MULTI-ENTRANCES SECURITY DOOR SYSTEM

YASOTHA A/P PADMANATHAN

This thesis is submitted as partial fulfillment of the requirements for the award of the Bachelor of Electrical Engineering (Hons.) (Electronics)

Faculty of Electrical & Electronics Engineering
Universiti Malaysia Pahang

JUNE, 2012

"I hereby acknowledge that the scope and quality of this thesis is qualified for the award of the Bachelor Degree of Electrical Engineering (Electronics)"

Signature : _____

Name : NIK MOHD KAMIL BIN NIK MOHD YUSOFF

Date : 19 JUNE 2012

Signature : _____

Author : YASOTHA A/P PADMANATHAN

Date : 19 JUNE 2012

Specially dedicated to
My beloved parents, brother, sister
and to all my beloved friends

ACKNOWLEDGEMENT

The successful completion of my project can be attributed to the combined efforts made by the individuals I hereby acknowledge. First of all, I would like to express my heartfelt gratitude and thanks to my supervisor MR. NIK MOHD KAMIL BIN NIK MOHD YUSOFF, for encouraging me to move ahead and for being with me right from the beginning of the project and guiding me at every step. Last but not least, I also thank my parents Mr.Padmanathan & Mrs. Thanemolly and my friends for being with me all the time and giving me moral support. Thank you.

ABSTRACT

Over the years, several security measures have been employed to combat the menace of insecurity of lives and property. This is done by preventing unauthorised entrance into buildings through entrance doors using conventional and electronic locks or discrete access code. Thus, the main idea in this project is to design a database security system that allows only authorised user to enter the premises. There are two entry point with each using different technologies; RFID & keypad. Once the user's identification is verified, the door is unlocked by using EDL (electronic door lock) and all the information such as user ID, date and time are stored in central office. The communication between the entrance points with central office by means of Zigbee wireless technology.

ABSTRAK

Sejak beberapa tahun kebelakangan ini, beberapa langkah-langkah keselamatan yang telah digunakan untuk memerangi ancaman yang mengancam keselamatan nyawa dan harta benda. Ini dilakukan dengan menghalang kemasukan ke dalam bangunan dengan menggunakan kunci konvensional dan elektronik atau kod akses diskret. Oleh itu, idea utama dalam projek ini adalah untuk merekabentuk satu sistem pangkalan data keselamatan yang membolehkan hanya pengguna yang sah sahaja boleh memasuki premis. Terdapat dua pintu masuk dengan setiap pintu menggunakan teknologi yang berbeza; RFID & pad kekunci. Selepas pengenalpastian pengguna disahkan, pintu dibuka dengan menggunakan EDL (kunci pintu elektronik) dan semua maklumat seperti ID pengguna, tarikh dan masa yang disimpan di pejabat pusat. Komunikasi antara pintu masuk dengan pejabat pusat adalah dengan menggunakan teknologi “wireless” ZigBee.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

RFID	-	Radio Frequency Identification
LCD	-	Liquid Crystal Display
MHz	-	Megahertz
GHz	-	Gigahertz
RF	-	Radio frequency
UART	-	Universal Asynchronous Receive Transmit
PIC	-	Programmable Intelligent Computer
V	-	Volts

LIST OF APPENDIXES

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Security and safety have always been of prime concern to every individual or an organization. Safety is the guarantee for the most essential existent of human beings. A security system is necessary for a building or an area to guarantee the safety of the residents and property. The security system has gone through single-route monitor system, control loop monitor system, and processor plus multimedia monitor system eras in the past twenty years. The digital monitor system which used abroad today is the fourth era production of the security system.

It's very annoying that all of the security systems show many shortcomings such as the signals transmitted through cable network, wiring network is a severe time-consuming and high-load work, and it always blocks the progress of the engineering, the information can be watched only in monitoring chamber. It's very difficult to extend system, because the wire connection is fixed, high energy-consuming system and the after-effect is very serious if the cable be cut.

No matter if the building is a corporate setup, home, a public place or a factory, it has become imperative to secure it against potential dangers such as theft, crime, and fire etc. An intelligent system is therefore required which should not only detect but also pre-empt such hazards. Today it has to be updated with the rapidly changing technology to ensure vast coverage, remote control, reliability, and real

time operation. Deploying wireless technologies for security and control in security systems offers attractive benefits along with user friendly interface. The advancements in security and information technologies have led to availability of many off the shelf products. Unfortunately the conventional solutions such as CCTV security solutions, IP network video solutions and fire alarm systems are too costly in terms of deployment and power efficiency; they are application specific, making them void to provide all in one.

For this reason, the Multi-Entrances Security Door System project is proposed. This project uses technology such as Radio Frequency Identification and Zigbee to provide further security system that can be implemented in offices and home premises.

1.2 WIRELESS TECHNOLOGIES

Radio Frequency Identification (RFID) and Zigbee are two wireless technologies that have each developed hosts of applications independent of each other. Each has benefits, with ZigBee supporting advanced sensor networks and RFID suitable for low-power wireless tracking of people and objects.

1.2.1 Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is a new technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, animal, or person. There is a wide research and development in this area trying to take maximum advantage of this technology, and in coming years many new applications and research areas will continue to appear. This massive growth in RFID also brings about some concerns, mainly the security and privacy of those who work with or use tags in their everyday life. RFID technology is much more secure compared to other networks.

RFID technology consist of RFID reader and RFID tags. RFID tags are also called RFID transponders and they are divided into passive and active RFID tags. In this project passive tags are being used. This technology allows the system nodes or tags to exchange data via radio frequency signal communication. After receiving a radio signal, the tags process this information in order to answer back the basic data required for identifying the tag uniquely. This data is processed in the reader side with the help of software tools such as an auxiliary database or some other communication system. Some of the most popular applications of the RFID technology include, object and good authentication, access control for vehicles and humans, race timing, animal identification, product tracking and inventory systems, etc.

1.2.2 Zigbee

ZigBee is one of the typical short-range wireless communication technologies, which has been widely used in a certain application areas including the family network, control network, mobile phones and other mobile terminals in foreign countries. ZigBee is a software standard that sits on top of the IEEE802.15.4 low data rate wireless standard. The ZigBee (IEEE 802.15.4) is a new technology that permits the implementation of Wireless Personal Area Networks (WPAN). It is very suitable for wireless sensor networks due to the very low power consumption. The selection of the Radio Frequency (RF) communication modules used for the wireless transmission part in this project is based on several criteria. They are range of communication, power consumption, ease of integration and the cost. So, for this project the XBee PRO wireless modules is chosen which conform to the IEEE 802.15.4 standard.

This system uses ZigBee to build transmission network, which is used for the transmission of sensor data, and uses customized wireless transmission protocol, which is designed based on simplicity and reliability. In the protocol, considering simplifying microcontroller functions of RFID & ZigBee node and reducing system cost, the wireless transmission protocol mainly achieves the capabilities of error checking, data framing, conflict mechanisms such as retransmission, etc.

1.3 PROBLEM STATEMENT

The existing security systems show many shortcomings such as difficult to extend and severe time-consuming because it is based on wiring network technology. For a wired network, certain levels of security are maintained since access to the physical medium is restricted to the devices physically connected to the network. It is very difficult to extend the system, because the wire connection is fixed. In additon, there are also insecurity in system identification due to the information can be watched only in monitoring chamber. Failure of keeping or tracking the database leads to increasing theft or insecurity to the lives and properties.

1.4 OBJECTIVES

To develop and design a secure door security system using various form of technology such as Radio frequency Identification (RFID) with a secure and effective Zigbee wireless transmission of data.

1.5 SCOPE OF PROJECT

The scope of this project is:

- Develop at least 2 different type of user identification such as using Radio Frequency Identification (RFID) & keypad.
- Use wireless transmission technology such as RF & Zigbee for nodes communication.
- Develop a database at master node for analysis.

1.6 THESIS OUTLINE

Multi-entrances Security Door System project's final thesis is a combination of 6 chapters that contains and elaborates specific topics such as the Introduction, Literature Review, Hardware Implementation, Software implementation, Result and discussion and Conclusion.

Chapter 1 is the Introduction of the project. The explanation for the project will be given in a general term. The objectives of the project will be elaborated. It is followed by the explanation in the scope of project and also the problem statements.

Chapter 2 is the Literature review for the development of multi-entrances door security system. This chapter describes the literature review of the project elaborately. Explanation will be focused on security system related researched and based on theory and conceptual ideas. Some literature reviews of current existing projects based on security system are also be discussed.

Chapter 3 is the Hardware design.. The explanation gives according to the function in the board. Flow of the project and how it is executed is explained in detail. This section gives explanation more towards on technical part of it.

Chapter 4 is the Software implementation part. Software development of the project is discussed here. Software used and how it is executed will be discussed here.

Chapter 5 discussed about results of testing conducted for the project. All the testing results are shown here with appropriate explanation.

Chapter 6 discusses the conclusion and further development of the project. This chapter also discussed about the total costing involved and potential of this project for commercialization.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Security is the condition of being protected against danger, loss, and criminals. In the general sense, security is a concept similar to safety. The slight difference between the two is an added importance on being protected outside threats or dangers. Individuals or actions that go or act against the general rules of protection are responsible for the breach of security.

Security has to be compared and contrasted with other related concepts: Safety, continuity, reliability. The key difference between security and reliability is that security must take into account the actions of people attempting to cause destruction. There is an immense literature on the analysis and categorization of security.

In this chapter, the review of literature is explained briefly with the guidance of the existing projects conducted by researchers for the development of the project, multi-entrances security door system. In literature review, the technologies such as Radio Frequency Identification (RFID) and Xbee Pro wireless technology that is used in this multi-entrances security door system is further discussed.

2.2 SYSTEM APPLICATIONS CONDUCTED BY RESEARCHERS

Over the years, security system is implemented in various places. A security measure plays an important role in daily life. Some of the researchers have conducted and successfully developed various types of security systems using different technologies.

2.2.1 The Design and Implementation of Intelligent Campus Security Tracking System Based on RFID and ZigBee

The project [1] is designed by Xiaokang Li and Li Gao and it is based on RFID and ZigBee wireless technology. The intelligent campus security tracking system uses physical methods and electronic technology, automatically detects theft in monitoring areas, generates alarm signals, and tracks targets through the detection point of RFID.

Figure 2.1 shows the flow of the operating system for the project. RFID & ZigBee nodes sense the RFID (master / slave) labels and it then send information in the labels to the ZigBee network real time, which is then transferred to the PC nodes. PC checks the label information in the database, when master label and slave label match or only master label appears; the system recognizes it as legal input. But when only slave label appears or master label and slave label don't match, the system recognize it as illegal input, then step to is proceeded. Position changes of RFID (slave) the tags are recorded, slave tags are tracked, and warning are shown at PC nodes. Then the database is keep tracked, looking for the owner of items and confirming information is sent to the owner through the system. When the owner logins WEB to search for items, he can see the real-time location of his valuables according to the hints. After confirmation, the valuables will be stopped at the entrance guard. As for false information, the owner can cancel this warning.

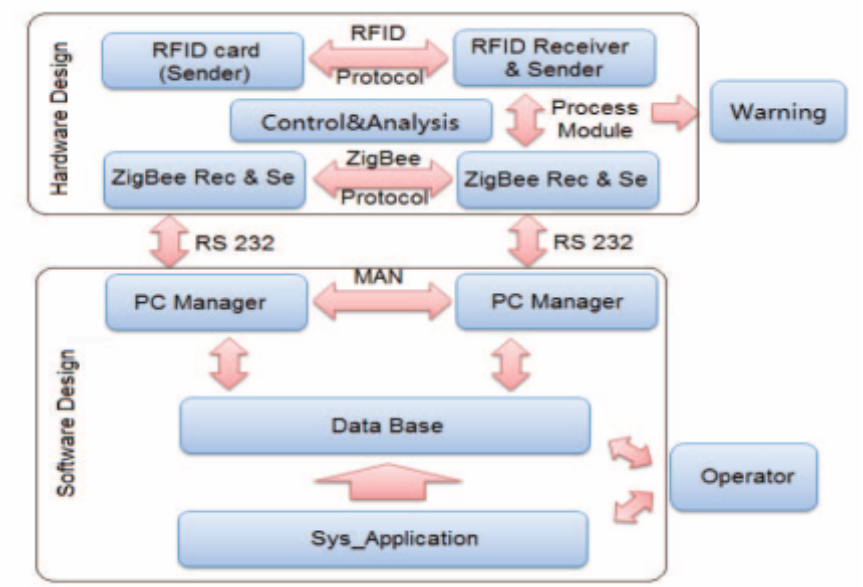


Figure 2.1: System architecture designed by Xiaokang Li and Li Gao

2.2.2 Scalable ZigBee-Based Smart Authentication and Access Control System Design Using XMOS Programmable Chips.

Wael Hosny Fouad Aly, Haytham Aboulabbas M., Moustafa H. Aly, Hossam Eldin Moustafa, have presented their paper on Scalable Zigbee based smart authentication and access control [2]. In their research paper, they have discussed an efficient, inexpensive, scalable, and ZigBee-based smart authentication and access control system that consists of a central node and remote nodes. The central node holds a database of authorized users and it is mesh-networked to a set of remote nodes which are spread throughout the premises of an enterprise. The goal of the system is to provide an online electronic access control system that will automate entry to the premises of an enterprise according to pre-assigned user credibility. The system consists of a central node and distributed remote nodes. Remote nodes are installed at the main entrance gates of the enterprise as well as at the office doors within the premises and wherever user tracking is required to be maintained by the system. Once a user carrying the RFID tag is in the vicinity of the reader that reside in the remote node at the main entrance gate, the tag will be detected and its ID number is read by the RFID reader module and is then transferred over the IEEE 802.15.4 wireless link to the central node to verify whether access is granted to enter or not. Upon proper authentication by the central node, the programmable chip that resides in the corresponding remote node will trigger an electric door strike that will allow the user to open the main entrance gate. Figure 2.2 shows the overall system model that has been proposed.

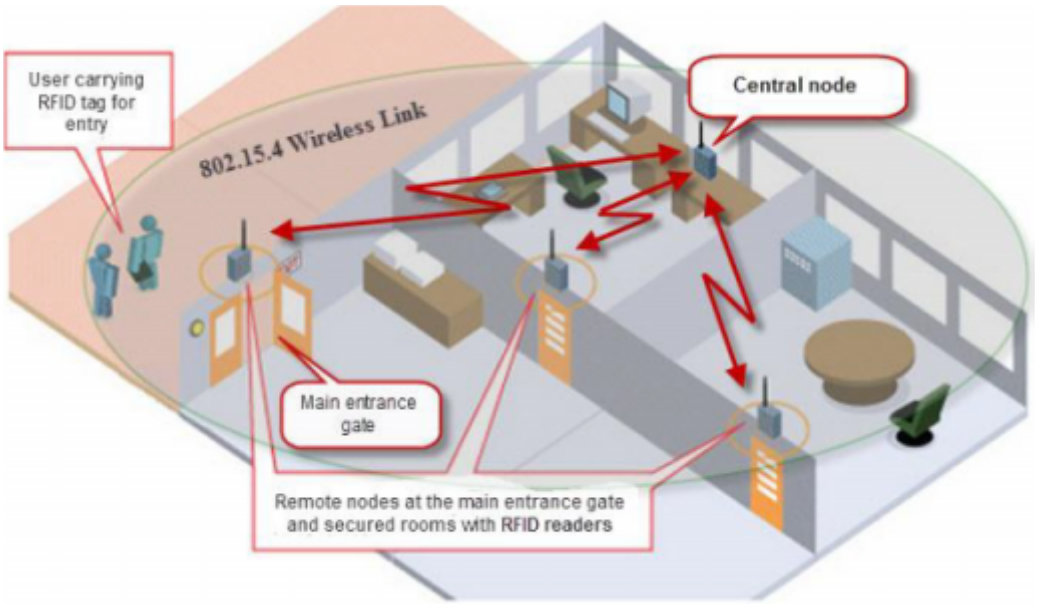


Figure 2.2: Model system proposed by Wael Hosny Fouad Aly, Haytham Aboulabbas M., Moustafa H. Aly, Hossam Eldin Moustafa

2.2.3 Wireless Networked Security System Based on ZigBee Technology.

In [3], present a wireless networked security system based on ZigBee technology. The system adopts hybrid topology structure based on cluster, which consists of many micro-sensor nodes, network coordinator nodes, network gateway (router), communication network and monitor centre (computer). For short distance transmission, the micro-sensor nodes collect data from the monitoring surroundings and transmit to the gateway using ZigBee communication. For long distance transmission, from the gateway to the monitor centre, system uses TCP/IP protocol. The gateway in this system is the protocol conversion used to transform a data package in ZigBee protocol to TCP/IP protocol before transmitting.

2.2.4 Building a Smart University using RFID Technology

In this paper [4], the researchers contemplate present the use of RFID technology in building a smart university. Prototype is developed considering major use cases involved in a smart university. The system covers maintaining attendance record, switching control of electrical items and security locks of rooms. Results show that consumption of energy and object tracking time is decreased while security of rooms and credibility of attendance record are increased. ZigBee is selected for this research due to its low cost, long communication range and low power consumption.

System is working as follows: First Reader detects RFID card and forward that ID to microcontroller. Microcontroller authenticates the ID and generates a specific number (3 byte code) against that ID. This specific number is then forwarded to the ZigBee transceiver via serial link from where it is broadcasted to receiving nodes. One of the receiving nodes is the database server where attendance record is managed. At the same time control circuit node receives the broadcast and automates the office equipments based on that specific profile. The profiles can be modified from the server as they are stored in NVRAM. Figure 2.3 shows the block diagram of the system.

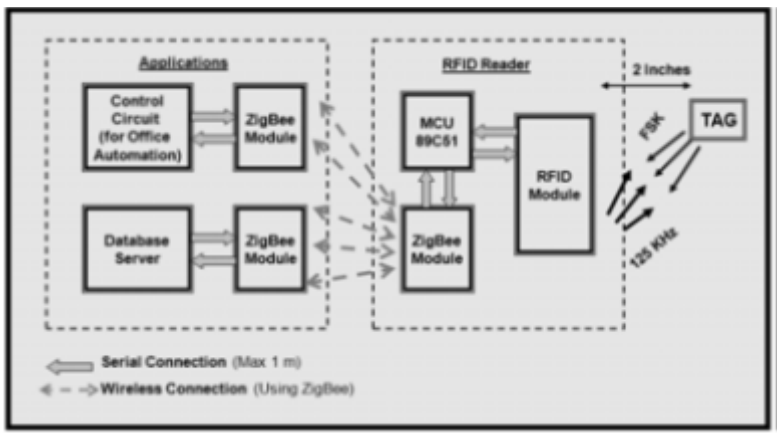


Figure 2.3: Block diagram of the system

2.2.5 Implementation of ZigBee-GSM based Home Security Monitoring and Remote Control system.

Arbab Waheed Ahmad, Naeem Jan, Saeed Iqbal, Chankil Lee [5], discusses on implementation of a novel security and control system for home automation. The proposed system consists of a control console interfaced with different sensors using ZigBee. Suspected activities are conveyed to remote user through SMS (Short Message Service) or Call using GSM (Global System for Mobile communication) technology. Upon reply, the remote user can control his premises again through GSM-ZigBee combination. In addition, traditional burglar alarm enhances security in case of no acknowledgment from remote user. This system offers a low cost, low power consumption and user friendly way of a reliable portable monitoring and control of the secured environment. Using the concept of serial communication and mobile phone AT-commands (Attention TelephonelTerminal commands), the software is programmed using C-Ianguage. The design has been implemented in the hardware using ZigBee EM357 module, Atmega128 MCU (microcontroller unit) and Sony Ericsson T290i mobile phone set. Figure 2.4 shows the block diagram and circuit connection of the system.

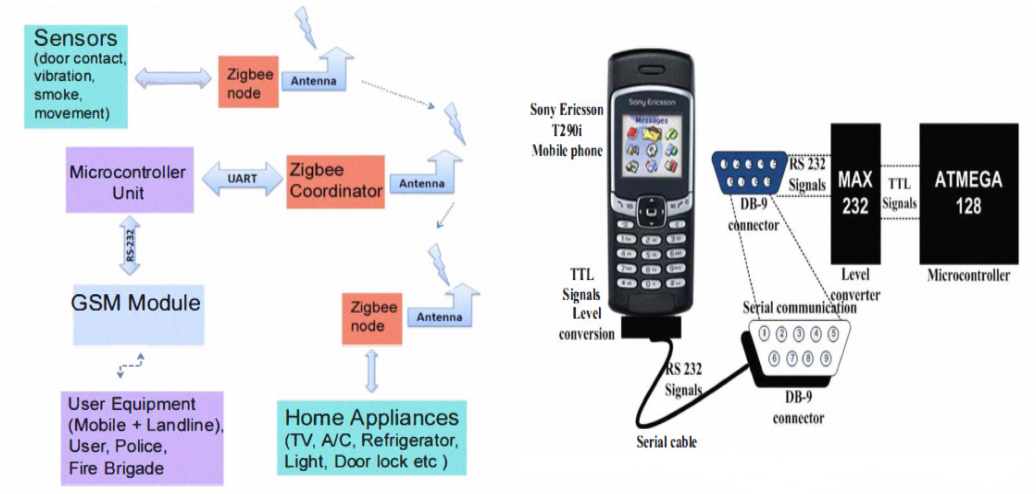


Figure 2.4: block diagram and circuit connection of the system.

2.2.6 Design of RFID Proximity Security Door Lock

This study [6] features the implementation of a security system utilizing Radio Frequency Identification (RFID) which, through the basic interface provided by Wiegand technology, allows interoperability with the MIFARE tag (smart card). This study discusses the RFID Proximity Security Door Lock (PSDL) system where is an access system that enables entry using a smart card, suitable for the safety requirements of companies, laboratories or factories, to ensure that only authorized personnel is allowed access. In terms of system design and development, this study consists of a combination of both hardware (circuit design) and software (program design). Unlike mechanical locks, which use keys that are prone to duplication, RFID-based door locks adopt contactless technology that utilizes smartcards embedded with encrypted serial keys that cannot be duplicated. This feature ensures the reliability of RFID door locks, providing a secure access control. Figure 2.5 shows the Block diagram of the system.

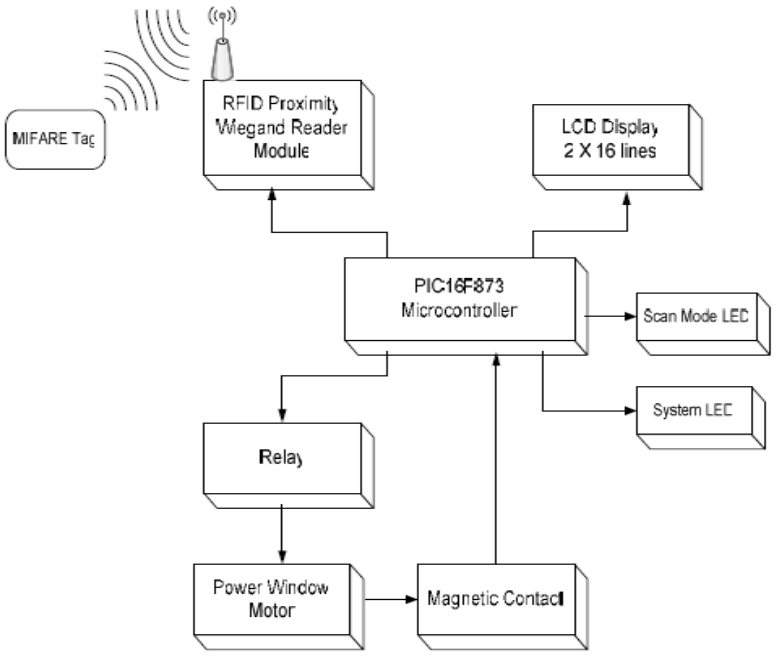


Figure 2.5: Block diagram of the system

2.2.7 Design of Dynamic RFID System using 89C51 Microcontroller based Embedded System for Effective Supply Chain Management.

This study [7] addresses the design and model the dynamic RFID System using 89C51 Microcontroller based Embedded System for effective and optimal supply chain management. This system is implemented using an embedded microcontroller. The embedded microcontroller used here is 89C51 microcontroller. Since this microcontroller has inbuilt peripherals it is called as embedded microcontroller. The person holds the RFID tag and the RFID reader is placed at the in front of the factory gate. The registered number and the corresponding code to the tag are already stored in the microcontroller. While the person is passing through gate, the reader automatically identifies the person. RFID transceiver value is transferred from the RFID reader to the 8-bit embedded microcontroller through serial port. After identifying the person, the active tag will enable and to open the factory gate and to allow the person to access the real work. The controller identifies the unauthorized person it will not allow the person, at that time web camera will be enabled then capture the photo for a particular person and stored on a administrator PC. In an advanced manner to design this system, the administrator PC storage images will be transferred to control room via wire or wireless technology. The control room will be sent the appropriate command to administrator for further decision.

2.2.8 Microcontroller Based Home Automation System with Security

This project shows home automation system which uses automatic control as a result of which power is saved to some extent. Two control units were used one for internal system and one for external system and these control unit based on ATMEL'sAT89S52 microcontroller. In this system, researchers have ensured a safe locking system. On seeing from outside the lock would not be visible but this inbuilt locking system ensures security. This lock can be opened and closed with the help of a password which will be entered using a keypad. The door will only open or close only if the password is valid else it will remain in its original state. The lock cannot be broken because to the person standing outside can just see the closed door and not the lock as it is inbuilt. The password is given with the help of controller and can be changed by simply making a small change in the program and then burning the program in the controller. Automated switching also described in the study where all the switches in the house can be controlled automatically [8].

2.2.9 A Scalable Intelligent Room Based on Wireless Sensor Networks and RFIDs

Iv´an Cabrera Altamirano and Francisco Rodr´ıguez Henr´ıquez [9] presents the analysis, design and implementation of an intelligent classroom whose two main components are realized using two emergent wireless technologies, namely, wireless sensor network, in this case they choose Zigbee and Radio-frequency identification (RFID) tags. The combination of these two technologies is discussed to produces a powerful and versatile solution that can offer automated access control to a classroom as well as the monitoring of relevant environment variables such as temperature, humidity and room lighting. They have design a readily scalable to a set of interconnected classrooms, by means of a routing protocol especially designed for achieving a multi-hop communication network.

2.2.10 Research on Application of RFID System with 2nd-Generation ID card Based on ZigBee Wireless Network

The researchers have presented about the RFID system in this article. The system consists of a reader and a computer management system (CMS). The reader plays the crucial role, and thus is the focal point of our research. The reader has determinant effects on the stability and security of the system, receiving information of the second generation ID cards as radio-frequency, and then sending it to the CMS; the CMS, on the other hand, upon reception of the information from the reader, conducts the corresponding processing and controlling. [10]

Main control system is connected with the reader module by an SPI connector. Once the RFID information stored in the module's controlling chip is captured, it will be sent through the wireless connector to the computer management system, and be processed there.

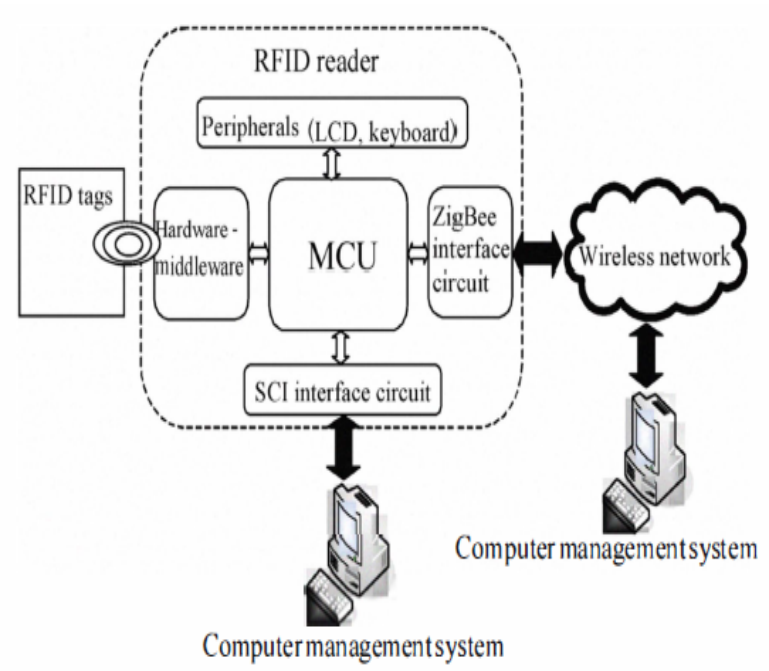


Figure 2.2.10: Block diagram of the system.

CHAPTER 3

HARDWARE IMPLEMENTATION

3.1 INTRODUCTION

The project consist two major parts; hardware and software. All the technical aspects regarding this project will be included in this section. The system is made up of four parts which includes the identification of RFID tag & password using keypad, verification of detected code or password, opening and closing of magnetic sensor doors according to people and transmission of data to central office.

3.2 System board of the Multi-entrances security door system

The basic block diagram of the system board is shown in figure 3.1. The system board consists of Microcontroller, RFID module, Keypad module, Zigbee module, Magnetic door lock and a PC. The overall system is divided into three parts, entrance1, entrance2 and the central office.

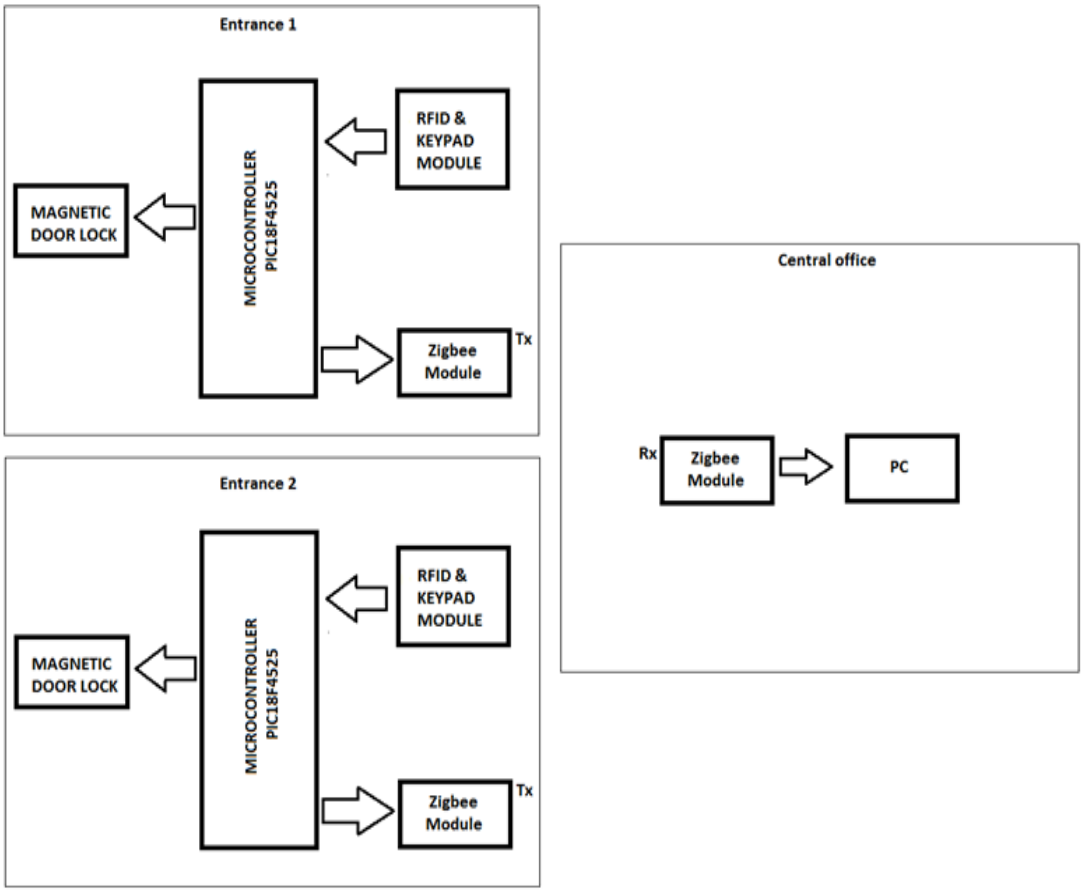


Figure 3.1: Basic Block Diagram of the multi-entrances door security system using wireless technology.

3.3 The system operation

Figure 3.2 shows the flow chart of the system where it describes the full operation for the system. When a RFID card is touched on the reader and a password is entered, the data is sent to PIC18F4525 Microcontroller. Then the PIC compares the ID card number and the password to authenticate the authorised user. If a user is identified, PIC18F4525 sends instruction to the magnetic door to unlock the door as well as a signal transmitted through Xbee PRO wireless technology to the central office.

The receiving end via XBee PRO wireless module is the secondary system of the project. Here the important data such as User's Name, ID card number, password, time in-out and date is being saved at database every time a user enters the premises. This is done for the security purposes.

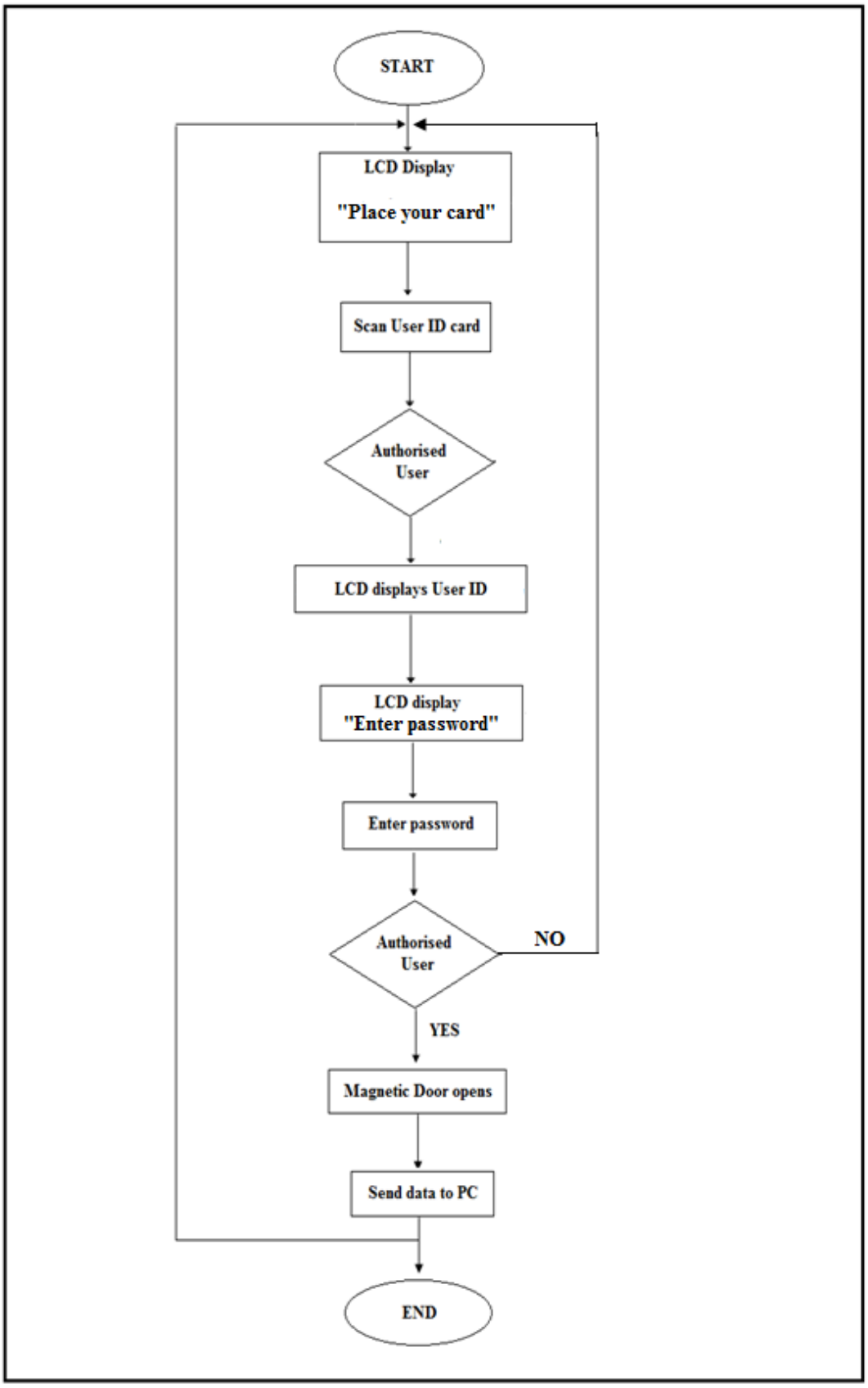


Figure 3.2: Flow chart of the multi-entrances security door system.

3.4 HARDWARE

Hardware part explains about all the circuit connections that made in this project. Each and every circuit are explained in detail for theirs functions part with the aid of schematic diagram.

3.4.1 Microcontroller PIC18F4525

The microcontroller used to operate circuits in this project is Microchip's PIC18F4525. The pin layout is shown in Figure 3.3. This powerful 10 MIPS (100 nanosecond instruction execution) yet easy-to-program (only 77 single word instructions) CMOS FLASH-based 8-bit microcontroller packs Microchip's powerful PIC® architecture into an 40- or 44-pin package and thus providing a seamless migration path of software code to higher levels of hardware integration. The PIC18F4525 features a 'C' compiler friendly development environment, 256 bytes of EEPROM, Self-programming, an ICD, 2 capture/compare/PWM functions, 8 channels of 10-bit Analog-to-Digital (A/D) converter, the synchronous serial port can be configured as either 3-wire Serial Peripheral Interface (SPI™) or the 2-wire Inter-Integrated Circuit (I²C™) bus and Addressable Universal Asynchronous Receiver Transmitter (AUSART). All of these features make it ideal for manufacturing equipment, instrumentation and monitoring, data acquisition, power conditioning, environmental monitoring, telecom and consumer audio/video applications. This PIC18F4525 was chosen because of its low power consumption and memory size of 256 bytes EEPROM data memory.

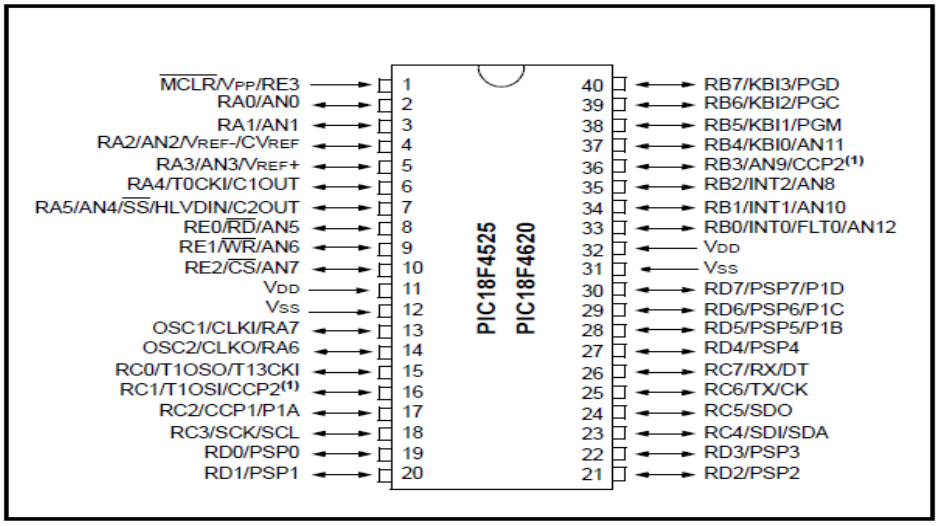


Figure 3.3: Pin layout of PIC18F4525

3.4.2 Power Supply Module

Figure 3.4 shows the connection of power module. The microcontroller should be connected to a power module as shown in the figure. The power module supplies a regulated +5V to power up the system. A 9V is supplied to the system and to be regulated by the LM7805 to produce a regulated +5V. The diode 1N4007 is connected as shown to protect the circuit from wrong polarity supply. The capacitors are connected to stabilize voltage at the input and output side of the LM7805 voltage regulator.

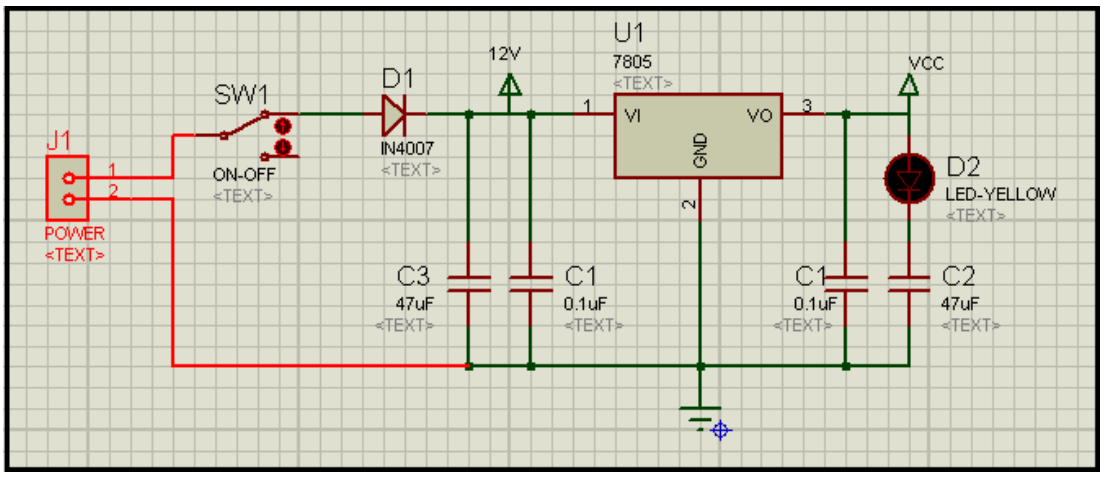


Figure 3.4: Power circuit

3.4.3 Reset Module

Figure 3.5 shows schematic diagram of reset circuit. The reset pin is an active high logic. To reset the microcontroller, the reset should be active high. When the push button is pressed, the current flows directly to ground or is it considered as short circuit. Therefore, there will be no current flow through the reset pin. Once the reset pin is released, the current flows through the reset pin and making it active low. The diode makes sure the current flows one way and the resistor is to filter the high current.

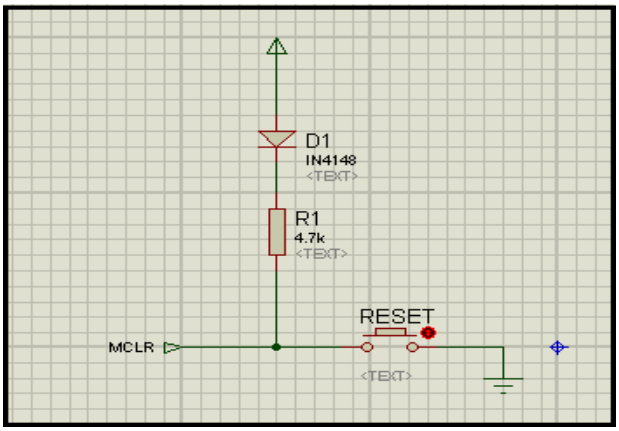


Figure 3.5: Reset circuit

3.4.4 Liquid Crystal Display

Figure 3.6 shows the LCD module connection. The LCD used for this project is a 2x16 character LCD. A 16x2 LCD means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data. The command register stores the command instructions given to the LCD. A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc. The data register stores the data to be displayed on the LCD. The data is the ASCII value of the character to be displayed on the LCD.

Vss and V_{EE} pins of the LCD are connected to ground while pin V_{DD} is connected to power supply of +5V. Pins RB4 and RB5 of microcontroller are connected to the enable (E) and select register (RS) pins of LCD respectively. As to operate the LCD in 4-bit mode, data bus pins from D4 to D7 is connected to pins RD4 to RD7 of microcontroller. Pins 15 and 16 of LCD represents for backlight positive input and backlight negative input. Thus, pin 15 is connected to power supply and pin 16 is grounded.

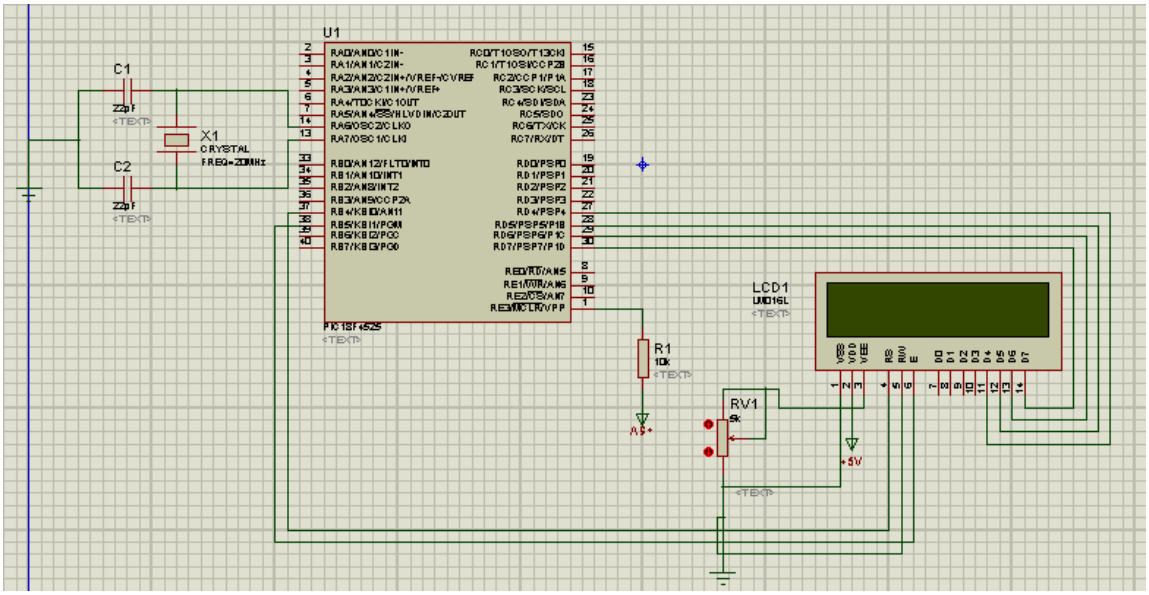


Figure 3.6: LCD Module

3.4.5 Serial Communication Module

Asynchronous serial communication uses the RS232 level standard to communicate between the microcontroller and computer. This is because the signal sends from the microcontroller propagates along the line and exposes to various form of noise. As a result, it may cause a voltage drop in the connections. Therefore RS232 level standard is used to increase the voltage level in order to ensure data can be transmitted and received by the destination.

Figure 3.7 is a simple connection of the serial communication with MAX232 circuit. The serial communication with PIC18F4525 is called asynchronous communication and requires only two connections which are Transmitting signal (TxD) and Ground (GND).

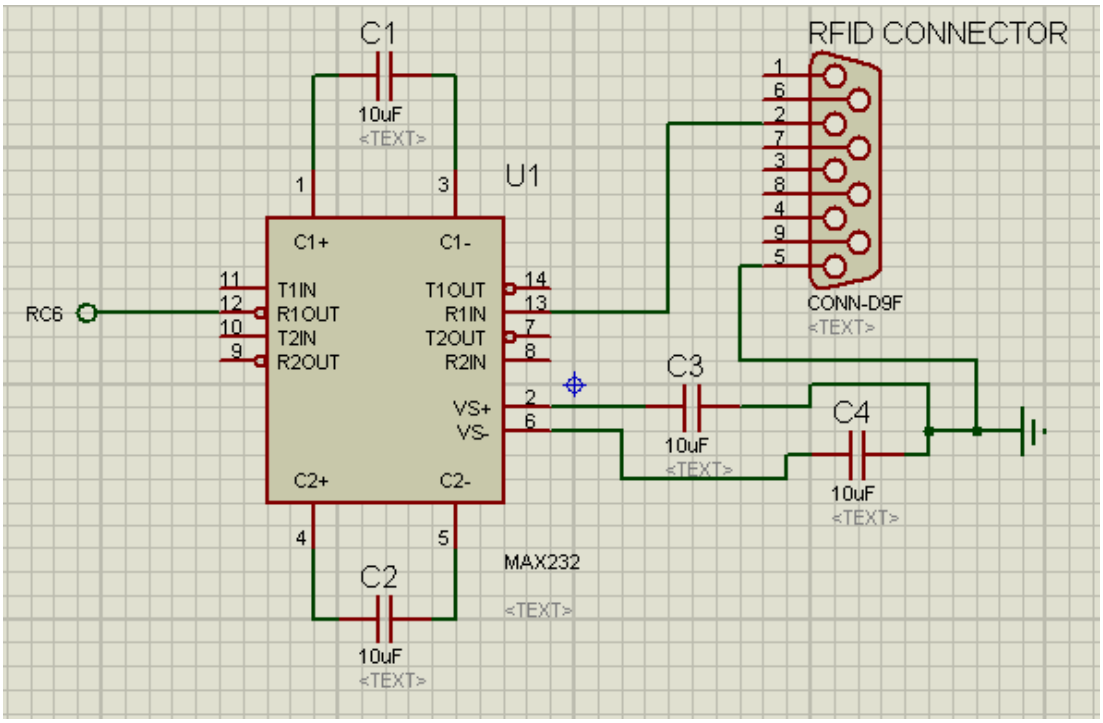


Figure 3.7: Serial communication module

3.4.6 RFID Reader and Tag

RFID-IDR-232N is plug and use RFID reader. It has been designed with capabilities and features of:

- Low-cost solution for reading passive RFID tags
- 9600 baud RS232 serial interface (output) to PC
- 2cm reading range
- 0.1s response time
- 12 bytes of data received include start of heading, RFID ID and start of text.

RFID-IDR-232N can be connected either to PC or microcontroller as a part of embedded system. RFID-IDR-232N will read the ID from RFID Reader. The ID is normally 10 digit of number. RFID-IDR-232N will automatically send this ID with 1 byte of start of heading (0x01), followed by 10 byte of ASCII character and 1 byte of start of text (0x02).

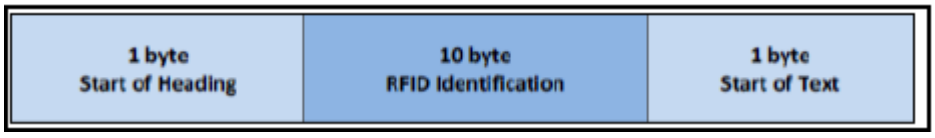


Figure 3.8: 12 byte ID packet data

The tag is the device that contains the identification data. It identifies the item it is attached to. The reader retrieves data from the tag. It is also called an interrogator that reads or reads/writes from/to the tag. The antenna attached to the reader emits electromagnetic waves and receives responses from the tag. Tags can be classified in two main categories based on their respective power source, passive and active tags. Passive tags have no attached power source and rely on excitations by the signal emitted from the reader antenna to energize itself. Active tags on the other hand contain an embedded battery as the power source. The passive and active tags can be further distinguished by their memory type. The classifications are RO (Read-Only), WORM (Write Only, Read Many) and RW (Read-Write). However, different

RFID carrier frequencies may result in different read-write ranges, data transmission speed, and cost. The operational frequencies available for RFID are low frequency (LF), high frequency (HF), ultra high frequency (UHF) and microwave.

Figure 3.9: RFID Reader and Female RS232 cable with USB and RJ11.

3.4.7 Xbee Module

Leveraging wireless technology can be challenging without the right combination of expertise and resources. The XBee product family is a series of modular products that make deploying wireless technology easy and cost-effective. Multiple protocols and RF features available in the popular XBee footprint. XBee and XBee-PRO ZB ZigBee modules provide cost-effective wireless connectivity to devices in ZigBee mesh networks. Utilizing the ZigBee PRO Feature Set, these modules are interoperable with other ZigBee devices, including devices from other vendors[†]. Programmable versions of the XBee-PRO ZB ZigBee module make customizing ZigBee applications easy, even without wireless design expertise.

3.4.7.1 Xbee Module vs XbeePro Module

XBee and XBee-PRO OEM RF Modules are small, high-performance, low-cost, wireless data transceivers. Both operate in the 2.4 GHz ISM band and because they have agency approvals (FCC, ETSI approvals pending), both can be operated without a station license. The XBee and XBee-PRO are pin-compatible with one another, though the XBee-PRO is slightly longer than the XBee. Both modules are available with a whip antenna, a low-profile chip antenna or a U.FL connector (to which an external antenna can be connected). The XBee transmits up to 1 mW of power, while the XBee-PRO transmits up to 60 mW of power. In addition to transmitting more power, the XBee-PRO is capable of receiving weaker signals than is the XBee; which means the XBee-PRO has better receiver sensitivity. Because the XBee-PRO is both more sensitive and transmits more power, it can send and receive data over longer distances than the XBee. Therefore for this project, I have decided to use Xbee-PRO. Figure 3.10 and 3.11 shows the mechanical drawing for the Xbee and Xbee pro while table 3.1 explains about the specifications.

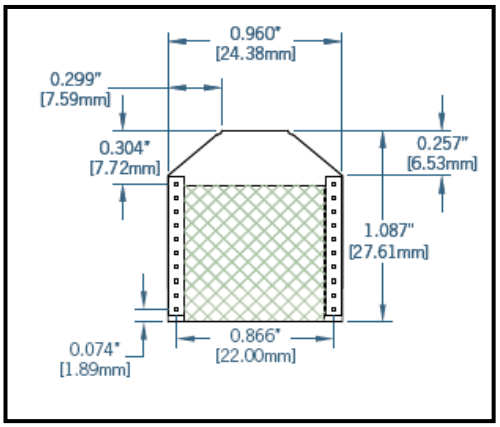


Figure 3.10: Mechanical drawing of XBee

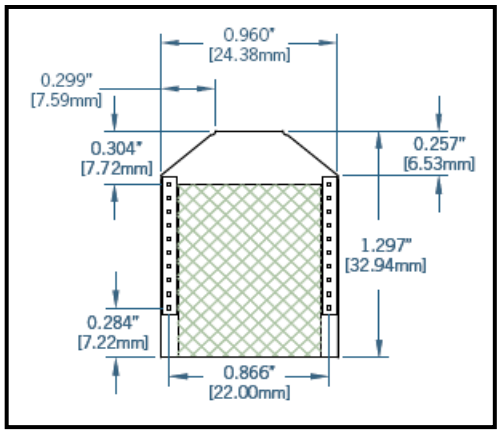


Figure 3.11: Mechanical drawing of XBee Pro

Specification	**XBee ZNet 2.5**	**XBee PRO ZNet 2.5**
Performance		
Indoor/Urban Range	up to 133 ft. (40 m)	up to 300 ft. (100 m)
Outdoor RF line-of-sight Range	up to 400 ft. (120 m)	up to 1 mile (1.6 km)
Transmit Power Output	2mW (+3dBm), boost mode enabled 1.25mW (+1dBm), boost mode disabled	63mW (+18 dBm) 10mW (+10 dBm) for International variant
RF Data Rate	250,000 bps	250,000 bps
Serial Interface Data Rate (software selectable)	1200 - 230400 bps (non-standard baud rates also supported)	1200 - 230400 bps (non-standard baud rates also supported)
Receiver	Sensitivity -96 dBm, boost mode enabled -95 dBm, boost mode disabled	-102 dBm

Table 3.1: Specifications of the XBee /XBee-PRO ZNet 2.5 OEM RF Module

3.4.7.2 Uart

One of the main advantages of XBee and Xbee Pro is its UART (Universal Asynchronous Receive Transmit) serial interface. This interface makes them ideal for communication with a PC, as well as a PIC microcontroller. Essentially, when operating in its normal receive/ transmit mode, the Xbee and Xbee Pro serve as a wireless serial communication. Thus, in simple applications they can be used as a replacement for serial cable. They can also handle baud rates as high as 115 200.

3.4.7.3 Xbee PRO Transmitter Ciruit

The XBee Pro transmitter module needs a 3.3V as its power supply. Any voltage more than this voltage level could damage the wireless module. Thus, a voltage regulator of LM1117 is used to regulate +5V into +3.3V and provides voltage to the XBee Pro wireless module. For the XBee Pro to transmit data from the host system, it should receive data from pin RC7 of microcontroller. Figure 3.12 shows the circuit connection of the XBEE pro receiver circuit.

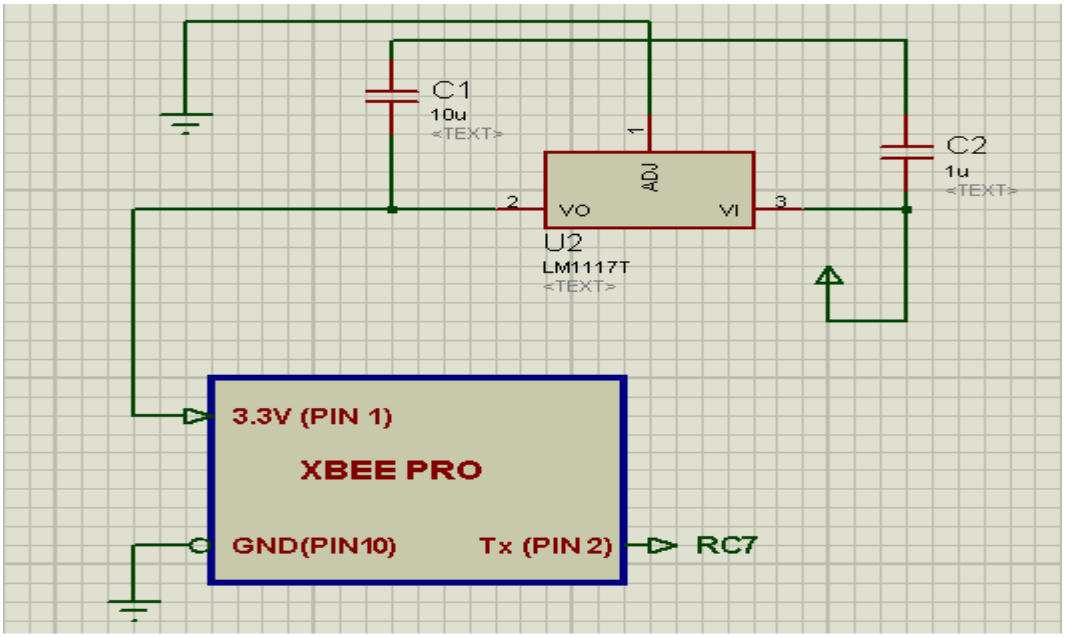


Figure 3.12: XBee Pro Transmitter Module

3.4.7.4 Xbee PRO Receiver Circuit

XBee Pro transmitter module needs a 3.3V as its power supply. Any voltage more than this voltage level could damage the wireless module. Thus, a voltage regulator of LM1117 is used to regulate +5V into +3.3V and provides voltage to the XBee Pro wireless module. After the XBee Pro receives data from the host system, it should transmit data to pin RC6 of microcontroller. Figure 3.13 shows the circuit connection of the XBEE pro receiver circuit.

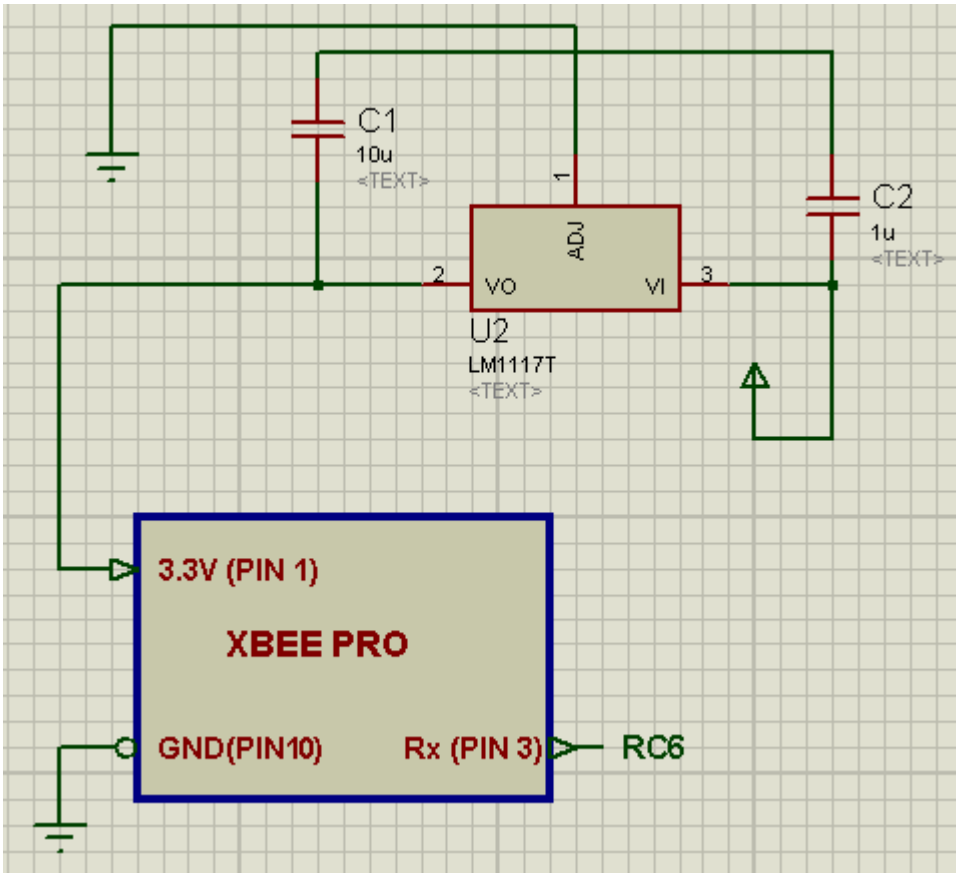


Figure 3.13.: XBee Pro Receiver Module

3.4.8 Keypad Module

Figure 3.14 shows a simple keypad circuit connection. The 4x4 Key Matrix is connected to PORTC & PORT a of PIC18F4525. The four columns are connected to RC0-RC3 and the four rows are connected to RA04- RA3. Each digit is refreshed every 20ms with a 5ms pulse. The keypad is sampled every 20 ms with four 3ms pulses. The keypad sampling is where the columns are connected to output pins, and the rows are connected to input pins. Each column is sequentially driven to a low voltage while at the same instance the four rows are sampled. If a key is pressed in a column which is at a low level, that low level will be conducted to the input pin through the closed key and the corresponding row will be sensed as a low. Before a new column is brought low, care should be taken to discharge the input pins.

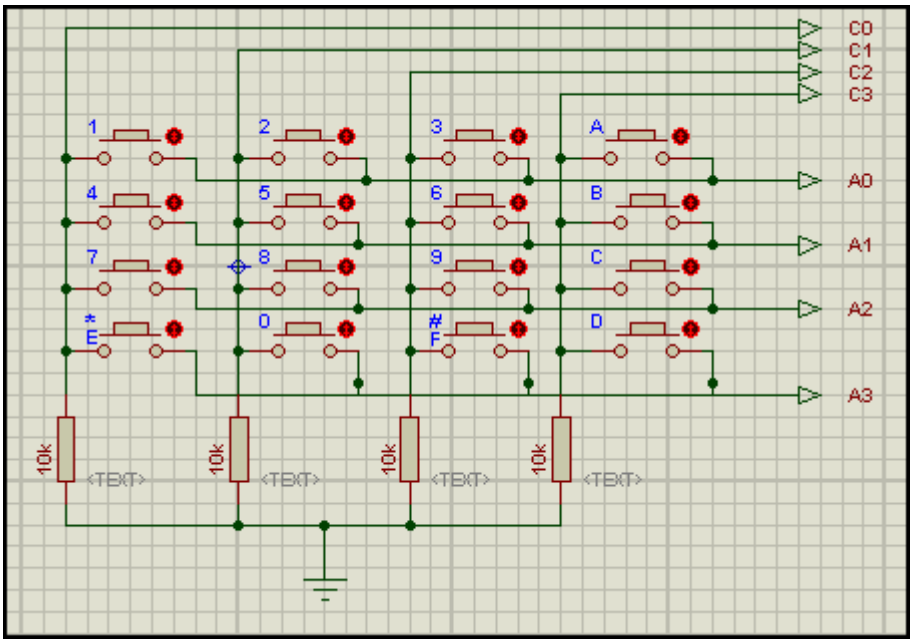


Figure 3.14: Keypad pin configuration

CHAPTER 4:

SOFTWARE IMPLEMENTATION

4.1 Introduction

The software design is basically used to create monitor programs which is written using c language. The program is stored in ROM. This monitor program is used for executing user's programming and loading object file (.hex file). The monitor program is very important because it allows user to load program without using Erasable Programmable Read Only Memory (EPROM) programmer.

4.2. The C language

C is a portable language intended to have minimal modification when transferring programs from one computer to another. The use of C in Microcontroller applications has been brought about by manufacturers providing larger program and RAM memory areas in addition to faster operating speeds. C programming language creates lists of instructions for a computer or a microcontroller to follow. C is one of thousands of programming languages currently in use.

C is excellent for actually writing system level programs, and the entire Applix 1616/OS operating system is written in C (except for a few assembler routines). It is an excellent language for this environment because of the simplicity of expression, the compactness of the code, and the wide range of applicability. C has been around for several decades and has won widespread acceptance because it gives programmers maximum control and efficiency.

4.3 The C Compiler

For the software development, the PIC C compiler is used for the writing the program coding. This program allows the code written in C programming language. The code must be compiled using PIC C Compiler's built in compiler to change the C code to hexadecimal (HEX) format, which is what the PIC understands and can run. Therefore it is important to compile after any and all changes are made to the code. After the code was developed and compiled using PIC C Compiler, the software PICkit 2 was used to write the code to the PIC.

The PICkit 2 programming software is launched. The following programming interface appears as shown in Figure 4.1 and notifies that the PICkit 2 the target device is found and connected.

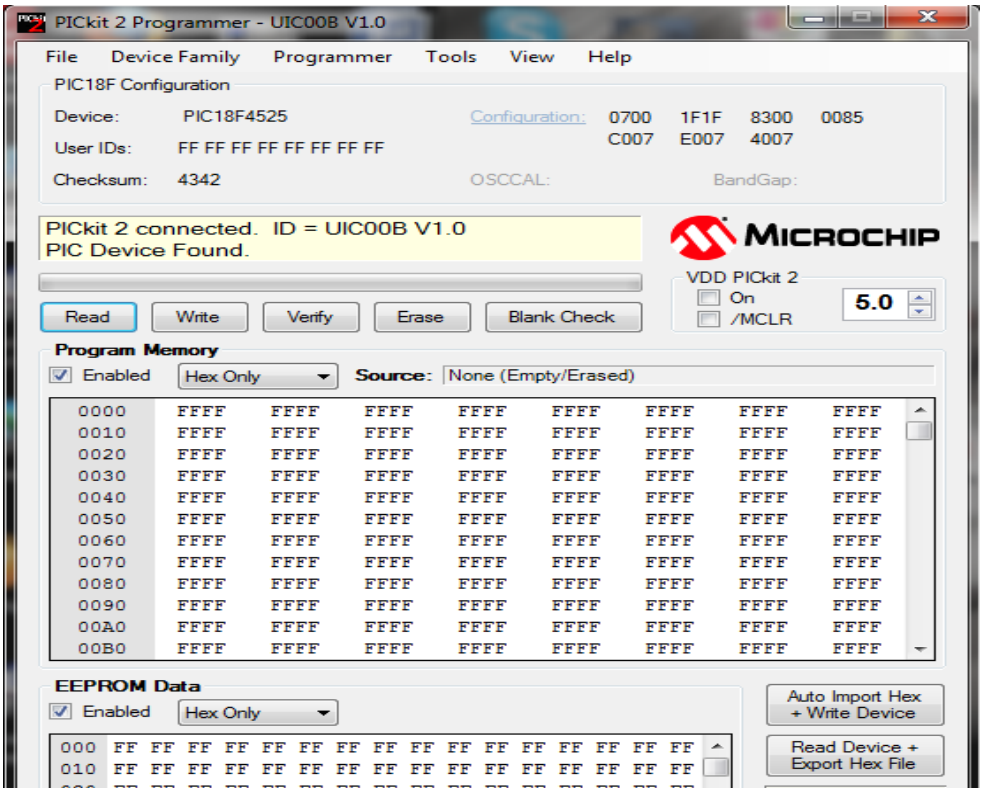


Figure 4.1: PICkit 2 Programmer Interface

4.4 Programming coding

4.4.1 LCD display

In this project, the first output of the system is an LCD display that will display the information about the system. The LCD display will display phrase "Place your card" once the system is switched on. In order for the LCD display to display the stated phrases, the PIC should be programmed with appropriate C programming language. The source code is shown in Figure 4.2 below.

```
Lcd8_Config(&PORTB,&PORTD,4,5,6,7,6,5,4,3,2,1,0);
Lcd8_Cmd(LCD_CURSOR_OFF);    // Turn off cursor
lcd8_Cmd(LCD_CLEAR);
PORTA=PORTB=PORTC=0x00;
do
{

 lcd8_out(1,1,"Place your card");
```

Figure 4.2: LCD display source code

4.4.2 Receive data from RFID reader

The main operation that should be done in this project is to receive data from RFID reader, compare it and send the received data wirelessly. Therefore, the data coming in from RFID reader is very important as this will assist to proceed to other operations such as data comparison and data transmission. If data cannot be received from RFID reader, the whole system will not function. Thus, for effectively receive data from the RFID reader; source code shown in Figure 4.3 is used.

```
void read_user(void)
{
 char val;
     val=0x00;
     id = 0x00;
     txt[0]==0x00;
     txt[0] = usart_read();
     if(txt[0]==0x01)
     {
          for(x=1;x<=11;x++)
          {
           txt[x] = usart_read();
          }

          lcd8_chr(2,1,'=');
          for(x=1;x<=10;x++)
          {
           if(txt[x]==' ')
           lcd8_chr_cp('0');
           else
           lcd8_chr_cp(txt[x]);
          }
```

Figure 4.3: C Code to Receive RFID Data

The source code shown above in Figure 4.3 explains that ten characters should be received from the reader where the ten characters represent a code.

4.4.3 Password coding

The opening of the door is success only when the desired password is pressed. Therefore, when the user have placed their card on the reader, the system reads the cards ID and displays it on LCD screen and later on asks for the password. Here the user has to enter the correct password. Once the user has successfully entered the password, the system recognizes the password and unlocks the door. The C code for password is displayed in figure 4.4.

```
delay_ms(3000);
lcd8_Cmd(LCD_CLEAR);
lcd8_out(1,1,"Place Password ");
lcd8_chr(2,1,'=');
for(x=0;x<=3;x++)
{
 pass[x]=read_key();
 lcd8_chr_cp(pass[x]);
 delay_ms(300);
}


 for(x=0;x<=3;x++)
{
 usart_write(pass[x]) ;
}

{
 if(txt[x]==' ')
 Usart_write('0');
 else
 Usart_write(txt[x]);
}
```

Figure 4.4: C code for password detection

4.5 Microsoft Visual Basic

Visual Basic (VB) is a third-generation event-driven programming language and integrated development environment (IDE) from Microsoft for its COM programming model first released in 1991. Visual Basic is designed to be relatively easy to learn and use. Visual Basic was derived from BASIC and enables the rapid application development (RAD) of graphical user interface (GUI) applications, access to databases using Data Access Objects, Remote Data Objects, or ActiveX Data Objects, and creation of ActiveX controls and objects. Scripting languages such as VBA and VBScript are syntactically similar to Visual Basic, but perform differently.

A programmer can put together an application using the components provided with Visual Basic itself. Programs written in Visual Basic can also use the Windows API, but doing so requires external function declarations. Though the program has received criticism for its perceived faults, from version 3 Visual Basic was a runaway commercial success, and many companies offered third party controls greatly extending its functionality.

Microsoft Visual Basic is one of the languages that changes to accommodate the shift. Visual basic is the latest object oriented programming development software for creating applications that run under any of the Microsoft windows environment. The designed screen can holds standard windows button such as command buttons, check boxes, option buttons, text boxes, and etc. Each of these windows object, operates as expected, producing a “standard” windows user interface. It allows user to design a user friendly environment system.

CHAPTER 5

RESULTS AND DISCUSSION

5.1 Introduction

In order to achieve the targeted goal for the project, various tests are conducted in this project. The result of testing shows that the system have achieved substantial goal. Since the system consist of development board and application module, each part is tested independently. Software called Proteus 7 Professional is used to simulate the microcontroller. The simulated microcontroller runs firmware just as in real life and it can interact with large range of peripheral circuit models and powerful debugging tools.

5.2 Software Simulation Results

For the simulation part, circuit diagram was tested in the software part first before proceeding to test it on hardware. For the software testing ISIS 7 Professional software used to get the expected result.

5.2.1 Simulation testing for LCD

For the initial start of the programming testing, LCD was tested using the C coding and simulated using Proteus simulator. The result obtained is shown in figure 5.1 below.

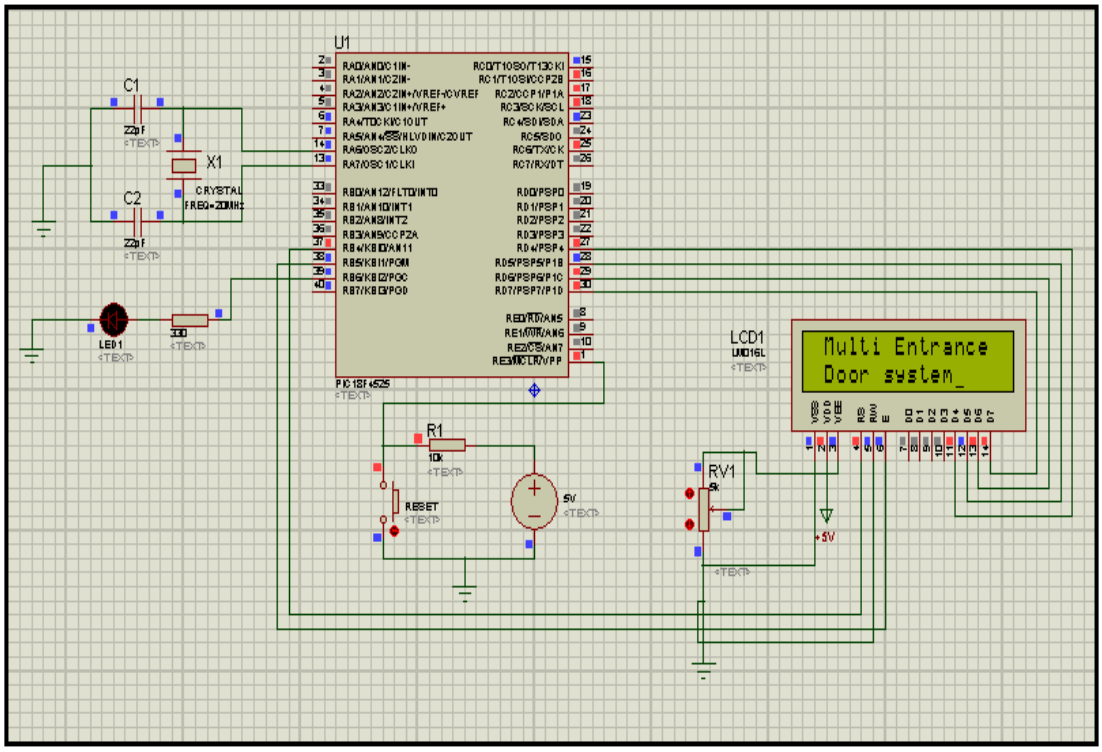


Figure 5.1: LCD testing result

5.2.2 Simulation testing for RFID reader

Figure 5.2 and 5.3 shows the testing done for the RFID reader. The Tx pin of the reader is connected to PIN_C7 which is the receiver pin. For the proteus simulation, the number is typed on the virtual terminal and it is then displayed on the LCD screen. The result obtained is shown below.

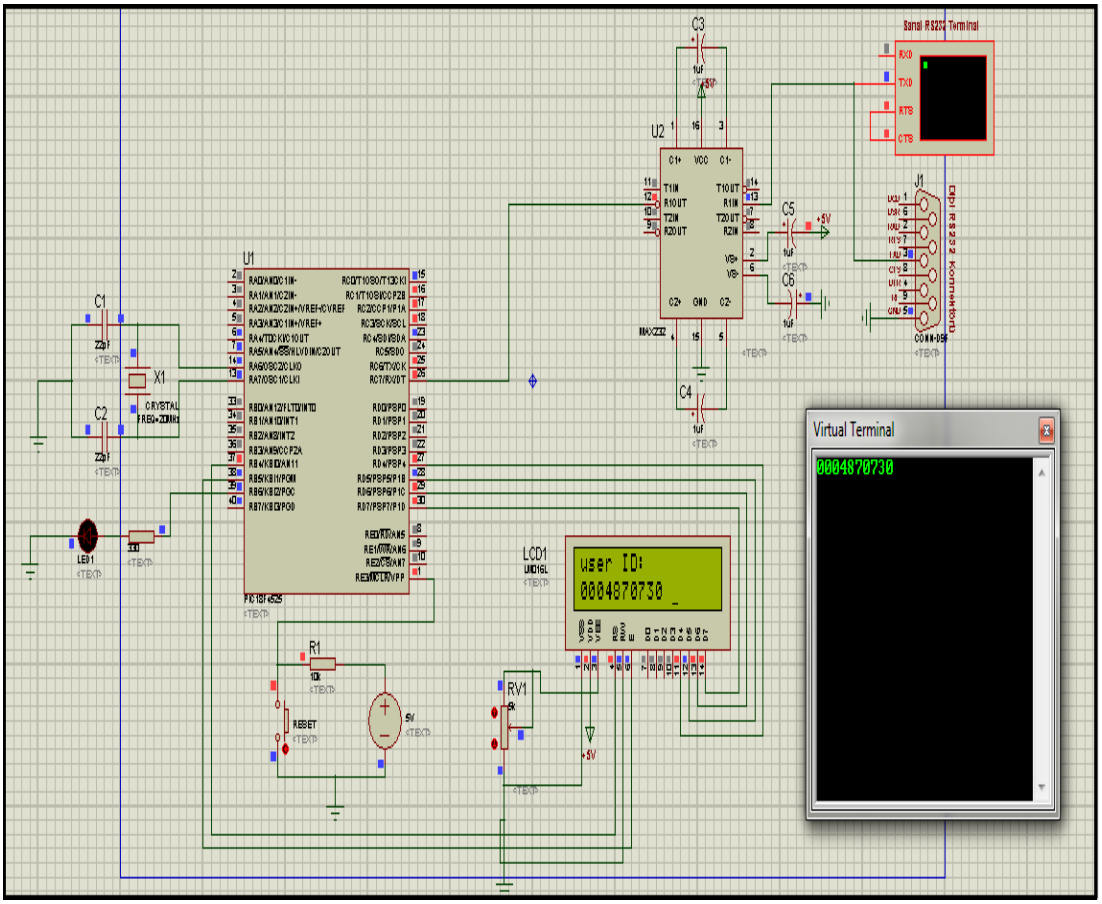


Figure 5.2: RFID reader testing

5.2.3 Simulation testing for Keypad

For the keypad part, the simulation is done for 4x4 matrix keypad. The keypad testing is done to test for the password configuration. Once the password is accepted, the result shows “Access Granted” and LED will light on. The obtained result is shown in figure 5.3 below.

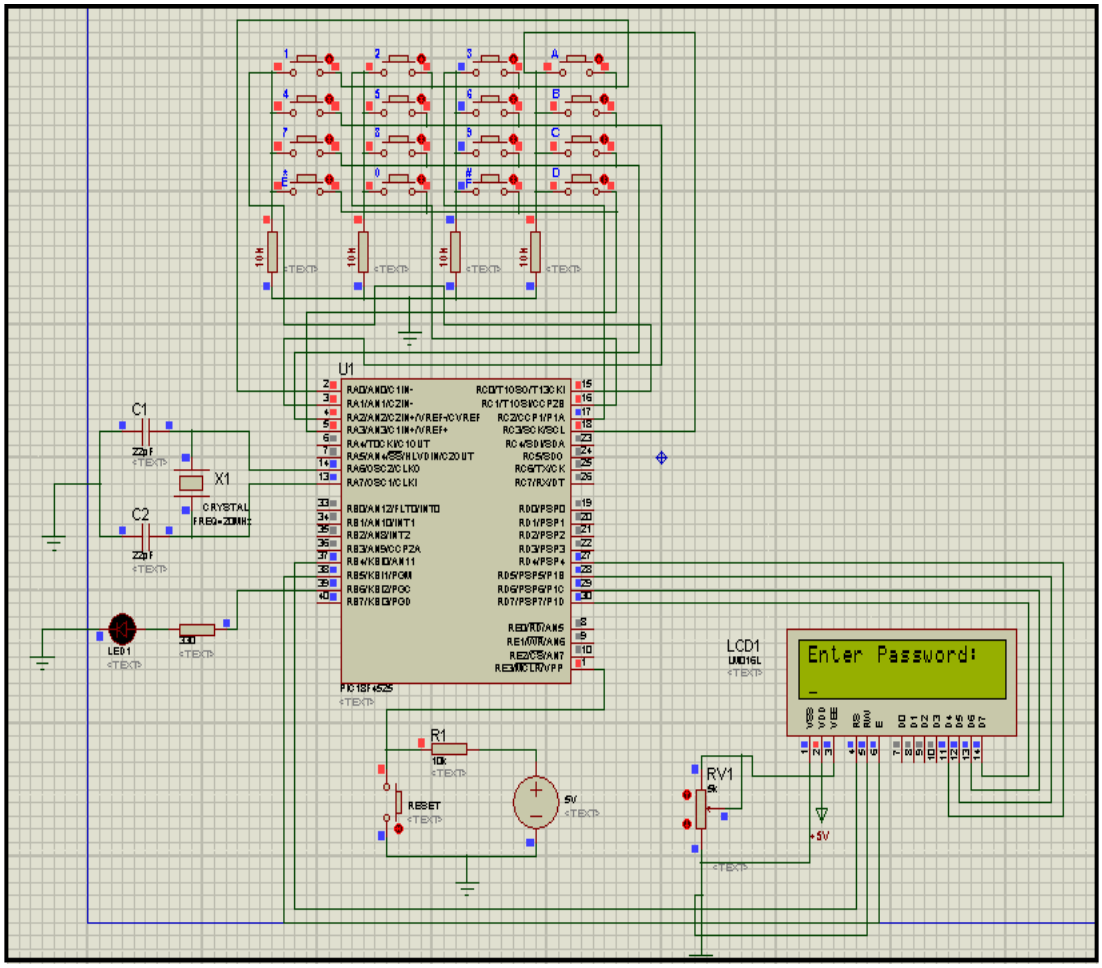


Figure 5.3: Keypad testing

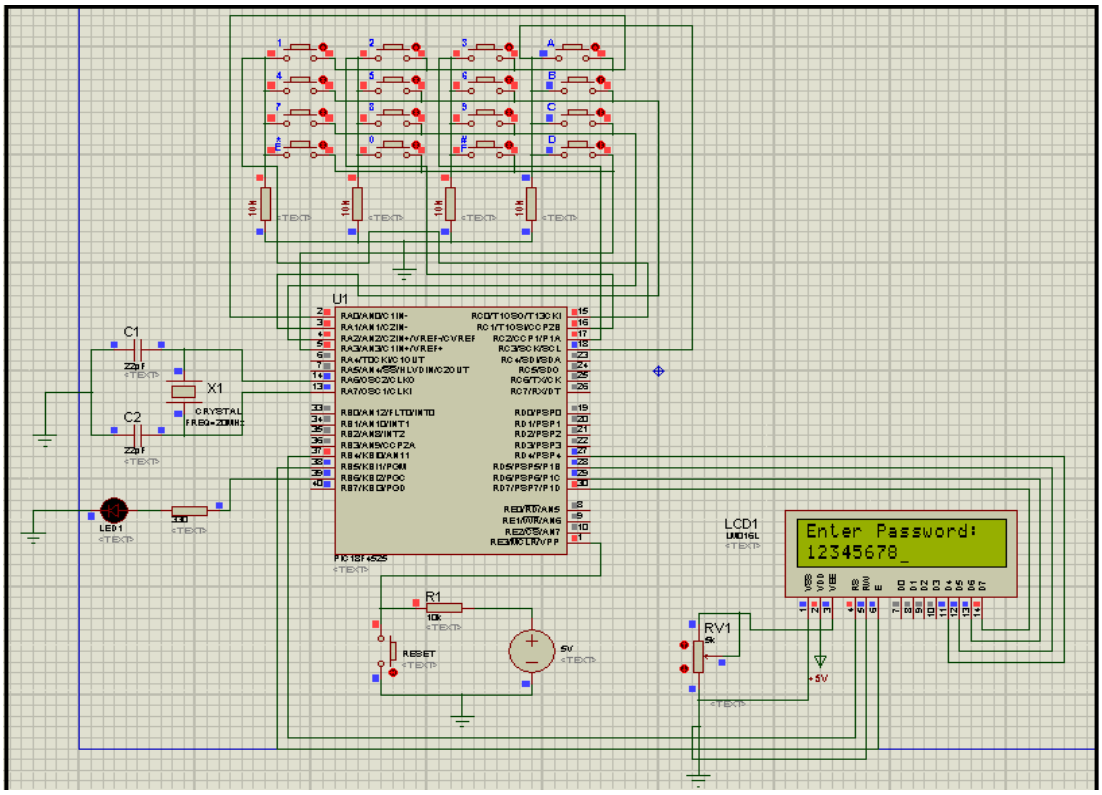


Figure 5.4: Keypad testing

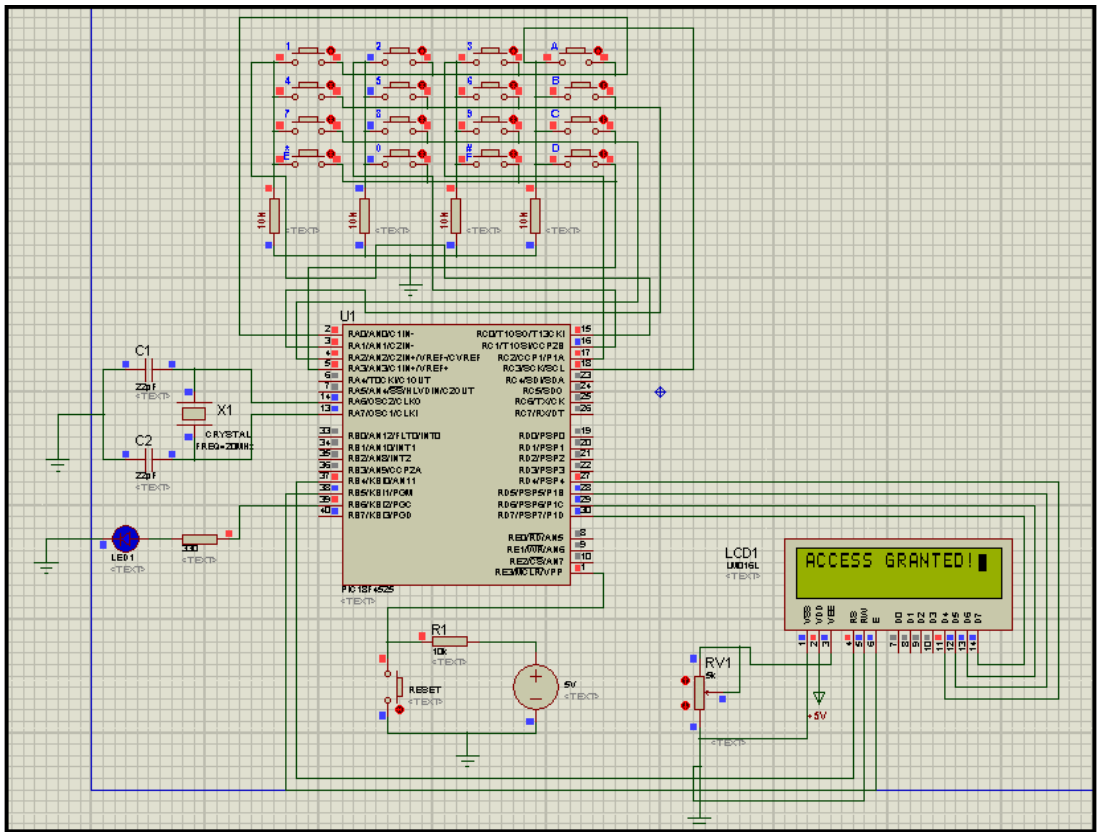


Figure 5.5: Keypad testing

5.2.4 Simulation for overall system

Once all the testing which was done individually is success, the programs were combined to get the desired result. The magnetic door can be opened only when the authorised user tags his/her ID card on the reader and inserts the password right after the scanning of the card. Once both the ID number and password is accepted, the door opens. In Proteus simulation, the magnetic door is represented by the LED.

For the first part when the system is initialized, the LCD display will conduct a user by displaying “WELCOME” as shown in Figure 5.6.

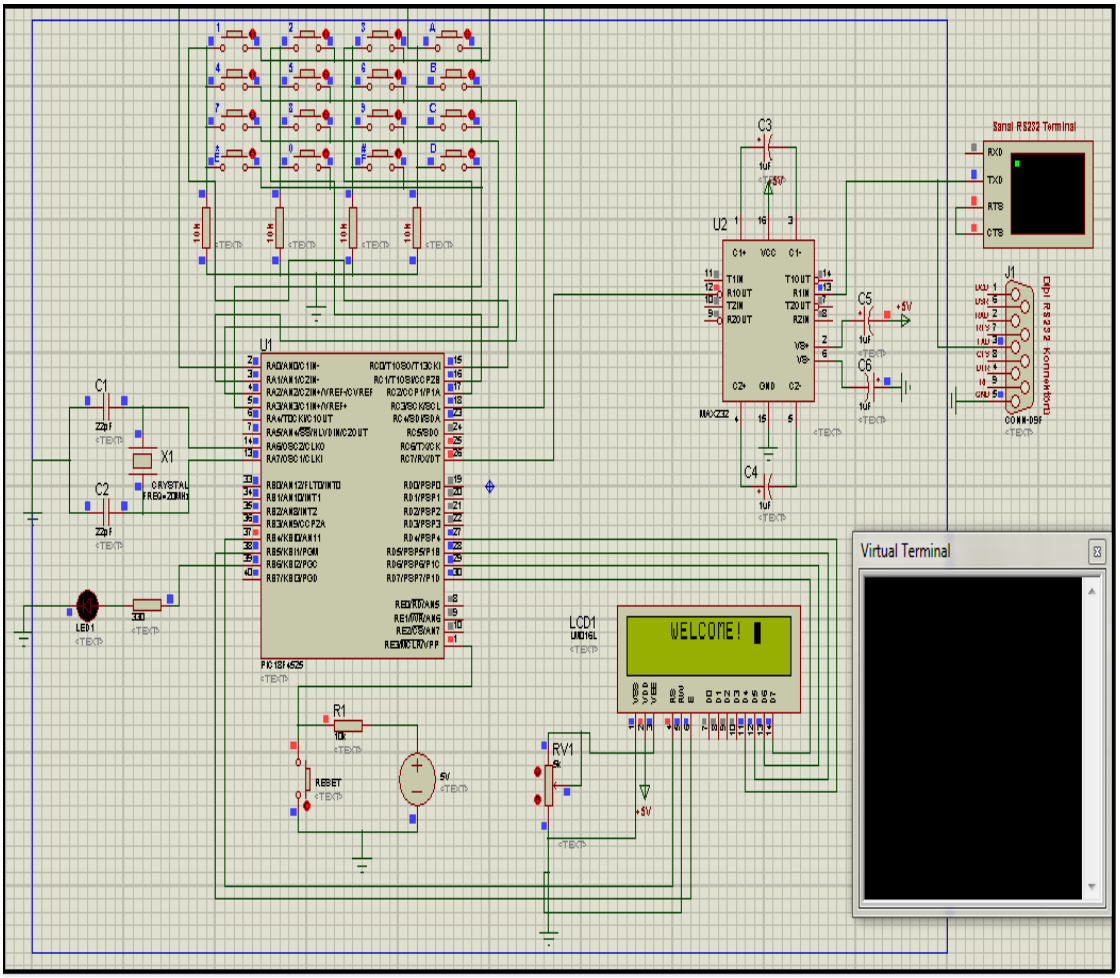


Figure 5.6: “WELCOME” display when system is initialized.

After displaying the welcome message, it will display “Place Your ID on the Reader” as shown in Figure 5.7. As soon as this phrase is displayed, the user has to place his identity card near the RFID reader.

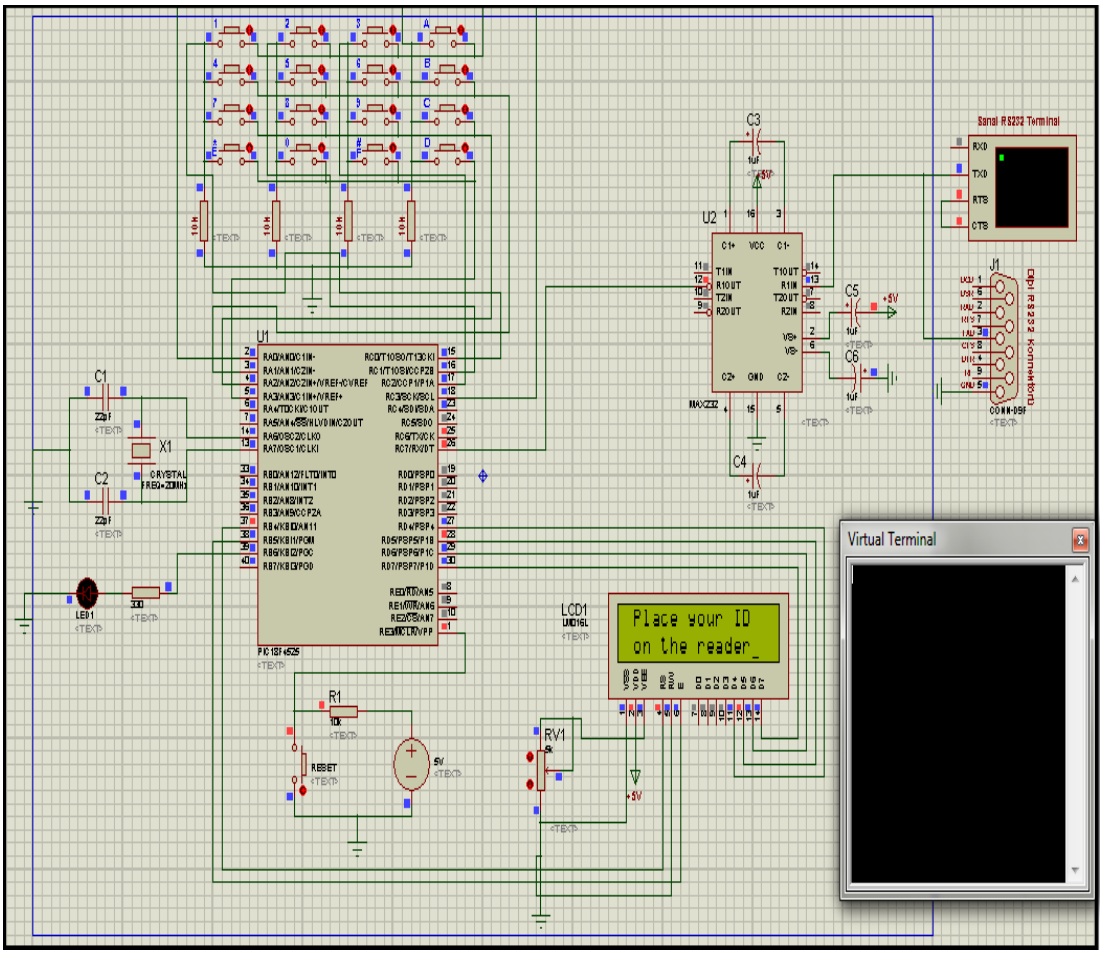


Figure 5.7: Instruction message to tag the ID card

The RFID is represented by a virtual terminal for simulation purposes. Thus, the user will enter the identity cards number into the virtual terminal. After the ID code is inserted, "User ID" and User Name" will be displayed on the LCD display as shown in Figure 5.8 and 5.9.

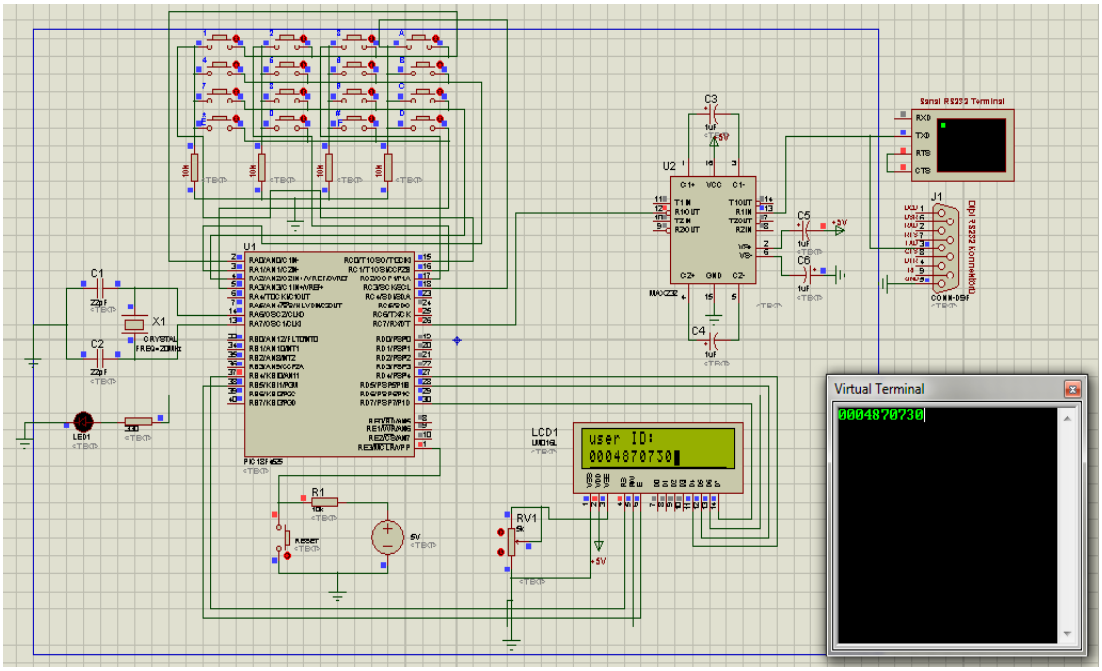


Figure 5.8: Displaying user's ID card number

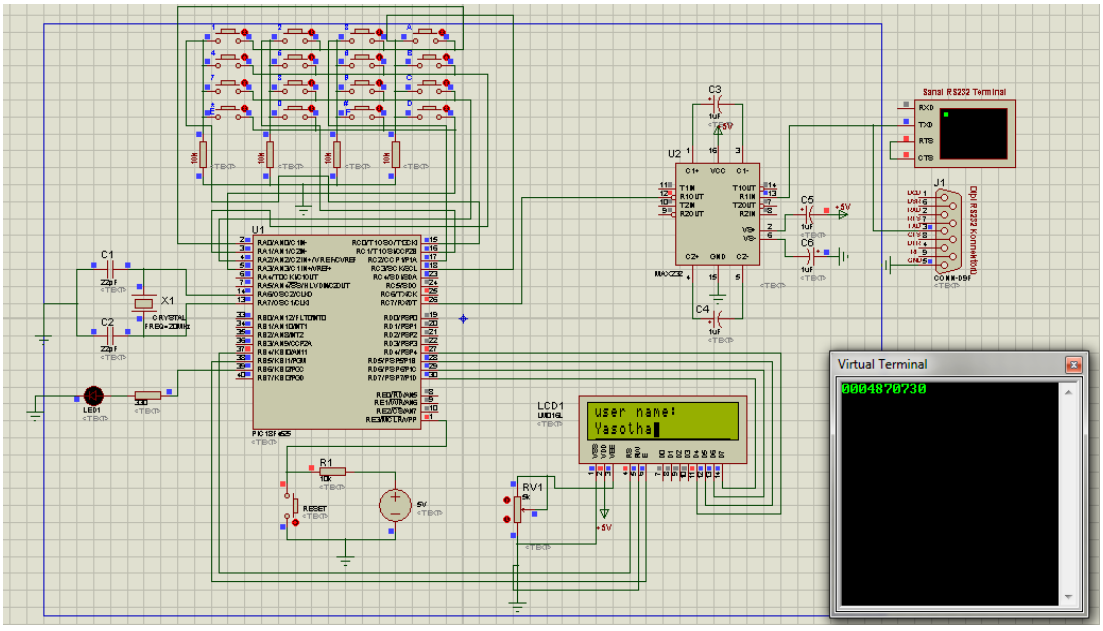


Figure 5.9: Displaying user's name

Once RFID card number is verified next is the verification of password which allows the user to unlock the door. The instruction set to enter the password and user entered password LCD display is shown in Figure 5.10.

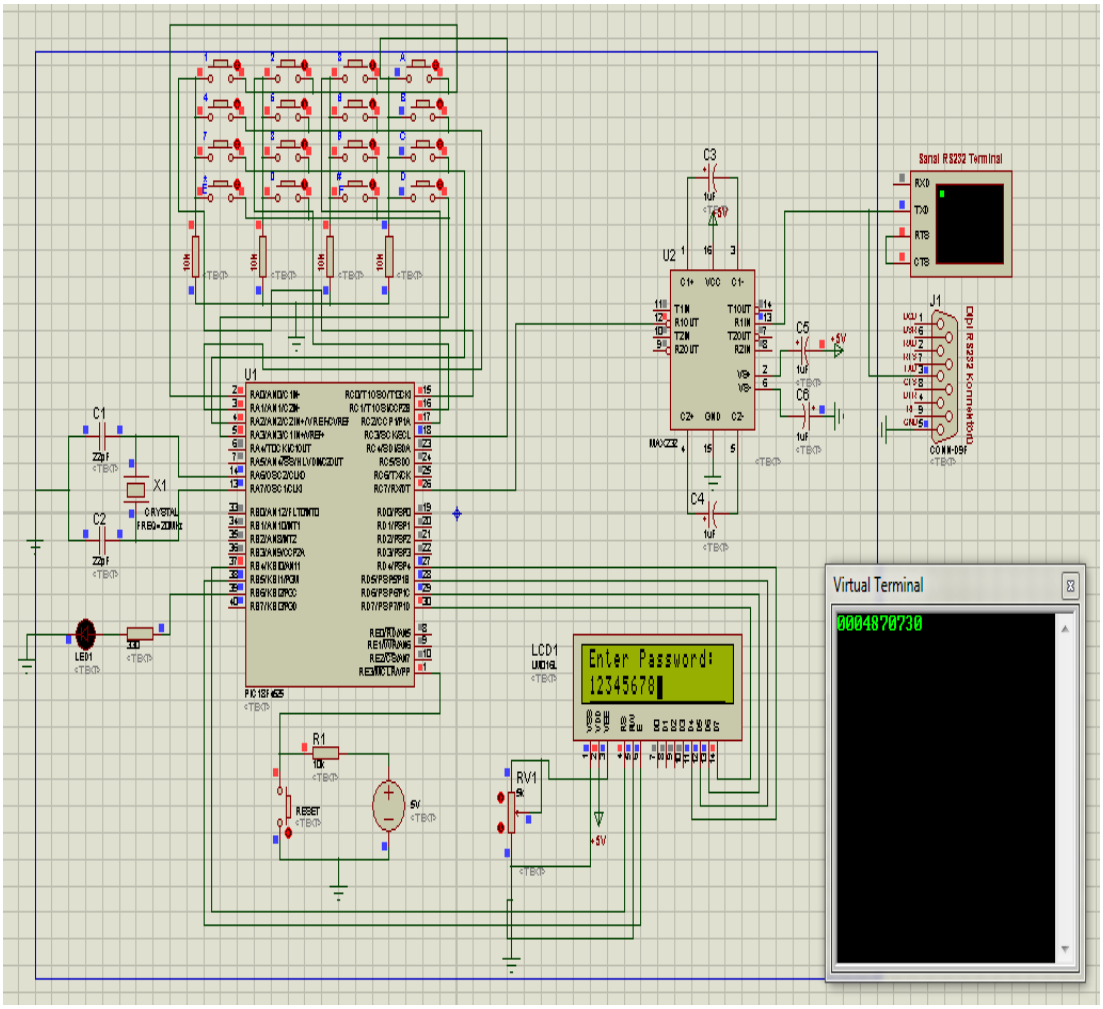


Figure 5.10: Password verification

Once user has entered the correct password, the door is unlocked and the data of the user is sent to central office wirelessly to be saved in database. In this simulation, activation of the door is represented by the LED, where is is active high when the activation is a success. The activation of the door is shown in figure 5.11.

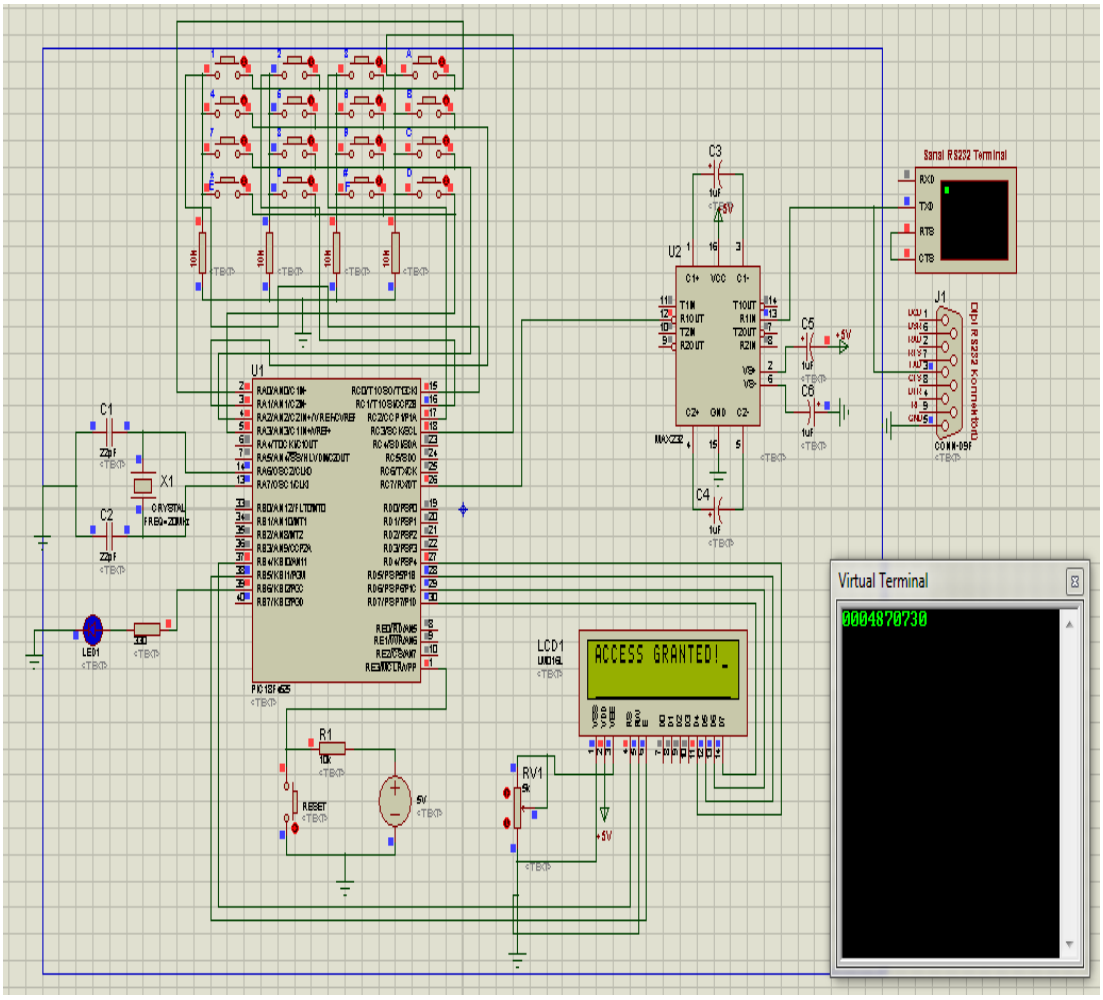


Figure 5.11: Activation to the door access.

5.3 Hardware result of the system

First of all, when the power is on, the system displays the “Place the card” message on the LCD screen. The output is shown in figure 5.12.

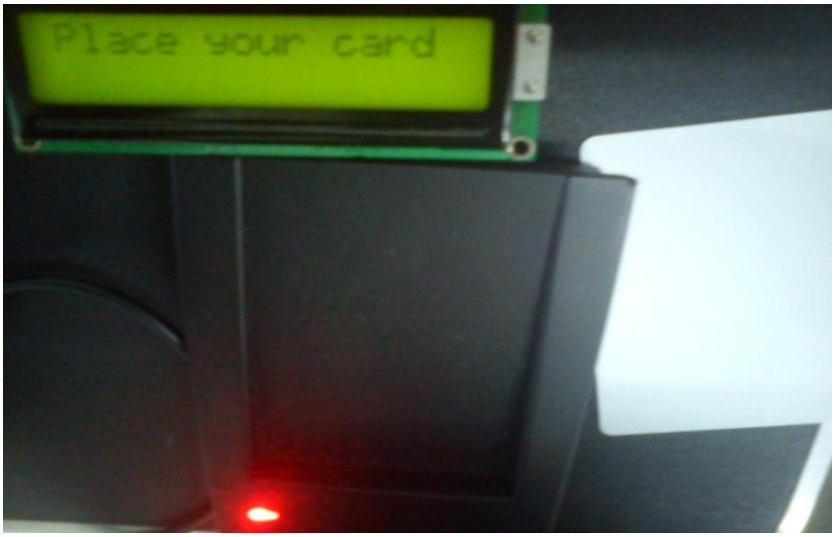


Figure 5.12: Display “Place the card” message

Once the card is detected, the microcontroller identifies the ID number and displays on LCD with the ID number. The result is shown in figure5.13.

Figure5.13: Display User ID number

Next will be the identification of the password where user has to key in the password manually on the keypad in order to access the door. The resultant output is shown in figure 5.14.

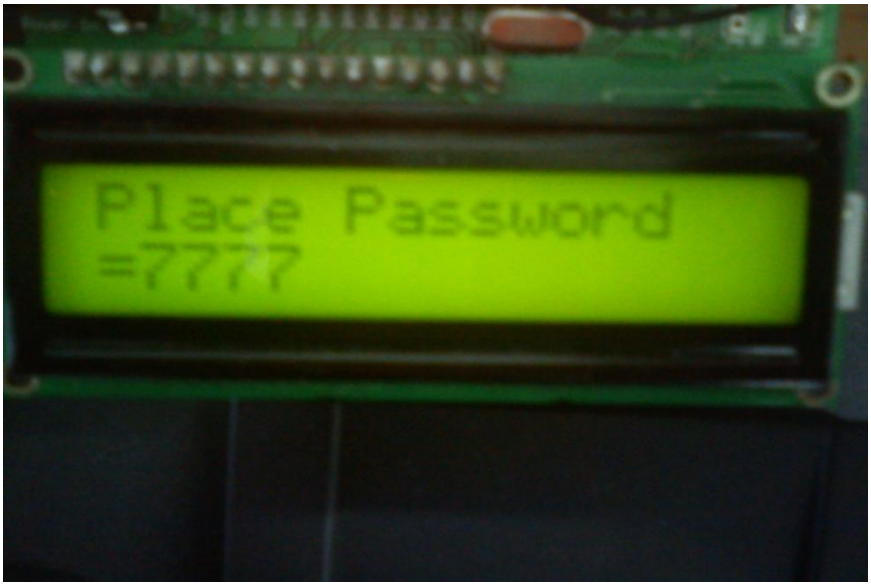


Figure 5.14: Display password

Once the password is valid, the display shows “Open Door” and the buzzer beeps. The door is unlocked when the correct ID code and password is received. The result is shown in figure 5.15.

Figure 5.15: Display “Open Door”

If the user has entered the wrong password, the LCD displays “Error Door” and also the buzzer beeps. The result is shown figure 5.16 & 5.17.

Figure 5.16: Wrong password

Figure 5.17: LCD displays “Error door”

As for the Microsoft visual basic, once the system is switched on, the communication of the both zigbee's have to be connected in order to receive the all the data to be saved on PC. Figure 4.5 shows the system which shows the wireless communication of both zigbee's is connected.

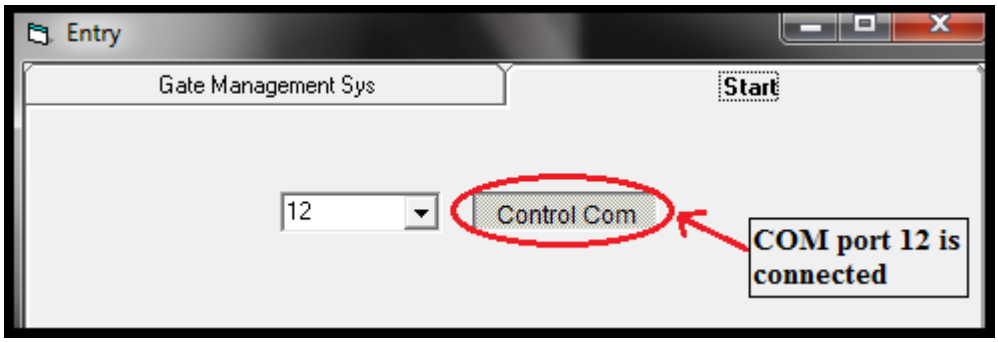


Figure 5.18: Zigbee connected to PC is connected at COM port 12

After the COM port is ON, the next step is for the admin to enter the system. Admin has his/her own ID and password where only authorised person can enter the system. Figure 4.6 shows the result of the administrator's entrance of the system.

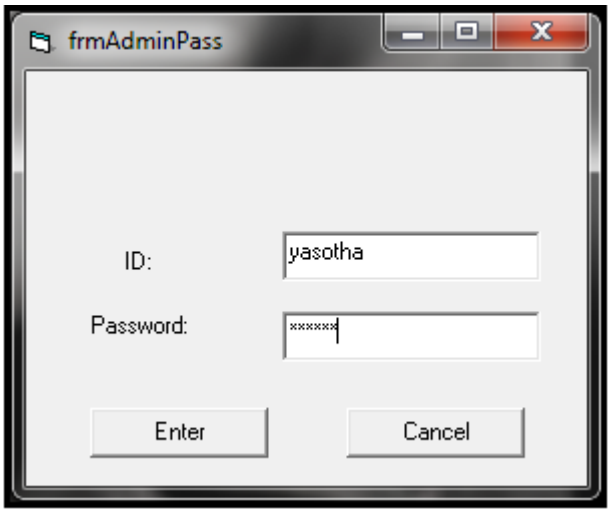


Figure 5.19: Administrator entrance

Once the administrator have entered the system, now the administrator can access to the records of the data has been received by the system. The administrator also can add new employees' record to system as well. Figure 5.20, 5.21 & 5.22 shows the result for employee's data saved in the system and also the recorded attendance data.

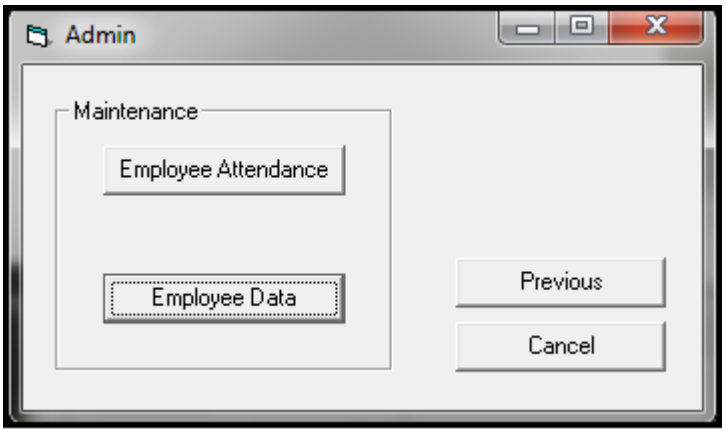


Figure 5.20: Access to Employee data & recorded attendance data

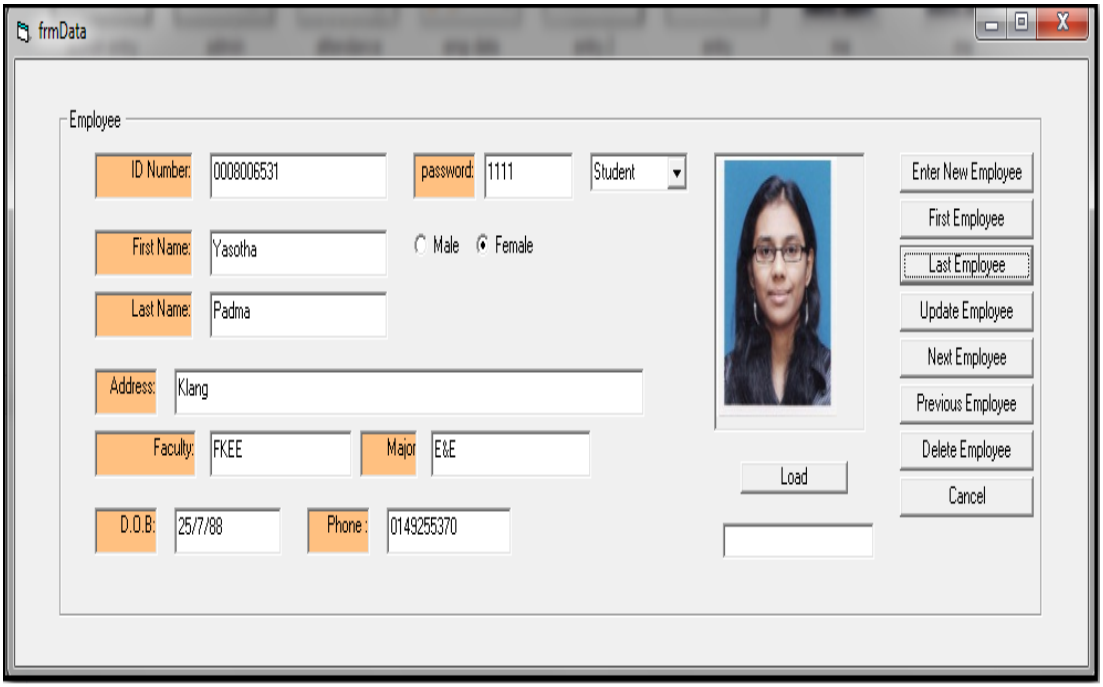


Figure 5.21: Employee data saved in PC

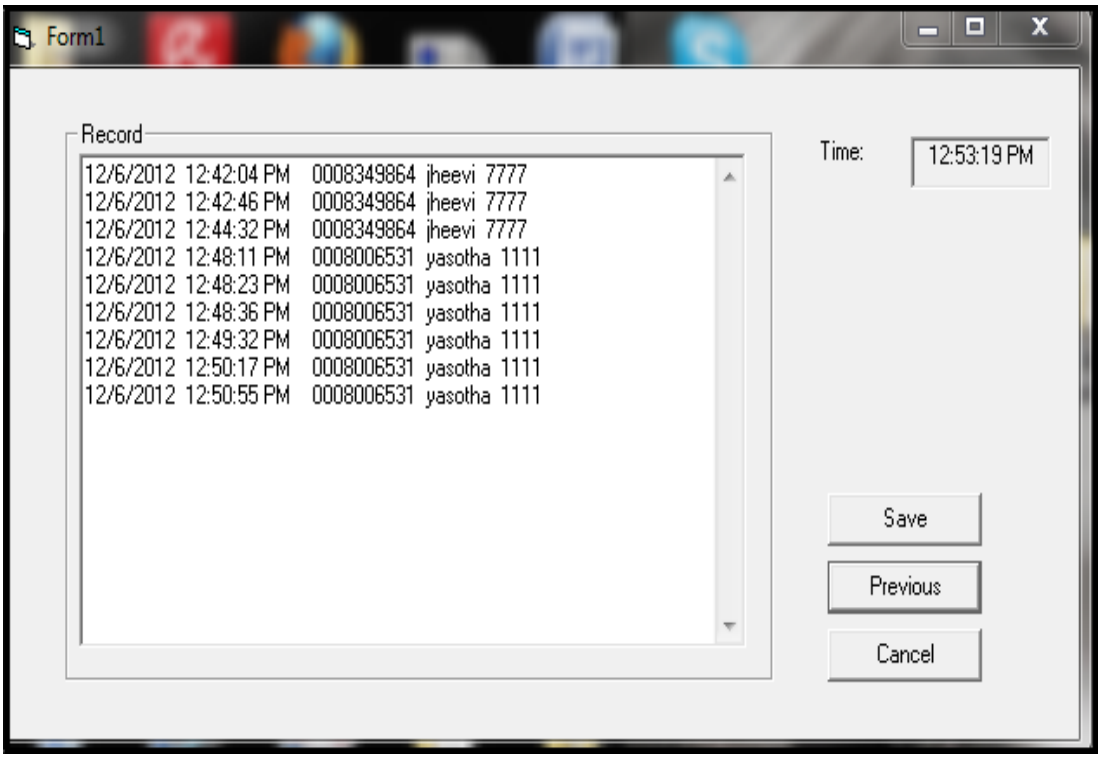


Figure 5.22: Recorded data of who entered the premises.

5.4 Discussion

In this project, two main technologies are used, namely Radio Frequency Identification (RFID) and Xbee Pro Wireless technology. In Radio Frequency Identification (RFID), the RFID reader will read data from RFID tag and displays the identified code on LCD display. The type of tag chosen is the passive RFID tag. Passive RFID tags have no internal power supply. Instead, a small electric current is created in the antenna when an incoming signal reaches it. This current provides enough power to briefly activate the tag, usually just long enough to relay simple information, such as an ID number. Because passive RFID tags do not contain any internal power supply, they can be very small in size, sometimes thinner than a piece of paper. The communication range for the passive RFID tags is very short. As there is no need for long communication range between the reader and the tag, passive RFID tag is chosen.

Xbee Pro wireless module operates at a frequency of 2.4GHz, has a communication range of 1.5km outdoor and 100m indoor. This is much higher than Xbee where it operates at the same frequency of 2.4GHz, but has shorter communication range of 100m outdoor and 30 m indoor. Thus, Xbee Pro is chosen as the wireless medium for data transmission rather than Xbee so that controlling a door is not limited within few hundred meters only.

CHAPTER 6

CONCLUSION

6.0 Conclusion

It can be concluded that all the objectives of this project is partially achieved. The outcome for this project is able to fulfil scope and the expected results are obtained. The Multi-entrances security door system can be implemented in offices and premises where it requires a tight security for their door access. Radio Frequency Identification (RFID) is used for tracing ID numbers. By using the PIC18F4525 microcontroller, the traced ID number and password can be verified and the data's are effectively transmitted through Xbee Pro wireless module. C programming language perfectly assists in receiving data from RFID reader and keypad by comparing the received data and also to transmit the received data.

In this report, fair progress had been obtained, largely in the design and development of the project. The whole of this report serves to bring sufficient knowledge and information regarding design for C programming, circuit design and project's hardware development.

6.2 Recommendations

The Proteus 7 Professional is effective software which simulates microcontroller to run firmware just as in real life and it can interact with peripheral circuits and powerful debugging tools. However Proteus 7 Professional has some limitation, it can't produce noises which occurs in actual hardware's output. Any problem that occurs in hardware might be due to noise in the circuit. Thus, simulation results can be used to as references.

In future development of this project:

i) The operation of the door can also be limited according to time such as operation hour from 7am to 7pm. This can be done by including a real-time clock into the circuit.

ii) Finger print technology and image recognition can be used instead of RFID technology for data identification.

iii) For transmitting data between Xbee Pro wireless modules, data encryption methods such as XTEA encryption method can be used so that data is not lost during transmission.

6.3 Costing and Commercialization

Multi-Entrances Security Door System is a system in which a door in premises can be controlled and accessed by authorised user only due to security purposes. Any occurrence of cases like theft can be easily notified by checking the database for information on who have entered the premises.

The total cost for this Multi-Entrances Security Door System is around RM600. This cost is far cheaper than the development board that exists in the Market. Furthermore the system can be redesigned to suit and meet the user's requirement. In other word, this product has high potential to be commercialized.

REFERENCES

[1] Ying Chen, Yuntao Wang, Xiaokang Li & Li Gao, "**The Design and Implementation of Intelligent Campus Security Tracking System Based on RFID and ZigBee**", Research innovation Fund for College Students of Beijing University of Posts and Telecommunications, Beijing, P.R. China, 2011

[2] Wael Hosny Fouad Aly, Haytham Aboulabbas M., Moustafa H. Aly, Hossam Eldin Moustafa, "**Scalable ZigBee-Based Smart Authentication and Access Control System Design Using XMOS Programmable Chips**". International Journal of Scientific & Engineering Research Volume 2, Issue 9, September-2011.

[3] Liting Cao, Yanxia Liu and Shuo Yang, "**Wireless Networked Security System Based on ZigBee Technology**", College of Automation Beijing Union University Beijing, China, 2008

[4] Aqeel-ur-Rehman, Abu Zafar Abbasi, Zubair A. Shaikh, "**Building A Smart University using RFID Technology**", 2008 International Conference on Computer Science and Software Engineering, Karachi, Pakistan.

[5] Arbab Waheed Ahmad, Naeem Jan, Saeed Iqbal, Chankil Lee, "**Implementation of ZigBee-GSM based Home Security Monitoring and Remote Control system**", 2011.

[6] Gilbert Thio, Tham Kok Foong, Rajparthiban Kumar, L.K. Moey**, "Design of RFID Proximity Security Door Lock",** School of Engineering, UCSI.

[7] P.Suresh, R.Kesavan, "**Design of Dynamic RFID System using 89C51 Microcontroller based Embedded System for Effective Supply Chain Management**", Proceedings of the 2011 International Conference on Industrial Engineering and Operations Management Kuala Lumpur, Malaysia, January 22 – 24, 2011

[8] Inderpreet Kaur (Asstt. Prof.), "**Microcontroller Based Home Automation System With Security",** (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 1, No. 6, December 2010, Mohali, India.

[9] Iv´an Cabrera Altamirano, Francisco Rodr´ıguez Henr´ıquez , "**A Scalable Intelligent Room Based on Wireless Sensor Networks and RFIDs",** 2010 7th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2010) Tuxtla Gutiérrez, Chiapas, México. September 8-10, 2010.

[10] Shi Binbin, Dai Minli, Xu Fengliang, "**Research on Application of RFID System with 2nd-Generation ID card Based on ZigBee Wireless Network",** 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies, Suzhou ,China

[11] Cytron Technologies. "RFID READER"
Available at: *www.cytron.com.my/listProductCategory*

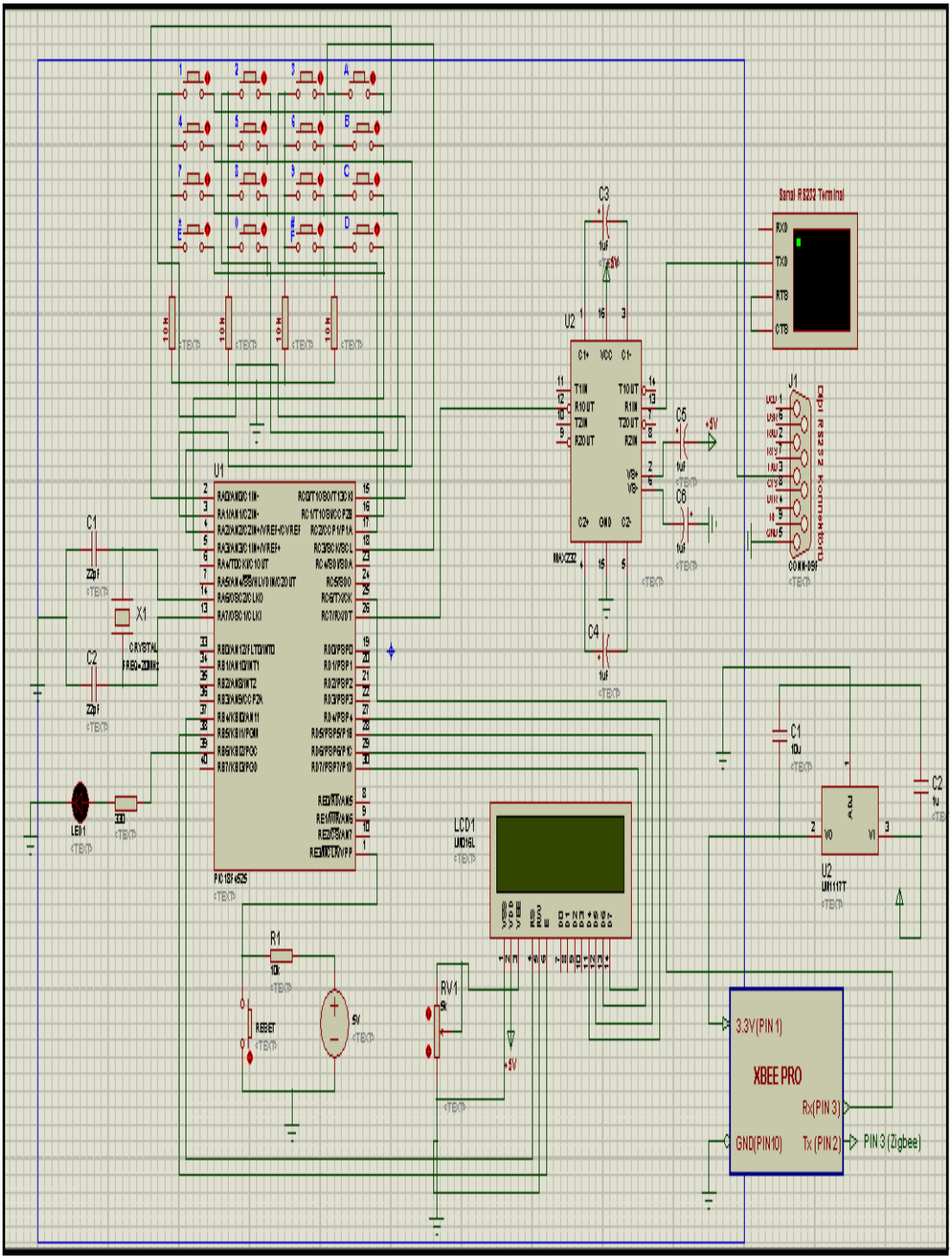
[12] Datasheet PIC18F2525/2620/4525/4620
Available at: *http://ww1.microchip.com/downloads/en/devicedoc/39626b.pdf*

[13] Product Manual Xbee-OEM
Available at: *www.maxstream.net*

APPENDIX A

CIRCUIT – HOST SYSTEM

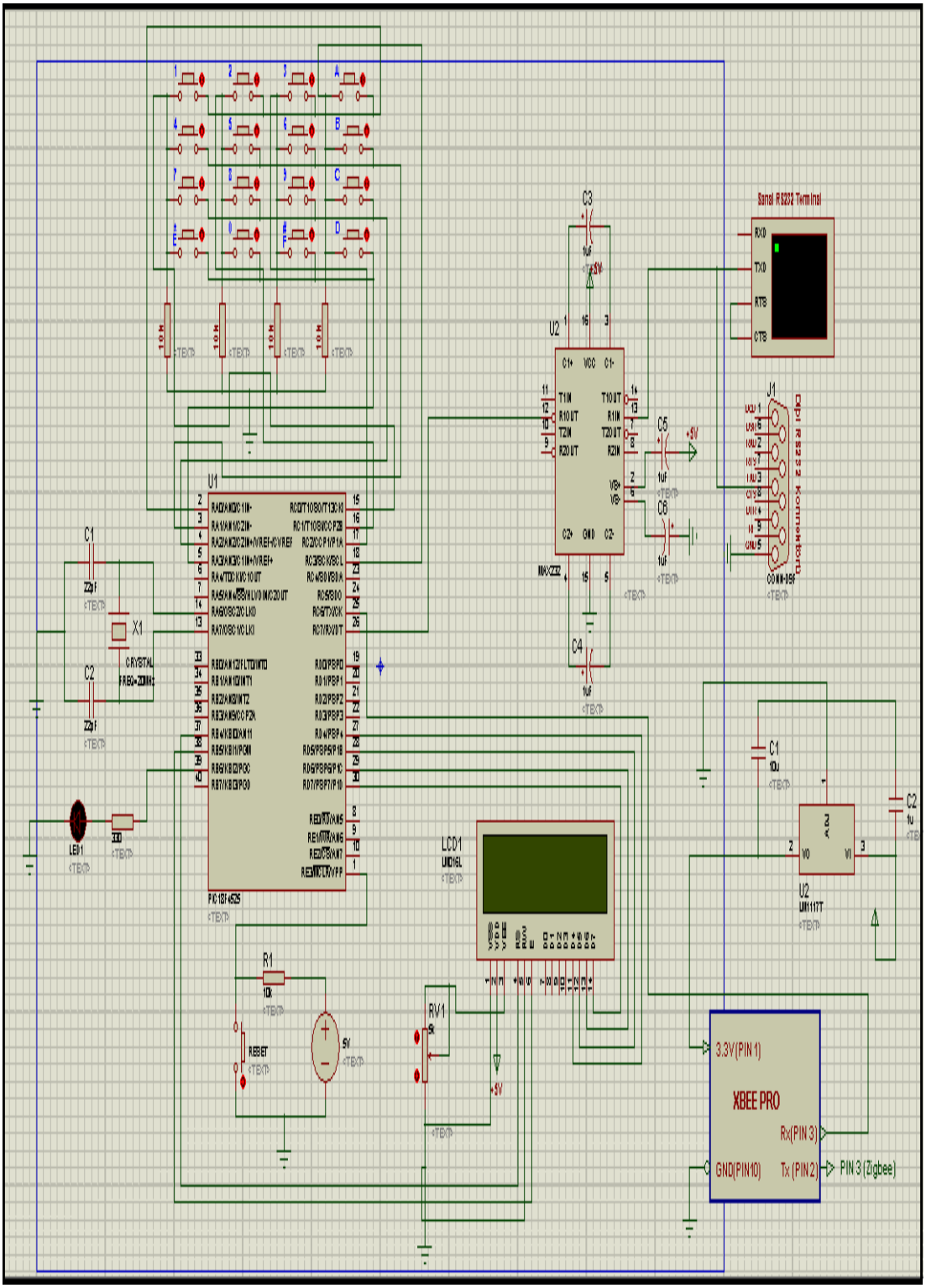
ENTRANCE 1



APPENDIX B

CIRCUIT – HOST SYSTEM

ENTRANCE 2



APPENDIX C

CIRCUIT – SECONDARY SYSTEM