditions often occur on a power system. The heavy current associated with short circuit is likely to cause damage to equipment if suitable protective relays and circuit breakers are not provided for the protection of each section of power system. If a fault occurs in an element of power system, an automatic protective device is needed to isolate the faulty equipment as quickly as possible to keep the healthy section of the system in normal operation.

The electromagnetic relay consists of a multi-turn coil, wound on an iron core, to form an electromagnet. When the coil is energised, by passing current through it, the core becomes temporarily magnetised. The magnetised core attracts the iron armature. The armature is pivoted which causes it to operate one or more sets of contacts. When the coil is de-energised the armature and contacts are released.

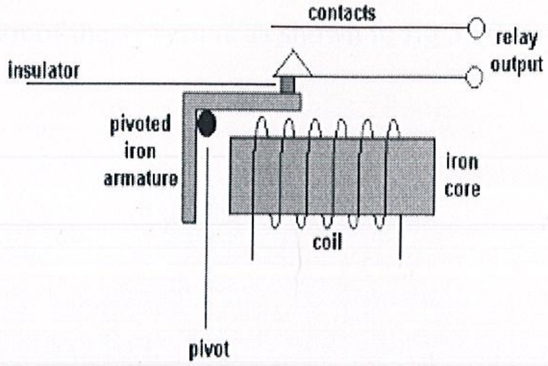


Fig 3.11: Electromagnetic Relay

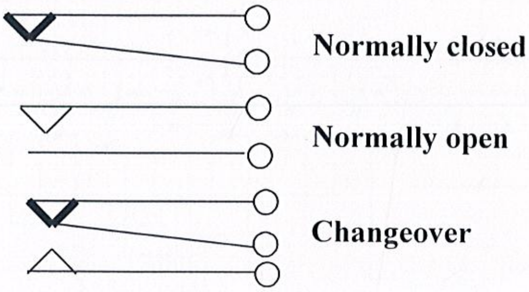


Fig 3.12: Relay Contacts

The spring sets (contacts) can be a mixture of N.O. N.C. and C.O. various coil operating voltages (ac and dc) are available. The actual contact points on the spring sets are available for high current and low current operation.

There are two different kinds of contacts:

NO normally open: The contacts are open until the coil of the relay is energised, whereupon they are closed to complete the outside circuit

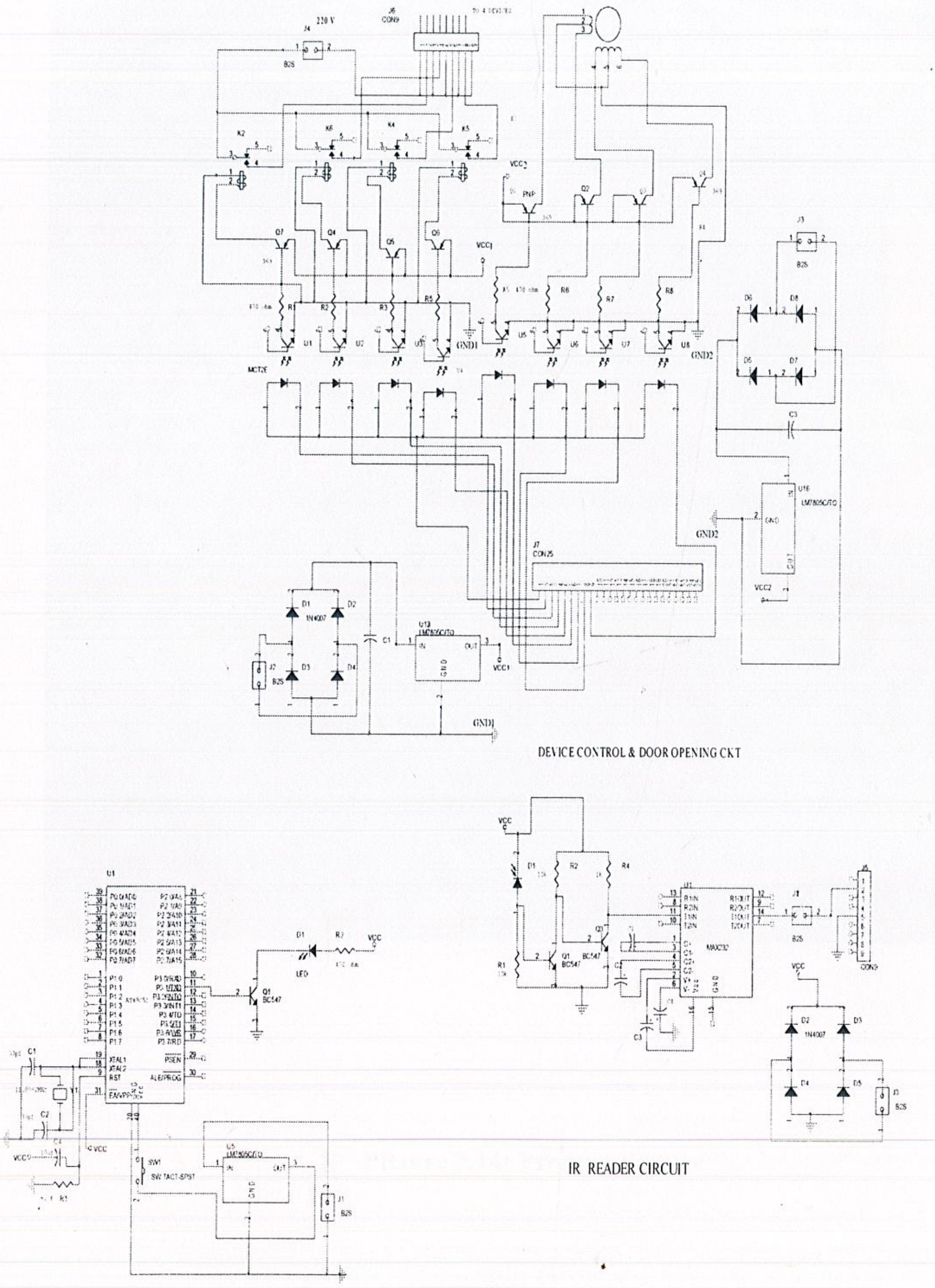
NC normally closed: The contacts are closed until the coil of the relay is energised, whereupon they are opened to break the outside circuit, switching it off.

Advantages of Relays

- Relays can switch AC and DC, transistors can only switch DC.
- Relays can switch high voltages, transistors cannot.
- Relays are a better choice for switching large currents (> 5A).

3.9 Schematic of System

The whole schematic diagram of the system is as shown in fig 3.30.



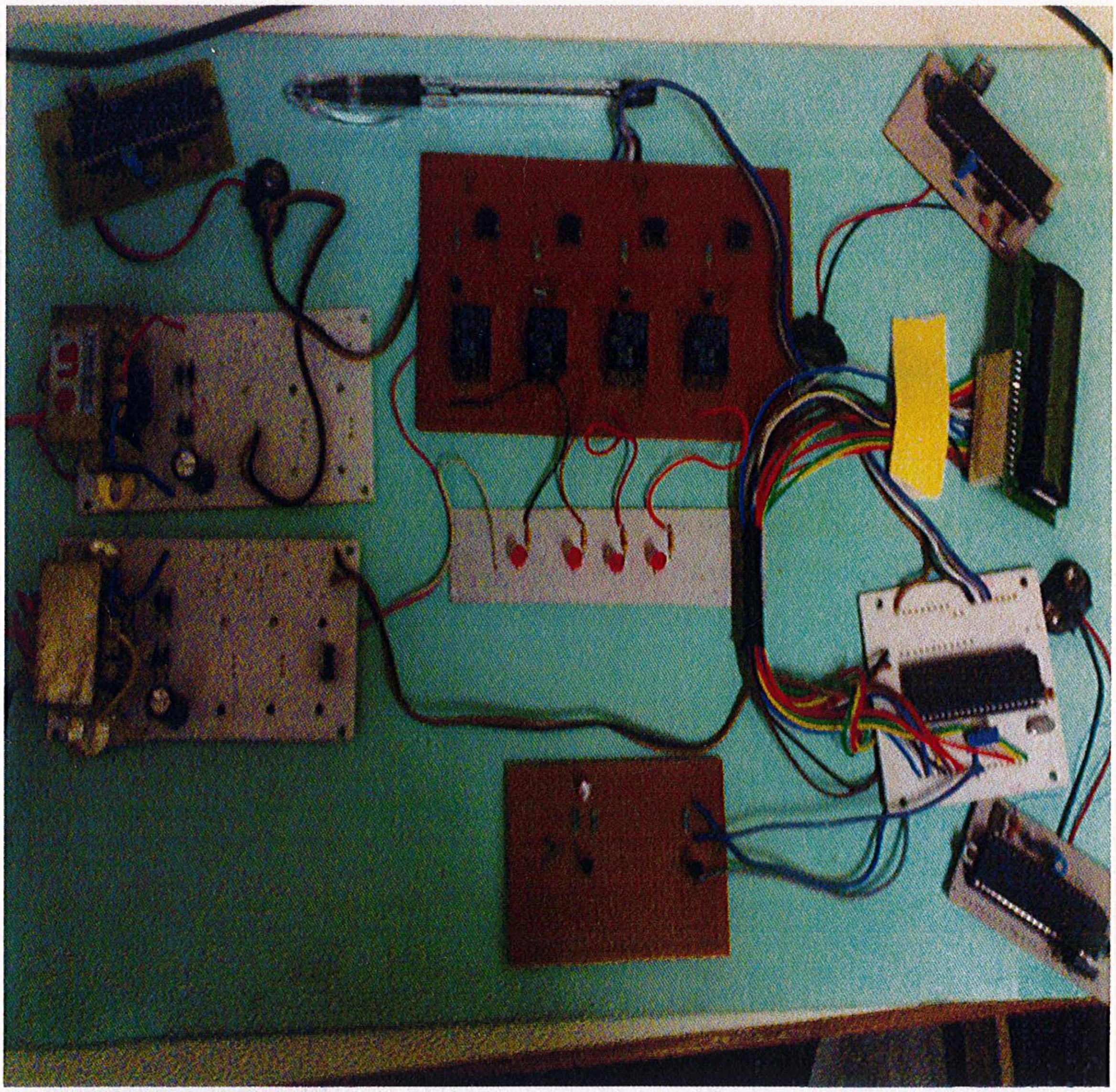
DEVICE CONTROL & DOOR OPENING CKT

IR READER CIRCUIT

IR SMART CARD

Fig 3.13: System Schematic

3.10 Picture of Product



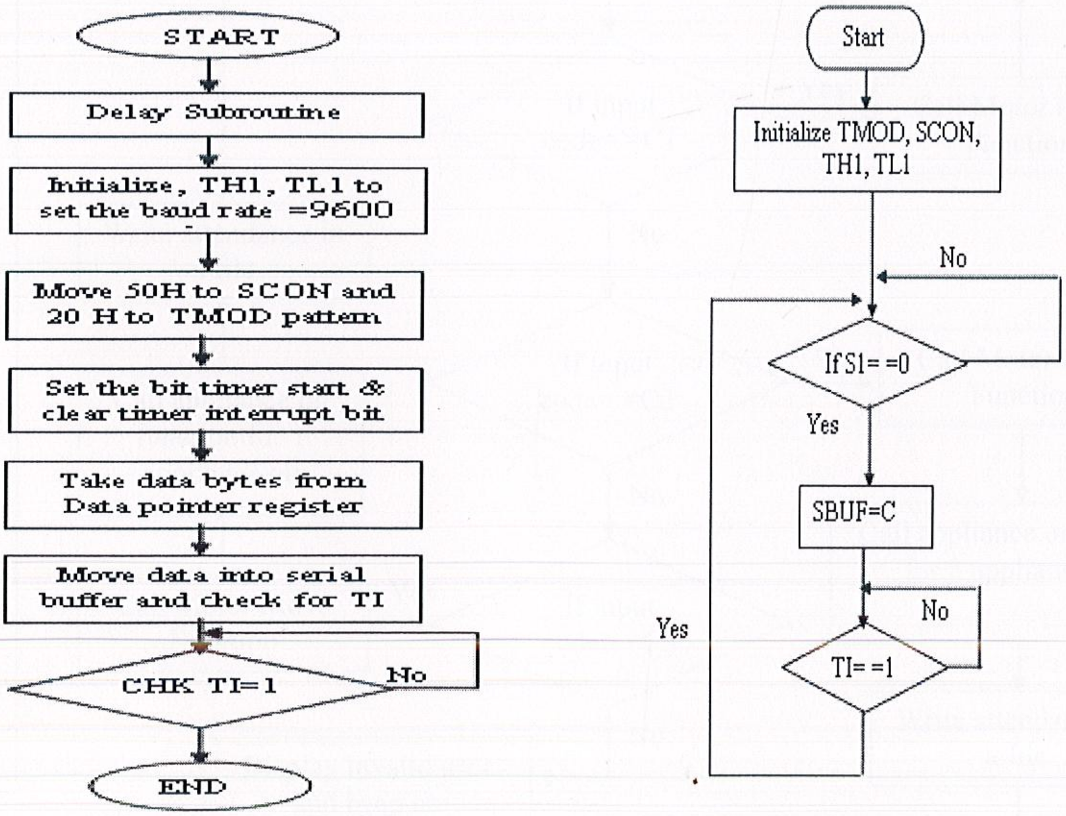
Picture 3.14: Product Picture

CHAPTER 4
SOFTWARE DESCRIPTION

4.1 Programming Structure

Encryption/decryption is often implemented as "firmware", i.e. a combination of hardware and software. The software part is the program which represents the mathematical functions needed to operate the encryption transformation.

The simulator was used for testing of program functions. To evaluate the software for correct operation the file was programmed into the microcontroller on the relevant development board. Programming of the microcontroller was achieved using MP5 software. EZ31 is an EEPROM programmer that interfaces directly with the computer serial port. This permits hexadecimal files to be loaded into the microcontroller. Initially the micro controller was programmed by removing it from the socket on the board and inserting it into the multi-pin socket on the programmer.



START
Delay Subroutine
Initialize, TH1, TL1 to set the baud rate =9600
Move 50H to SCON and 20 H to TMOD pattern
Set the bit timer start & clear timer interrupt bit
Take data bytes from Data pointer register
Move data into serial buffer and check for TI
CHK TI=1
No
END
Start
Initialize TMOD, SCON, TH1, TL1
No
If S1= =0
Yes
SBUF=C
No
Yes
TI= =1

Fig 4.1: Flow Chart for Serial Transmission & Card

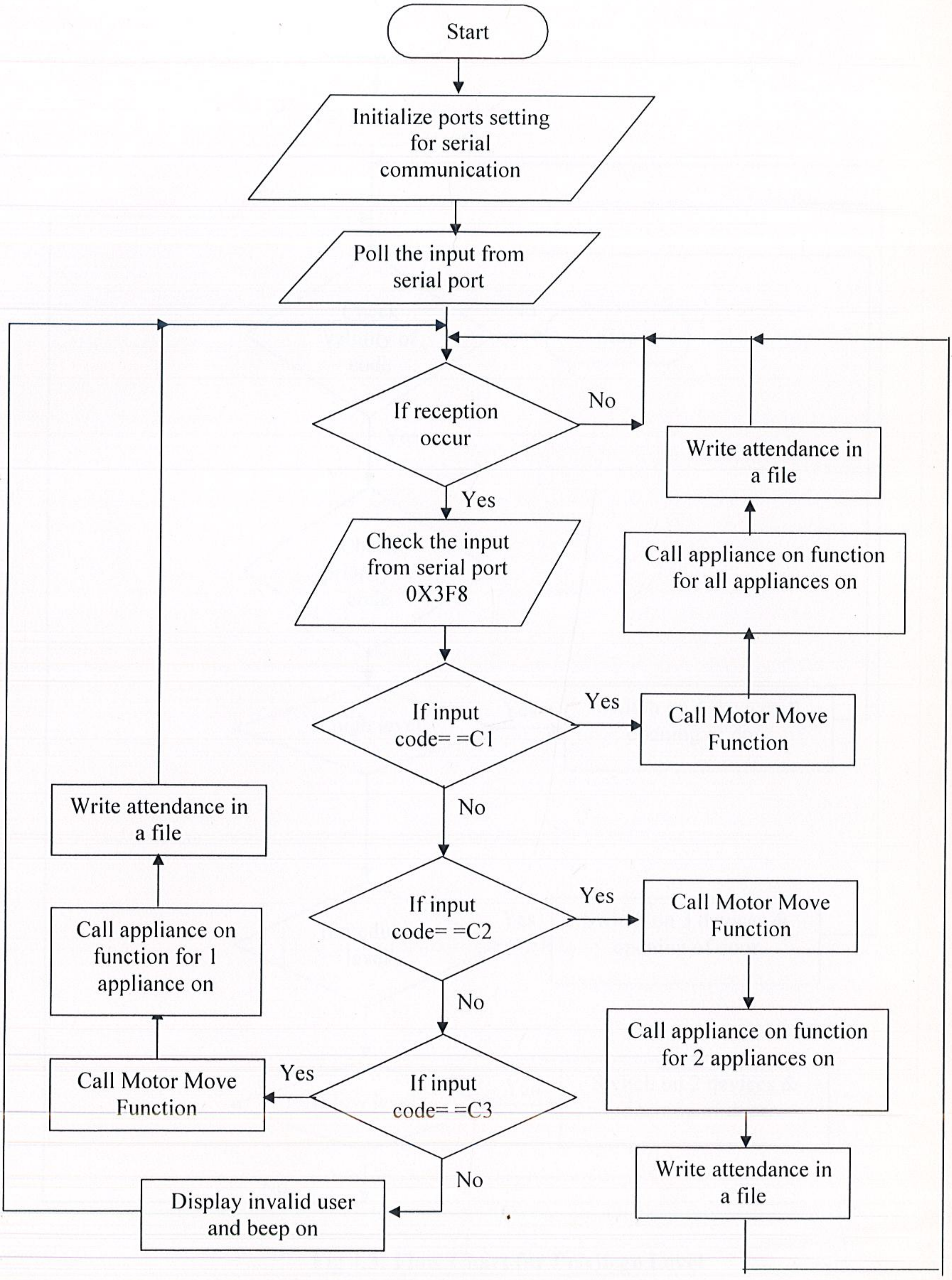

Start
Initialize ports setting for serial communication
Poll the input from serial port
If reception occur
No
Yes
Check the input from serial port 0X3F8
If input code= =C1
Yes
Call Motor Move Function
Call appliance on function for all appliances on
Write attendance in a file
No
If input code= =C2
Yes
Call Motor Move Function
Call appliance on function for 2 appliances on
Write attendance in a file
No
If input code= =C3
Yes
Call Motor Move Function
Call appliance on function for 1 appliance on
Write attendance in a file
No
Display invalid user and beep on

Fig 4.2: System Flow Chart

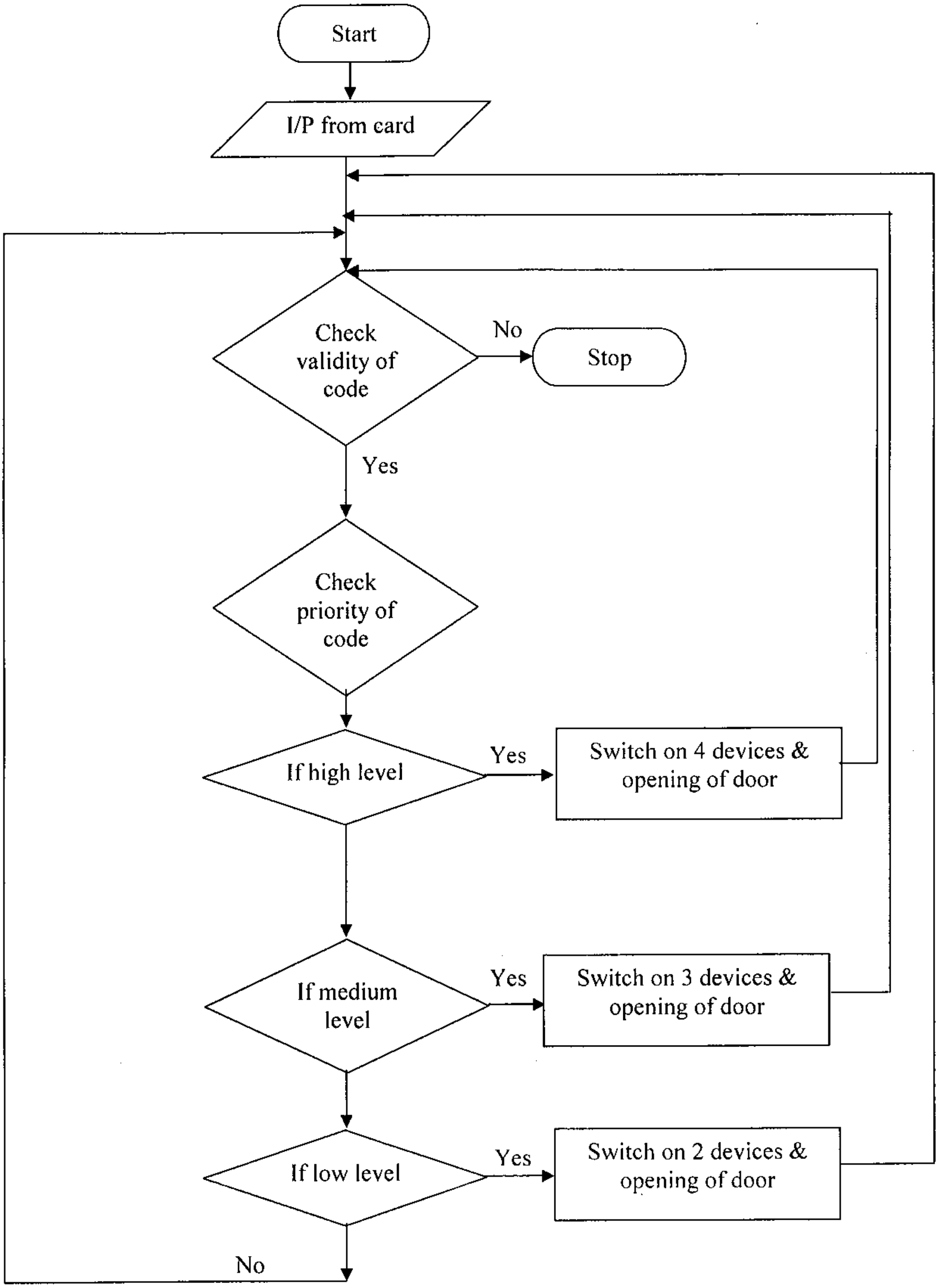
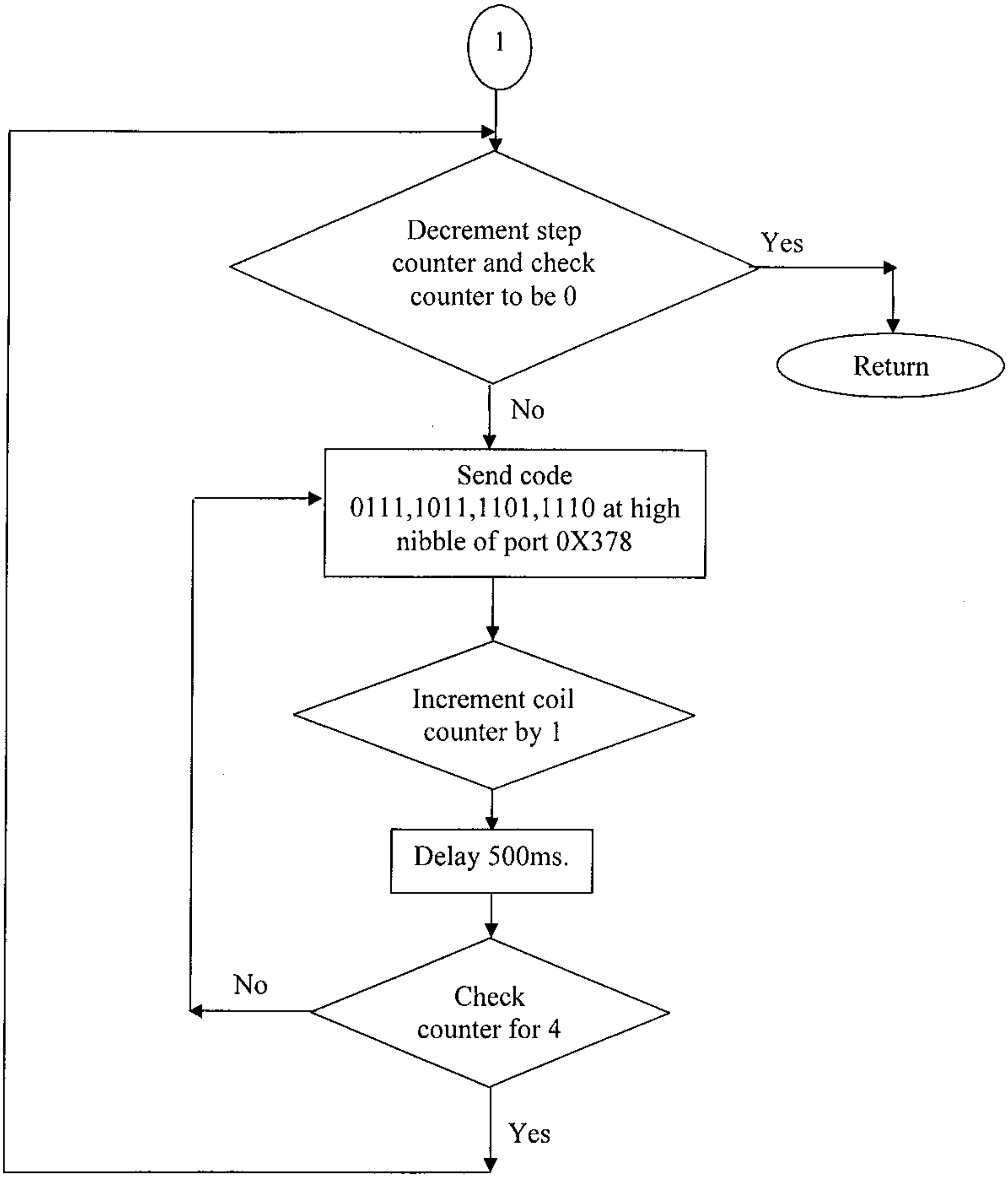


Fig 4.3: Flow Chart for Privilege Level


1
Decrement step counter and check counter to be 0
Yes
Return
No
Send code 0111,1011,1101,1110 at high nibble of port 0X378
Increment coil counter by 1
Delay 500ms.
No
Check counter for 4
Yes

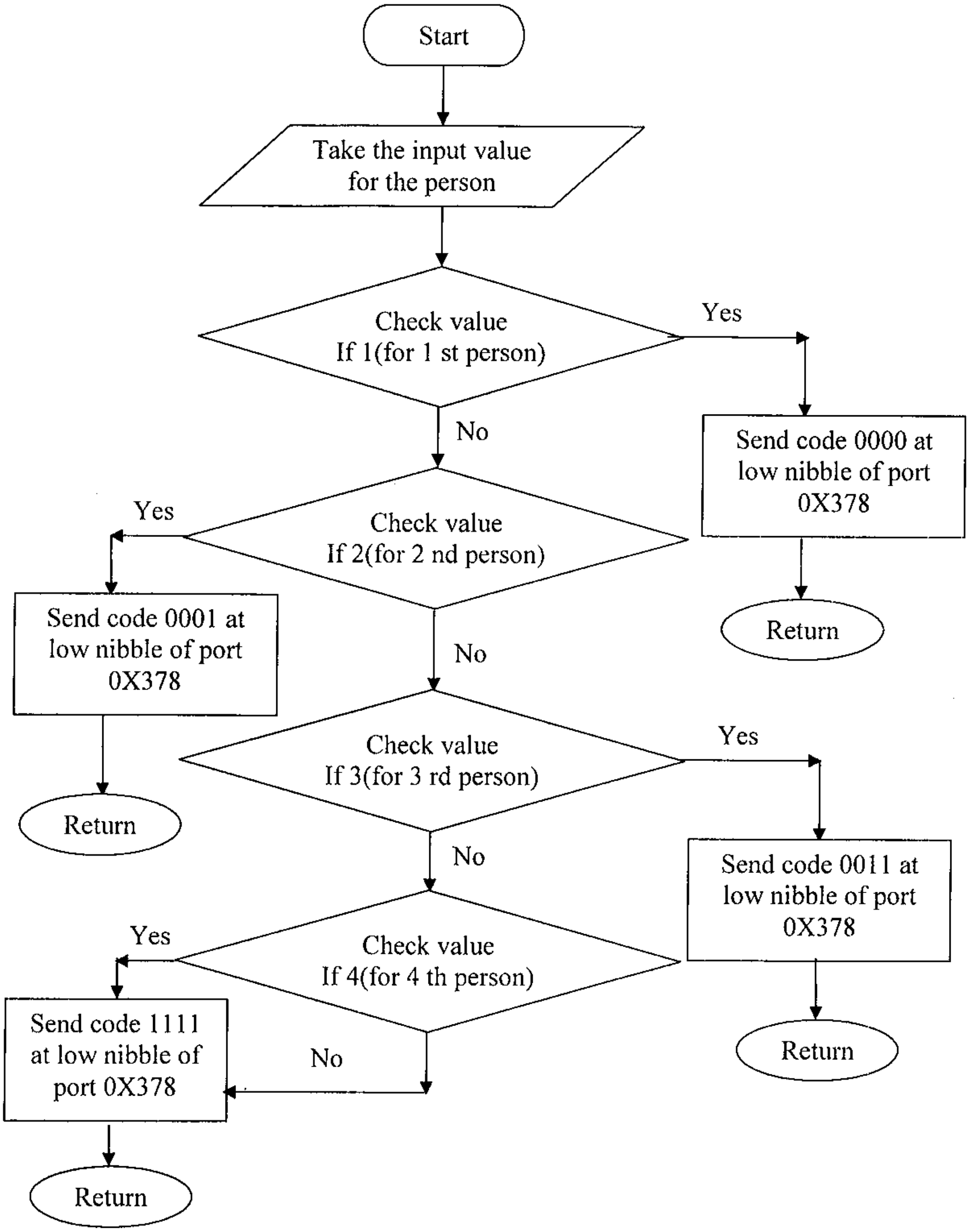

Start
Take the input value for the person
Check value If 1(for 1 st person)
Yes
Send code 0000 at low nibble of port 0X378
Return
No
Check value If 2(for 2 nd person)
Yes
Send code 0001 at low nibble of port 0X378
Return
No
Check value If 3(for 3 rd person)
Yes
Send code 0011 at low nibble of port 0X378
Return
No
Check value If 4(for 4 th person)
Yes
Send code 1111 at low nibble of port 0X378
No
Return

Fig 4.4: Flow Chart for Device Control

CHAPTER 5

RESULTS, CONCLUSION AND FUTURE SCOPE

5.1 Results

Control of the access the program is achieved by making the decryption end of the system operational for only those persons who have fulfilled certain conditions such as correct code. It is the task of the Access Control Module to achieve this by checking the program parameters versus the user's entitlements before authorizing any decryption process.

Dimensions, mechanical characteristics, and electrical interface of Smart Cards have all been specified by the International Organization for Standardization (ISO). Thanks to its processing capability, storage capacity, and security features, the Smart Card is a perfect candidate for the implementation of a Access Control Module. Thanks to its physical dimensions, a Smart Card can easily be fitted inside a cardboard package

Here total no. of cards is four. In which three cards having validity to enter in application area rest one is not valid. Testing is done to check whether the reader is responding in right way or not. On PC screen validity or no validity is displayed. Cards are C1, C2 and C3 which are placed in random manner .In which C3 is invalid.

Trial No.	Application Order	Authentication Order
1	C1, C2, C3.	Valid ,valid, not valid
2	C2, C3, C1	Valid, not valid, valid
3	C3 , C1, C2	Not valid ,valid ,valid

Table 5.1: Testing of Validity of Code

5.2 Conclusion

Smart card based personal identification cards offer significant benefits for individuals, businesses and governments. Individuals using smart identification cards enjoy greater satisfaction through quicker and more secure access to information and services. The efficiency, consolidation of program and security features provided through the use of smart identification cards enable governments and businesses to securely improve services, while reducing operating costs. And, through privacy-sensitive system designs, individual information can be protected from misuse.

Issues related to the requirements of implementing physical secure system could be identified. These are the principal way of selection - proximity or pointing; information transfer characteristics - unidirectional vs. bidirectional, data rate; information storage and processing capacity; manufacturing costs and power economy. Furthermore, conformity existing infra structure is of importance.

While the investment for an access control system may be higher than traditional locks and keys, it provides you with far more security. The increased security is flexible and easier to modify as the owner's requirements change. The maintenance of an access control system is less than that of a conventional keyed setup, due to the fact that operational changes are electronic and do not require the mechanical changes that must be done by a trained locksmith.

In this microcontroller based secure access system used core is ATMEL'S 89C51 program executed by the card's microcontroller is written in EEPROM at the mask-producing stage and can be modified in any way. This guarantees that the code is strictly controlled by the manufacturer. For storing user-specific data, individual to each card, the first generation of non-volatile memories used EPROM's which required an extra "high" voltage power supply (typically from 15 V to 25 V). This access system only contain EEPROM which requires a single 5 V power supply (frequently that of the microcontroller) and can be written and erased thousands of times (cycles). Finally, a communication port (serial via an asynchronous link) for exchanging data and control information between the card and the external world is available. A common bit rate is 9600 bit/s a first rule of security is to gather all these elements into a single chip.

5.3 Future scope

Future for smart cards depends mainly on the introduction of multi application cards and overcoming the simplistic mindset that – smart cards are just a method of making a payment. Soon it will be possible to authorize the use of electronic information in Smart Cards by using a spoken word or the touch of a hand. It will be used to carry a lot of sensitive and critical data about the consumers ever more than before when compared with the magnetic strip card. Smart Cards are a relatively new technology that already affects the everyday lives of millions of people. This is just the beginning; soon it will influence the way we shop, see the doctor, and even enjoy leisure. Contact and contactless technologies can be implemented on one card in future.

CHAPTER 6

REFRENCES

- Dr. Marc Lassus, "smart cards: accost effective solution against electronic fraude," no.437, IEE 1997.
- "Contact less Smart Card Technology for Physical Access Control," Avision, Inc. Report, April 1, 2002.
- W.Rankl & W.Effing "Smart Card Hand Book".
- IBM Redbook "Smart Card Case Study"
- C.A.Pinto, A.C.Borim, J.M.Fernandes, A.R. Ferreira "Wireless implementation for access control to restricted areas," IEEE Transaction vol.1-5, no.7803, pp.1078-1081, 1999.
- F.Y, Yang and J.K.Jan "A provable secure access control using smart cards," IEEE Transaction vol, 13, no.3, July 10, 2003.
- Klaus Vedder, "smart cards," IEEE Transaction,1992
- Andrew J Clark ,"Smart Card Paper," Dec. 1990
- Jeffrey B.Carruthers, "Wireless Infrared Communications," Wiley Encyclopedia of Telecommunications, 2002.
- Muhammad Ali Mazidi ,"The 8051 Microcontroller and Embedded Systems,"
- Kenneth J.Ayala "The 8051 microcontroller, programming & applications".
- David A. Williams, "Optocoupler Selection for High Frequency Power Supplies," IEEE Transaction, 1995.
- Dr. P. S. Bimbhra, "Generalized Theory of Electrical Machines".