A MINOR PROJECT REPORT

ON

(MODERN WIRELESS ENTRY/EXIT SYSTEM BASED ON RFID AND GSM TECHNOLOGY)

SUBMITTED IN PARTIAL FULFILLMENT FOR THE AWARD OF DEGREE OF

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted By:

RAHUL JOSHI (9915102106)

AMAN MATHUR (9915102094)

FARAZ HUSSAIN (9915102002)

Under the Guidance of

MR. YOGESH KUMAR

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

JAYPEE INSTITUTE OF INFORMATION TECHNOLOGY, NOIDA (U.P.)

NOVEMBER, 2017

CERTIFICATE

This is to certify that the minor project report entitled, "**Modern Wireless Entry/Exit System Based on RFID and GSM Technology**" submitted by **Rahul Joshi, Aman Mathur, Faraz Hussain** in partial fulfillment of the requirements for the award of Bachelor of Technology Degree in **Electronics and Communication Engineering** of the Jaypee Institute of Information Technology, Noida is an authentic work carried out by them under my supervision and guidance. The matter embodied in this report is original and has not been submitted for the award of any other degree.

Signature of Supervisor:
Name of the Supervisor: MR. YOGESH KUMAR
ECE Department,
JIIT, Sec-128,
Noida-201304

Dated:

DECLARATION

We hereby declare that this written submission represents our own ideas in our own words and where others ideas or words have been included, have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission.

Place:

Date:

Name: RAHUL JOSHI
Enrollment: 9915102106

Name: FARAZ HUSSAIN
Enrollment: 9915102002

Name: AMAN MATHUR
Enrollment: 9915102094

ABSTRACT

The main goal of this project is to design and implement a smart wireless entry/exit system based on RFID (Radio Frequency Identification) and GSM technology which can be organized in bank, secured offices and homes. In this system only authentic person can have access through gate. We have implemented a wireless entry/exit system based on RFID and GSM technology containing intruder identification system using RFID and GSM which can activate, authenticate, and validate the user and allow in real time for secure access. The main advantage of using passive RFID and GSM is more secure than Lock-Key and Password Protected System. This system consists of AVR microcontroller, RFID reader, GSM modem, PIR Motion Sensor and LCD. In this system The RFID reader reads the ID number from passive tag and send to the microcontroller, if the ID number is invalid then microcontroller send the SMS to the authenticated person mobile number, to inform the presence of an unauthorized person, if the person forcefully enters, the PIR Motion Sensor detects the presence of someone and the authenticated person receives a SMS using GSM Modem. If the ID number is valid then the user is authorized to get access through the door.

ACKNOWLEDGEMENT

We would like to express our deepest gratitude to all those who have provided us with the possibility to complete this report. A special gratitude to our project mentor, **Mr. Yogesh Kumar**, whose contribution in stimulating suggestions and encouragement has helped us to coordinate our project especially writing this report.

Furthermore we would like to acknowledge with much appreciation the crucial role of the staff of Jaypee Institute of Information Technology, who gave the permission to use all required equipment and the necessary material to complete the task "**Modern Wireless entry/exit system based on RFID and GSM**" and helped us assemble the parts. We have to appreciate the guidance given by other supervisors as well especially in our project presentation that has improved our presentation skills.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

1.1 INTRODUCTION

In this present age, safety has becomes an essential issue for most of the people especially in the rural and urban areas. Some people will try to cheat or steal the property which may endanger the safety of money and other valuable items in the bank, house, and office. To overcome the security threat, a most of people will install bunch of locks or alarm system. There are many types of alarm systems available in the market which utilizes different types of sensor. The sensor can detect different types of changes occur in the surrounding and the changes will be processed to be given out an alert according to the pre-set value. By the same time this system may not be good for all the time. In this project we have implemented safety of the bank locker, house, and office (treasury) by using RFID and GSM technology which will be more secure than other systems. Radio-frequency identification (RFID) based access-control system allows only authorized persons to have access through, with GSM technology. Basically, an RFID system consists of an antenna or coil, a transceiver (with decoder) and a transponder (RF tag) electronically programmed with unique information. There are many different types of RFID systems in the market. These are categorized on the basis of their frequency ranges. The passive tags are lighter and less expensive than the active tags. Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is a common European mobile telephone standard for a mobile cellular radio system operating at 900 MHz In the current work, SIM300 GSM module is used. In this project we have designed and implemented a secure entry/exit based on RFID and GSM technology. In this system only authentic person can have access.

1.2 MOTIVATION

Automated security systems play an important role of providing an extra layer of security through user authentication to prevent break-ins at entry points and also to track illegal intrusions or unsolicited activities within the vicinity of the home (indoors and outdoors).

In today's age of digital technology and intelligent systems, home automation has become one of the fastest developing application-based technologies in the world. The idea of comfortable living in home has since changed for the past decade as digital, vision and wireless technologies are integrated into it. Intelligent homes, in simple terms, can be described as homes that are fully automated in terms of carrying out a predetermined task, providing feedback to the users, and responding accordingly to situations. In other words, it simply allows many aspects of the home system such as temperature and lighting control, network and communications, entertainment system, emergency response and security monitoring systems to be automated and controlled, both near and at a distance.

1.3 Evolution of modern wireless entry exit system

1.3.1 LOCK AND KEY SYSTEM

A warded lock uses a set of obstructions, or wards, to prevent the lock from opening unless the correct key is inserted. The key has notches or slots that correspond to the obstructions in the lock, allowing it to rotate freely inside the lock.

Disadvantage

Warded locks are typically reserved for low-security applications as a well-designed skeleton key can successfully open a wide variety of warded locks.

1.3.2 Password Protected System

A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which is to be kept secret from those not allowed access.

Password Based Door Lock System using Microcontroller, where a secure password will act as a door unlocking system. Traditional lock systems using mechanical lock and key mechanism are being replaced by new advanced techniques of locking system.

Disadvantage

Just as you can forget your keys and be locked out of your home, you can also forget the pass code to access your keyless entry system and be locked out.

One final disadvantage of keyless door locks is that electrically-powered systems may not function properly in the case of a power failure.

1.3.3 Security Systems with Alarms

A security system is a system designed to detect intrusion – unauthorized entry – into a building or other area. Security alarms are used in residential, commercial, and industrial properties for protection against burglary (theft) or property damage, as well as personal protection against intruders.

Disadvantage

False Alarm: These security systems are prone to false alarms that involve the alarm ringing when anyone from your family enters the restricted area. Or there are instances when the alarm is triggered by itself without any reason.

Can be stolen: Irrespective of the type of burglar alarm you have, it can be stolen from the site where it is installed. Wireless systems are comparatively easier to disconnect. Some burglars can easily disconnect the wired alarm systems.

CHAPTER 2

2.1 MICROCONTROLLER

The ATmega8 is a low-power CMOS 8-bit microcontroller based on the AVR RISC architecture. By executing powerful instructions in a single clock cycle, allowing the system designed to optimize power consumption versus processing speed. The AVR core combines a rich instruction set with 32 general purpose working registers. All the 32 registers are directly connected to the Arithmetic Logic Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle. The resulting architecture is more code efficient while achieving throughputs up to ten times faster than conventional CISC microcontrollers.

The ATmega8 provides the following features: 8K bytes of In-System Programmable Flash with Read-While-Write capabilities, 512 bytes of EEPROM, 1K byte of SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible Timer/Counters with compare modes, internal and external interrupts, a serial programmable USART, a byte oriented Two-wire Serial Interface, a 6-channel ADC where four (six) channels have 10-bit accuracy and two channels have 8-bit accuracy, a programmable Watchdog Timer with Internal Oscillator, an SPI serial port, and five software selectable power saving modes. The Idle mode stops the CPU while allowing the SRAM; Timer/Counters, SPI port, and interrupt system to continue functioning.

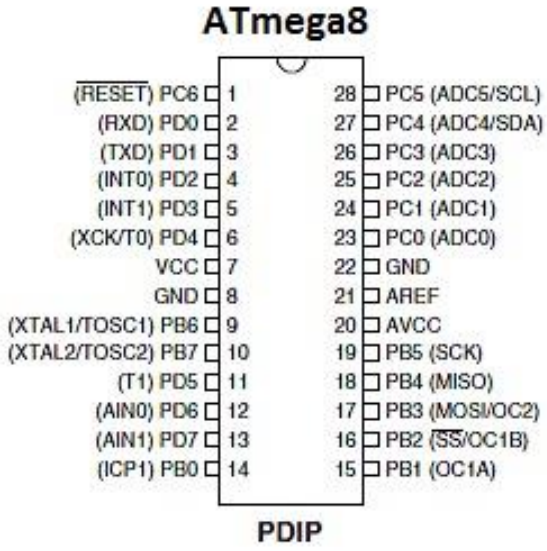

Fig 2.1 Pin Diagram

2.1.1 Pin Descriptions

(a) VCC:

Digital supply voltage.

(b) GND:

Ground.

(c) Port B (PB7-PB0) XTAL1/XTAL2/TOSC1/TOSC2:

Port B is an 8-bit bi-directional I/O port. As inputs, Port B pins that are externally pulled low will source current if the pull-up resistors are activated. Depending on the clock selection fuse settings, PB6 can be used as input to the inverting Oscillator amplifier and input to the internal clock operating circuit. Depending on the clock selection fuse settings, PB7 can be used as output from the inverting Oscillator amplifier. If the Internal Calibrated RC Oscillator is used as chip clock source, PB7.6 is used as TOSC2.1 input for the Asynchronous Timer/Counter2 if the AS2 bit in ASSR is set.

(d) Port C (PC5.PC0):

Port C is an 7-bit bi-directional I/O port. As inputs, Port C pins that are externally pulled low will source current if the pull-up resistors are activated.

(e) PC6/RESET:

If the RSTDISBL Fuse is programmed, PC6 is used as an I/O pin. Note that the electrical characteristics of PC6 differ from those of the other pins of Port C. If the RSTDISBL Fuse is unprogrammed, PC6 is used as a Reset input. A low level on this pin for longer than the minimum pulse length will generate a Reset, even if the clock is not running. Shorter pulses are not guaranteed to generate a Reset.

(f) Port D (PD7-PD0):

Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). As inputs, Port D pins that are externally pulled low will source current if the pull-up resistors are activated.

(g) RESET:

Reset input. A low level on this pin for longer than the minimum pulse length will generate a reset, even if the clock is not running.

(h) AVCC:

AVCC is the supply voltage pin for the A/D Converter, Port C (3-0), and ADC (7-6). It should be externally connected to VCC, even if the ADC is not used. If the ADC is used, it should be connected to VCC.

(i) AREF:

AREF is the analog reference pin for the A/D Converter.

(j) ADC (7-6) :

ADC (7-60) serves as analog inputs to the A/D converter.

2.2 RFID (Radio Frequency Identification) Technology:

2.2.1 What is RFID?

RFID is short for Radio Frequency Identification. RFID is a technology which is working on radio waves. Generally a RFID system consists of 2 parts. A Reader, and one or more Transponders, also known as Tags. RFID systems evolved from barcode labels as a means to automatically identify and track products and people. You will be generally familiar with RFID systems as seen in:

- **Access Control:** RFID Readers placed at entrances that require a person to pass their proximity card (RF tag) to be "read" before the access can be made.
- **Contact less Payment Systems:** RFID tags used to carry payment information. RFID's are particular suited to electronic Toll collection systems. Tags carried by people transmit payment information to a fixed reader attached to a Toll station. Payments are then routinely deducted from a users account, or information is changed directly on the RFID tag.
- **Product Tracking and Inventory Control:** RFID systems are commonly used to track and record the movement of ordinary items such as library books, clothes, electrical goods and numerous items.

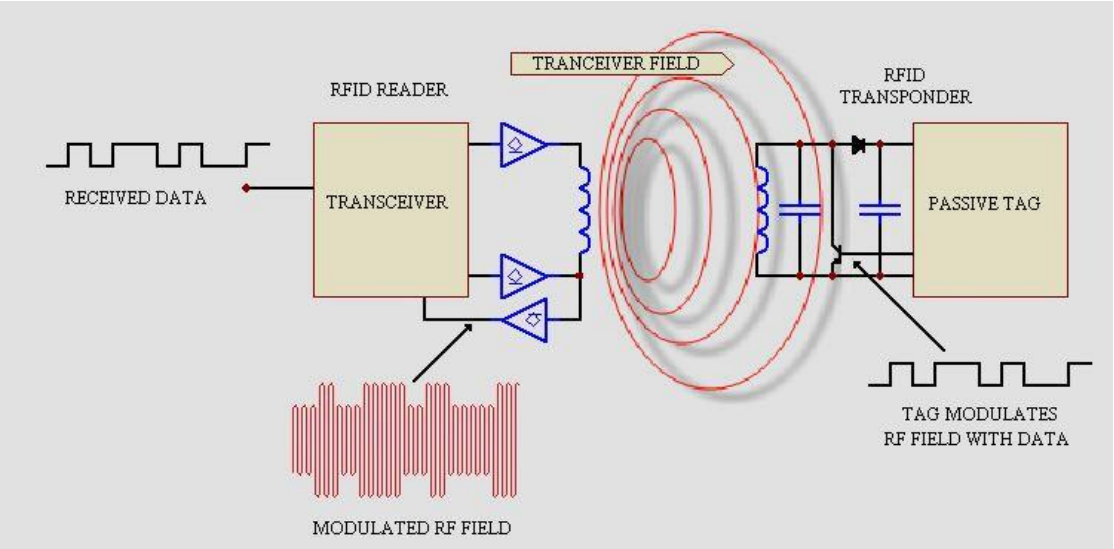

Fig 2.2 RFID System

2.2.2 How do RFID's work?

Basically, an RFID system consists of an antenna or coil, a transceiver (with decoder) and a transponder (RF tag) electronically programmed with unique information. There are many different types of RFID systems in the market. These are categorized on the basis of their frequency ranges. Basically, an RFID system consists of three components: an antenna or coil, a transceiver (with decoder) and a transponder (RF tag) electronically programmed with unique information. An RFID reader is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data. An RFID tag is a microchip combined with an antenna in a compact package; the packaging is structured to allow the RFID tag to be attached to an object to be tracked. "RFID" stands for Radio Frequency Identification. The tag's antenna picks up signals from an RFID reader or scanner and then returns the signal, usually with some additional data (like a unique serial number or other customized information). A passive tag is an RFID tag that does not contain a battery, the power is supplied by the reader. When radio waves from the reader are encountered by a passive RFID tag, the coiled antenna within the tag forms a magnetic field. The tag draws power from it, energizing the circuits in the tag. The tag then sends the information encoded in the tag's memory. The RX and TX pins of RFID reader connected to Tx and Rx pins of ATmega8 Microcontroller respectively. Then the reader senses the data from the Tag and transmits the sensed data to microcontroller via serial port.

Shown in fig 2.2 is a typical RFID system. In every RFID system the transponder Tags contain information. This information can be as little as a single binary bit, or be a large array of bits representing such things as an identity code, personal medical information, or literally any type of information that can be stored in digital binary format. Shown is a RFID transceiver that communicates with a passive Tag. Passive tags have no power source of their own and instead derive power from the incident electromagnetic field. Commonly the heart of each tag is a microchip. When the Tag enters the generated RF field it is able to draw enough power from the field to access its internal memory and transmit its stored information. When the transponder Tag draws power in this way the resultant interaction of the RF fields causes the voltage at the transceiver antenna to drop in value. This effect is utilized by the Tag to communicate its information to the reader. The Tag is able to control the amount of power drawn from the field and by doing so it can modulate the voltage sensed at the Transceiver according to the bit pattern it wishes to transmit.

2.3 GSM

GSM, stands for Global System for Mobile Communication. It is very compact in size and easy to use as plug in GSM Modem with a simple to interface serially. Use it to send SMS, make and receive calls, and do other GSM operations by controlling it through simple AT commands from micro controllers and computers. It uses the highly popular SIM300 module for all its operations. It comes with a standard RS232 interface which can be used to easily interface the modem to micro controllers and computers.
The modem consists of all the required external circuitry required to start experimenting with the SIM300 module like the power regulation, external antenna, SIM Holder, etc.

Features:

1. Provides the industry standard serial RS232 interface for easy connection to computers, microcontrollers and other devices
2. Power, RING and Network LEDs for easy debugging
3. Can be used for GSM based Voice communications
4. Can be controlled through standard AT commands
5. Comes with an onboard wire antenna for better reception

6. The SIM300 allows an adjustable serial baud rate from 1200 to 115200 bps (9600 default)
7. Operating Voltage: 9V

Following AT commands we are using in the program:

1. AT

   To check whether modem is working properly or not.
2. ATE0

   When the board is reset, configuration changes from the last session are loaded.
3. AT+CMGF

   Select SMS format.
4. AT+CMGS

   Send SMS Message To Given Number.

CHAPTER 3

3.1 GENERAL ARCHITECTURE

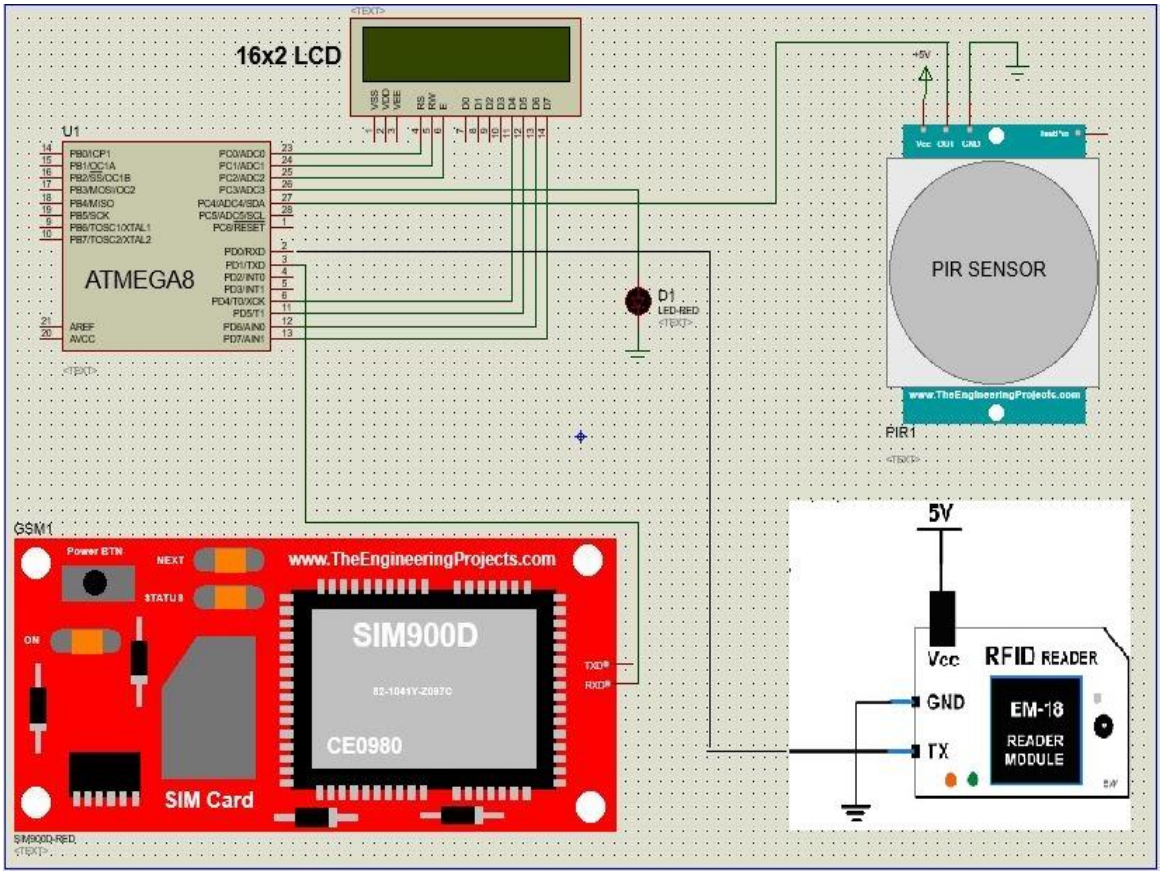

Fig 3.1 Schematic Diagram

The proposed general architecture incorporates subsystems PIR sensor, GSM module, RFID reader into a single automated architecture for practical implementation in intelligent home environments. The figure shows a simple architecture diagram of the proposed system and its setup and connectivity. The modules work independently and parallel but share computational resources.

3.2 WORKING

RFID based security system using ATmega 8 has a RFID reader attached to it. RFID reader reads the unique alphanumeric code of RFID tags and sends it to ATmega 8. Then ATmega 8 detects whether RFID card is valid or invalid. If the card is invalid and PIR

sensor detects motion then system turns on the buzzer and sends SMS to the authorized person's mobile number. However, if the RFID card shown by the user is valid and PIR sensor detects motion then the electrical appliances are turned on. But, in case, a card is not detected and PIR sensor detects motion then it turns on the buzzer and an SMS is sent to the authorized person's mobile number. And if PIR sensor detects no presence then no action is taken even though the card is valid or invalid.

3.2.1 Sensory System: It consists of various sensors like PIR sensors for detecting human presence for granting access. It is also possible to add temperature sensors, camera and other sensing devices for improving the security of homes. These sensing values are sent to the microcontroller with intermediate circuitry like Analog to Digital Converter (ADC).

3.2.2 Microcontroller: This is the heart of the system wherein central processing of data takes place. ATmega 8 microcontroller collects the data or information from various sensors and compares it with appropriate prescribed limits. It is programmed by embedded C or assembly language. By receiving the sensor signals, it takes the corresponding course of action by sending commands to the output devices.

3.2.3 GSM Modem: GSM modem allows the computer to communicate over the mobile network through calls, SMS and MMS messages. It consists of a SIM card and operates over a subscription through a mobile network. It is a highly flexible plug-and-play device capable of connecting to a PC.

3.2.4 Final Control Devices: These devices include buzzers and motors with driver ICs and LCDs display. Final control devices generate alarms of different kinds by using buzzers; doors operations are controlled by using motors. All these devices act upon the commands directed from a microcontroller.

3.3 Working Code

```
#define F_CPU 8000000UL

#include<avr/io.h>

#include<stdio.h>
```

```
#include<util/delay.h>
#include<string.h>
int x=0,i=0,k=0,j=0;
char card1[]="02003ED7F318";
char card[];
char msg1[]="PLACE UR CARD";
char msg2[]="ACCESS GRANTED";
char msg3[]="ACCESS DENIED";
char msg4[]="WELCOME";
char msg5[]="GSM INITIALISED";
char msg6[]="MSG SENT";
void lcd_command(unsigned char cmd)
{
        PORTD = (cmd & 0xF0);           //MSB
        PORTC |= 0b00000100;            //en=1
        _delay_ms(1);
        PORTC &= 0b11110000;            //en=0
       _delay_ms(1);
       PORTD = ((cmd<<4) & 0xF0);       //LSB
       PORTC |= 0b00000100;             //en=1
        _delay_ms(1);
        PORTC &= 0b11110000;            //en=0
}
void lcd_data(unsigned char da)
{
        PORTD = (da & 0xF0);            //MSB
        PORTC |= 0b00000101;            //en=1
        _delay_ms(1);
```

```
        PORTC &= 0b11110001;            //en=0
        _delay_ms(1);
        PORTD = ((da<<4) & 0xF0);       //LSB
        PORTC |= 0b00000101;            //en=1
        _delay_ms(1);
        PORTC &= 0b11110001;            //en=0
}
void lcd_init()
{
        lcd_command(0x02);
        lcd_command(0x60);
        lcd_command(0x28);
        lcd_command(0x0C);
}
void lcd_string(unsigned char a[])
{
        while(a[i]!='\0')
        {
                lcd_data(a[i]);
                i++;
        }
}
void usart_init()                       //Usart initialisation transmission and receiving
{
        UBRRL=51;
        UCSRB=UCSRB|(1<<RXEN)|(1<<TXEN);
        UCSRC=UCSRC|(1<<URSEL)|(1<<UCSZ1)|(1<<UCSZ0);
}
```

```
void getcard_id(void)                    //Function to get 12 byte ID no. from rfid card
{
        for(i=0;i<12;i++)
        {
                card[i]= usart_getch();          // receive card value byte by byte
        }
}
int usart_getch()
{
while ((UCSRA & (1 << RXC)) == 0);       // Do nothing until data has been received
return(UDR);                             // return the byte
}
void pir_home()
{
        if(PINC==0b00010000)
        {
                PORTC=0b00001000;
        }
}
void pir_theft()
{
        if(PINC==0b00010000)
        {
                gsm();
        }
}
void gsm()
{
```

```
        putsf("AT");
       enter();
      _delay_ms(100);
      _putsf("ATE0");                              //the board is reset
      enter();
      _delay_ms(100);
      putsf("AT+CMGF=1");                          //select sms format
      enter();
      _delay_ms(100);
      putsf("AT+CNMI=1,1,0,0,0");
      enter();
      _delay_ms(100);
      putsf("AT+CMGS=\"08619615585\"");      //Send SMS Message To Given Number
      enter();
      _delay_ms(100);
       putsf("Alert!");                             //Message to be Sent
       enter();
      _delay_ms(100);
}
int main(void)
{
        DDRC=DDRC|(1<<1)|(1<<0)|(1<<2)|(1<<3);        //LCD_DATA port as output
        DDRD= 0xF0;
        lcd_init();                                   //initialization of LCD
        _delay_ms(50);                                // delay of 50 milliseconds
        usart_init();                                 // initialization of USART
        while(1)
        {
```

```
            lcd_command(0x80);                  //cursor on 1st line
            lcd_string(msg4[]);                 //Function to display string on LCD
            _delay_ms(100);                     //cursor on 2nd line
            lcd_command(0xC0);
            lcd_string(msg5[]);
            lcd_command(0x80);
            lcd_string(msg1[]);
            getcard_id();                       //Function to get RFID card no.
            if(strcmp(card1,card)==0)           //check whether card matched
            {
                  lcd_command(0x80);            //cursor on 1st line
                  lcd_string(msg2[]);
                  pir_home();
      }

            else                                //card does not match
            {
                  lcd_command(0x80);
                  lcd_string(msg3[]);
                  pir_theft();
                  lcd_command(0x80);
                  lcd_string(msg6[]);
            }
      }
      return 0;
}
```

CHAPTER 4

4.1 CONCLUSIONS

We have implemented a Bank locker security system using passive RFID and GSM. It is a low cost, low in power conception, compact in size and standalone system. The GSM based home security system has been designed and tested with the mobile network. A flexible way to control explore the services of the mobile, AT commands is used in the system. The communication of home is only through the SMS which has been tested with the mobile networks and is working on any mobile network. The system has tested on the model of smart home and further it will be tested in actual home. The complexity of the algorithm of the system can be increased by introducing number of sensors to make the energy efficient home.

4.2 ADVANTAGE

1. RFID Tag detection not requiring human intervention reduces employment costs and eliminates human errors from data collection.
2. As no line-of-sight is required, tag placement is less constrained.
3. RFID tags have a longer read range than barcodes.
4. Remote indication: With the use of GSM technology owner of the house or industry get remote indication through SMS. So even if the user is away from home or industry, he/she will be intimated about the hazardous or undesirable conditions / situations inside the house.
5. This system is Cost effective. Also it is Fast and efficient.
6. Easy to install.
7. Power Saving: As electrical appliances will only turned on when someone is present inside the house, otherwise are switched off.
8. No typical password has to be remembered.

4.3 FUTURE SCOPE

1. Door-screening process

A lot of theft would be eliminated if every person who knocked on your door or rang your doorbell had to provide proper identification. The security industry already has motion-activated cameras, and even ones that you can speak through, but sometimes cameras fail to properly identify suspects, especially if the thieves are wearing a mask or disguise. In the future, it would be nice to have system where a visitor had to provide more information about themselves at the door, whether that's providing a fingerprint or having their retinas scanned. This may seem overkill, but I would love it if my door took people's fingerprints and would announce who's at the door while I sat on the couch and avoided solicitors. Plus, the technology already exists and just needs to be effectively implemented into widespread and cost-efficient home security systems.

2. Motion sensors that know you

There are already pet-immune motion sensors that can tell the difference between an intruder and your pet, based on the amount of heat each entity radiates. But wouldn't it be awesome if your motion detectors could not only tell the difference between an intruder and your pet, but also the difference between individual members of your family? Maybe you want to be notified when your child opens a medicine cabinet, but you don't want to be bothered with an alert if your spouse opens it. If sensors could actually identify individual people, then you could save a lot of stress and false alarms.

3. Facial recognition software

Along the same lines of getting proper identification at the door, it would be cool to have cameras with built-in facial recognition software. That way, not only could your camera take footage of an intruder, but it could cross-reference that face with Facebook and Google+ profiles and police mug shots to instantly identify the culprit. It's not too far off from an article in "The New York Times" that describes a burglar who was caught on video and then positively identified with help from the pictures on his Facebook profile.

4. Two Step Verification through OTP

In this system The RFID reader reads the id number from passive tag and send to the microcontroller, if the id number is valid then microcontroller send the SMS request to the authenticated person mobile number, for the original password to open the bank locker, if the person send the password to the microcontroller, which will verify the passwords entered by the key board and received from authenticated mobile phone. if these two passwords are matched the locker will be opened otherwise it will be remain in locked position, This system is more secure than other systems because two passwords required for verification.

REFERENCES

[1] Muhammad Ali Mazidi, “Book on AVR microcontroller and Embedded Systems using C”

[2] Gyanendra K Verma, Pawan Tripathi, “A Digital Security System with Door Lock System Using RFID Technology”, International Journal of Computer Applications (IJCA) , Volume 5– No.11, August 2010

[3] Malik Sikandar Hayat Khiyal, Aihab Khan, and Erum Shehzadi. “ SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security”, *Issues in Informing Science and Information Technology. Vol. 9. 2009*

[4] Al-Ali, A.R. Rousan, M.A. Mohandes, M. “GSM-Based Wireless Home Appliances Monitoring & Control System”, *Proceedings of International Conference on Information and Communication Technologies: From Theory to Applications,* pp 237-238, 2004.

[5] X. L. Meng, Z. W. Song, and X. Y. Li, “RFID-Based security authentication system based on a face-recognition structure,” in Proc. WASE International Conference on Information Engineering, 2010, pp. 97-100.