Major Project Report

On

SMS BASED BANKING SECURITY SYSTEM

Submitted in partial fulfillment of Academic Requirement forthe Award of Degree of

BACHELOR OF TECHNOLOGY

in

Electronics and Communication Engineering(ECE)

Submitted by

SARIPELLA SRIKANTH SAI VARMA **20R01A04A8**

Under the esteemed guidance of

Mr.P.Venkatapathi

M.Tech(PhD)

(Assistant Professor, ECE Department)

CMR INSTITUTE OF TECHNOLOGY

(UGC AUTONOMOUS)

Approved by AICTE, Permanent Affiliation to JNTUH, Accredited by NBA and NAAC Kandlakoya(V), Medchal Dist-501 401

www.cmrithyderabad.edu.in

2023-24

CMR INSTITUTE OF TECHNOLOGY

(UGCAUTONOMOUS)

Approved by AICTE, New Delhi, Permanently Affiliated to JNTUH, Hyderabad

Accredited by NBA and NAAC With A Grade

Kandlakoya (V), Medchal Dist-501401

www.cmrithyderabad.edu.in

CERTIFICATE

This is to certify that a Major Project entitled with **" SMS BASEDBANKING SECURITY SYSTEM"** is being submitted by:

SARIPELLA SRIKANTH SAI VARMA **20R01A04A8**

to JNTUH, Hyderabad, in partial fulfillment of the requirement for award of the degree of B.Tech in Electronics &Communication Engineering and is a record of a bonafide work carried out under our guidance and supervision. The results in this project have been verified and are found to be satisfactory. The results embodied in this work have not been submitted to have any other University forward of another degree or diploma.

Signature of Guide	**Project Coordinator**	**Signature of HOD**
Mr.P.Venkatapathi	**Mrs.A.Padma Priya**	**Dr.K.Niranjan Reddy**

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

I am extremely grateful to **Dr. M Janga Reddy**, Director, **Dr. B. Satyanarayana**, Principal, and **Dr. K. Niranjan Reddy**, Head of Department, Dept of Electronics & Communication Engineering, CMR Institute of Technology for their inspiration and valuable guidance during entire duration.

I am extremely thankful to Project Coordinator **Mrs. A. Padma Priya,** Major Project Coordinator, and internal guide **Mr.P.Venkatapathi** Assistant Professor, Dept of Electronics &Communication Engineering, CMR Institute of Technology for their constant guidance, encouragement, and moral support throughout the project.

I will be failing in duty if i do not acknowledge with thanks to the authors of their references and other literature referred in this Project.

I express my thanks to all staff members and friends for all the help and coordination extended in bringing out this Project successfully in time.

Finally, I am very much thankful to my parents and relatives who guided us directly orindirectly for every step towards success.

SARIPELLA SRIKANTH SAI VARMA **20R01A04A8**

ABSTRACT

SMS Bank locker security is important for everyone. Many times we forgot to carry the key of our bank locker. In these cases it is really difficult to open the locker. This project is designed to solve this purpose. Main concept behind this project is of a bank locker-latch opening using two passwords entered through SMS and keypad. Each bank locker will have a GSM modem connected to it. When owner of the bank locker wants to open the locker then he/she has to sends a password through SMS. Then micro controller connected to GSM modem reads the contents of password. If contents are correctthen it will enable the keypad to enter second password. Now user has to enter second password usingKeypad. If second password is correct then system allows user to access locker. We have provided a DC motor which will operate when both passwords are correct. Buzzer will be turned on if any one oftwo password is wrong. Micro controller sends SMS to user for wrong password as well as for correct password. We have also provided an Infrared sensor in this project. Infrared sensor will be triggered when some person is standing in front of Locker. Then system will send SMS to the owner. This is lowwarning message as, “Some person is standing in front of your bank locker”. IR sensor will be turned off password through SMS.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SCREENSHOTS

CHAPTER 1
INTRODUCTION

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 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 a alert according to the pre-set value. Bythe same time this system may not be good for all the time. In this paper we have implemented safety of the money in the bank locker, house, and office (treasury) by using RFID and GSM technology whichwill be more secure than other systems. Radio-frequency identification (RFID)based access-control system allows only authorized persons to open the bank locker 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. Some of the most commonly used RFID kits are low-frequency (30- 500 kHz), mid-frequency (900 kHz-1500MHz) and high frequency (2.4-2.5GHz).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. The SIM300 moduleis a Triband GSM/GPRS solution in a compact plug in module featuring an industry-standard interface.It delivers voice, and fax in a small form factor with low power consumption..in this paper we have designed and implemented a bank locker security system based on RFID and GSM technology. In thissystem only authentic person can be recovered money from bank locker with two password protectionmethod.

1.2 ABOUT PROJECT

SMS-based banking security systems utilize text messages as a means to enhance security in banking transactions and account access. Here our project is to secure the banking locker when a person wants to use the locker he need to enter his password to unlock it. Every locker has its own pass-code when he enters the pass-code UNO reads the pass-code and verifies from its stored data and send the SMS tothe registered mobile number. By sending SMS saying right or wrong pass-code.

Bank locker security is important for everyone who uses it. Many times we lost or forgot to carry the key of our bank locker. In these cases, it gets really difficult to open the bank locker. The main concept behind SMS based bank locker security system project is a bank locker latch opening using two passwords that are entered through SMS and keypad. Each bank locker will have a GSM modem connected to it.

We have provided a DC motor which will operate when passwords is correct. Buzzer will be turned on if the password is wrong. The arduino sends SMS to the user for the wrong password alert. We have also provided an Passive Infrared sensor in this project. The infrared sensor will be triggered when some person is standing in front of Locker.

Despite these challenges, SMS-based bank security systems remain a widely adopted and effective method of enhancing the security of online banking transactions and protecting customers' financial information from unauthorized access. As technology continues to evolve, banks may explore additional authentication methods, such as biometric authentication or token-based authentication, to further strengthen security and improve the user experience.

1.3 Problem Statement

Despite advancements in online banking security, traditional authentication methods such as username and password combinations remain vulnerable to phishing attacks, password breaches, and unauthorized access. To address these security concerns and enhance the protection of customers' financial information, there is a need for a more robust and reliable authentication system. This project aims to develop an SMS-based bank security system that leverages one-time passwords (OTPs) delivered via text messages to users' mobile phones, providing an additional layer of security for online banking transactions. The system will mitigate the risk of unauthorized access, improve user authentication processes, and ensure compliance with regulatory standards while maintaining convenience and accessibility for customers. By implementing this SMS-based security solution, banks can bolster the security of their online banking platforms and safeguard sensitive customer data against cyber threats.

In the realm of banking and financial services, the security of customers' valuable possessions remains a critical concern. Traditional bank locker systems, while offering a degree of protection, face various challenges in providing optimal security, accessibility, and user experience. These challenges include limited availability of lockers, high operational costs, susceptibility to theft or damage, and concerns regarding privacy and convenience. To address these issues and enhance the effectiveness of bank locker systems, there is a need for innovative solutions that prioritize security, affordability, convenience, and customer satisfaction. This research aims to identify the key challenges associated with existing bank locker systems and explore potential strategies for improving security, accessibility, and overall functionality to meet the evolving needs and expectations of customers in the digital age

CHAPTER 2
SYSTEM PROPOSAL

2.1 EXISTING SYSTEM

Two-Factor Authentication (2FA): Many banks use SMS to deliver one-time pass-codes for two-factorauthentication during the login process. Users are required to enter this code along with their regular username and password to access their accounts online or perform sensitive transactions.

Transaction Alerts: Banks send SMS notifications to customers for every transaction made with their account. These alerts typically include details such as the transaction amount, merchant name (if available), and the remaining account balance. Customers can quickly identify any unauthorized transactions and report them to the bank.

Account Alerts: Customers can set up SMS alerts for various account activities, such as low balance warnings, large withdrawals, or changes to account settings. This allows them to monitor their accountsin real-time and detect any suspicious or unauthorized activity promptly.

Password Reset and Account Recovery: SMS is often used as part of the password reset and account recovery process. When users forget their passwords or need to recover access to their accounts, they can request a verification code via SMS to authenticate their identity and regain access.

Fraud Prevention: Some banks use SMS to communicate with customers about potential fraud or security threats. For example, if the bank detects unusual activity on a customer's account, they may send an SMS alert asking the customer to confirm whether the transaction was authorizedTo Stop the Bank vault robbery, a GSM based security system named- “GSM Based Bank Vault Security System” has been proposed. By this project more security level of Bank vault has been ensured. There have been done more research and work in GSM Based automated security system. Several security systems were developed in [1], [2]. In [1], microcontroller ATMega16 are connected together and also connected with an alarm system and GSM modem. In [2], developed a multilayer Bank security system using

microcontroller ATMega16 which is integrated RFID, PIR sensor, IRIS and Fingerprint scanner and alarm system. In this proposed GSM Bank vault security system, four sensors have been used. Also an IP camera and GSM Module have been used.he simplified block diagram of the proposed security system. The figure shows that the system design comprises various hardware modules. The primary modules are sensors (sound, motion, laser and gas) which send signals to the Arduino when any of sensors activated in the vault room. All sensors are connected to the Arduino UNO Board and Arduino also connected to the alarm system to create an alarm and GSM modem to send a warning message.

The existing system is a system which is currently been implemented and used. The proposal of the new system is to remove the shortcomings of the currently used system. The existing systems use various technologies for instance: biometric and GSM technology, RFID tags, image processing etc. All these come with limitations and drawbacks which can significantly impact the security.

The biometric technology used includes facial recognition and fingerprint which requires large data base; furthermore they are not cost effective and require the need for ample amount of investment.

Data breaches of biometries can still be done, Biometric devices using facial recognition can limit the privacy of the users too.

RFID tags ie., radio-frequency identification tags uses electromagnetic fields to automatically identify and track tags attached to the objects. These RFID tags use smart barcodes in order to identify themselves. Even with such advancement and advantage it still has the major drawback of causing hindrance if the network signals are unavailable, which causes it to cease another existing system uses RFID tags, pattern analyser, image processing making it a three level process. This can be very time consuming because huge datasets are required to collect all the information and maintaining them in the server further the implementation of a camera is required too to capture the pattern flow of the user, which also makes it expensive.

An alternative existing system uses fingerprint authentication to open their respective locker uses biometric technology and requires the user to gain access to their locker via their fingerprint. The system has following drawbacks:

The accuracy and the working of the system is affected by skin conditions of people, System is associated with forensic applications Involves serious health issues due to touching of the single scanning sensor device by countlessindividuals. Which has serious implications in pandemic such as covid-19 etc. Difficult to capture complete and accurate fingerprint image in cases based on the age and health

Collection of high quality nail to nail image requires training and specific skills.

There are various and vast options available which can be efficiently implemented in the system. The system proposes a secure way of operating the bank locker via the use of GSM modem, there quite useful ways too to access and safeguard our valuables, locker by using biometric finger print, iris recognition, RFID tags, image processing etc. The fingerprint sensor, is very popular and significantly used in various countries across the world. It offers high accuracy for fingerprint recognition and long term stability too. The human finger is pressed on a scanning device to capture the image of the finger of a person. Once it is captured it is cross checked or verified with the stored fingerprint of the owner, which is unique to everyone. It can also be used as a reference sample for any future verifications of the same individual. The mentioned process is not as easy as it is read, the fingerprint sensor comes with its own limitations. The accuracy and functioning of the system is affected by the skin conditions of the people. Storing biometric database can be expensive and might not be used or implemented everywhere and by everyone. Given the pandemic situations such as covid-19 etc. this technology has serious implications and consequences. This technology also finds it difficult to capture the complete and accurate fingerprint image in some cases based in age and occupation of the person too. The collection of such high quality nail to nail image needs extensive training and high set of skills.

IRIS RECOGNITION: Iris recognition technology can also be used to access the bank lockers, and possibly gives very high level of security too. It is a form of biometric technology identification technique that can verify the uniqueness of an individual with exceptional accuracy. The iris recognition technique requires four main stages, which are:

Image capture: A high quality image of the individual's left and right iris must be captured using camera. These camera's use near-infrared (NIR) sensors to capture the minute and intricate details of the iris with much greater accuracy than visible light.

Compliance check and image enhancement: the next step is to perform quality and compliance checks to ensure that the captured image is suitable as a biometric template for future iris scanning

All these steps in combination gives us the efficient iris recognition system, even though it invests such huge amount of time and money, it cannot be used considering our proposed system.
increase the cost and budget. Generally requires close proximity to the camera which might cause discomfort for some. The hazard of iris scanning is the danger of the national database flest can track people covertly, at a distance or in motion, without their knowledge or consent. This raises significant civil liberties and privacy concerns. Quality problems also arise due to poor subject presentation e.g., a crossed eye, rotated iris or off-axis gaze. It is also possible to trick or bypass iris scanners. In 2012, security researchers at the Universidad Autonoma de Madrid were able to recreate images of iris's from digital codes stored in security databases, which also makes it more prone to hacking. Accordingly this available or existing technique cannot be implemented in proposed system.

2.1.1 Disadvantages

- Dependency on Power Supply
- Risk of Loss or Damage
- Compatibility Issues
- Risk of Hacking or Cyberattacks

2.2 PROPOSED SYSTEM

Current real time M-banking application of various banks uses plain text messages without any securityalgorithm for sending data in SMS banking hence any malicious user can access customer important data on mobile. Proposed secure M-banking is based on symmetric crystallographic techniques where common secret key is shared among bank customer and bank server. Proposed Architecture consists of4 components as Customer Mobile application, Bank Server application, Bank side mobile / GSM Modem, Bank database and wireless OTA.

this elucidate the overview of the proposed system including the discussion of the overall understanding of the project and the scope of the work. Earlier discussion on the limitations of the existing systems is done. Now we consider the model of the proposed system. The process of design and implementation involves continual tradeoffs between cost and performance. Quantifying the performance implications of various alternatives is central to this process. It is also extremely challenging. With evolving technology and confluence of ideas from software and hardware engineering this system achieves the required objectives. The purpose of this chapter is to present the elements of the system and technologies used.In this evolving world to keep pace with the science and technology is salient, and one cannot overlook the need for security and growing need for it. Home was predominantly preferred to store their prized possessions and valuables, but moving on the building of commercial organizations and firms called banks led to achieving a step towards security. Bank lockers are facility provided by the banks as safety deposits that allow the customers to store their important and valuable items. With the application and use of GSM (global system for mobile communications) Is the most secured cellular telecommunications system available today which maintains high end-to-end security and retains the confidentiality of calls and anonymity of the subscriber ceasing the possibility of any cyber attacks.

2.2.1 Advantages

- Convenience
- User-Friendly Interface
- Real-Time Alerts
- Scalability

CHAPTER 3
LITERATURE SURVEY

3.1 LITERATURE SURVEY

In this chapter some of related works connected to the monitoring system using GSM services are illustrated. In [4] has developed a Prepaid Water Meter System for prepaid billing of water utilization through remote monitoring without any human inclusion. This system may be fast and reliable billing of water as well as preventing any mishandling of it. However, [5] developed a water meter reading using GSM system that is worthy for remote places to monitor the water meter reading before any billing process. This could minimize the use of human resource for reading the meter and producing a bill. There was also a work on monitoring of electrical meter reading using GSM network done by [6]. The system was able to monitor the meter Journal of Emerging Technologies and Innovative Research (JETIR) www.jetir.org 67 reading and send an SMS to the official center for billing purpose. This could lessen the number of estimated reading when the authorize person is unable to reach the meter. In [7], this system is used to control home appliance tenuously and offer security when the owner is away from the place. The similar work presented in [8] which designed and developed a smart home application system. The system allows the property owner to be able to monitor and control the residence appliances via a mobile phone set by sending commands in the form of SMS messages and receiving the home appliances status. In [9], one more approach using GSM technology to communicate with the remote devices via SMS is remote metering system, in this paper illustrates a technique for remotely reading electricity meter readings using SMS. Both postpaid and prepaid are feasible to implement using this architecture as SMS based data gathering can be done very quickly and efficiently. In [10] [11], this paper projected a Zigbee-GSM based Monitoring and Remote Control System. In this systems used both Zig bee and GSM for communicating between user and devices. Users may remotely monitor and control their home devices using GSM. In [12], the most important objective of the paper is to design and develop a highly developed vehicle locking system in the real time situation. The design & development of a theft control system for an automobile, which is being used to prevent/control the theft of a vehicle. This system consists of an embedded system and Global System Mobile communication (GSM) technology. This system developed by Pravada P. Wan hade and Prof. S.O. Dahad, the developed system is installed in the vehicle. The mobile is connected to the micro controller, which is in turn, connected to the engine.

Once, the vehicle is being stolen, the information is being used by the vehicle owner for further processing. The information is passed onto the central processing insurance system which is in the form of the SMS, the micro controller unit reads the SMS and sends it to the Global Positioning System (GPS) module and says to lock it or to stop the engine immediately. The main concept of this paper vehicle is controlled by GSM and GPS. The designed unit is reliable and efficient system for providing security to the vehicles through GSM, GPS and serial communication. Name of the author: Sagar S. Palsodkar*, Prof S.B. Patil Title: Biometric and GSM Security for Lockers Publication: Int. Journal of Engineering Research and Applications Concept about work: In this review paper we will develop biometric (finger or face) and GSM technology for bank lockers. Because in this system bank will collect the biometric data of each person for accessing the lockers because in this system only authenticated person recover the money, documents from the lockers[1]. Advantages: As biometric and GSM security has been used hence more advantages then other system. Limitations: As fingerprint or face biometric system is used then large data base is required Name of the author: R.Ramani ,S. Selvaraju, S.Valarmathy, P Niranjan Title: Bank Locker Security System based on RFID and GSM Technology Publication: International Journal of Computer Applications Concept about work:The main goal of this paper is to design and implement a bank locker security system based on RFID and GSM technology which can be organized in bank, secured offices and homes. In this system only authentic person can be recovered money from bank locker.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[2]. Advantages: This system is more secure than other systems because two passwords required for verification. Limitations: As network signals are not available, then locker may not be opened Name of the author: P. Sugapriya#1, K. Amsavalli#2 Title: Smart Banking Security System Using Pattern Analyzer Publication: International Journal of Innovative Research in Computer and Communication Engineering Concept about work: Initially pattern flow are collected as data sets and maintained in bank agent server. The machine has a camera to capture the pattern flow of user and sent for processing features of the logic were compared and user where recognized. In addition to the authentication of user there is another system to identify the user before that RFID tad checking is needed. Image processing is used and keypad password is needed.

In future bank can implement this type of authentication option for banking and from this projectshows that all the bank accounts can be accessed without using cards through this face recognition efficiently andsafely[3]. Advantages: Three level banking security is used. Limitations: Time consuming method because huge datasets are require Name of the author: Gayathri and Selvakumari Title: Fingerprint and GSM based Security System. Publication: International Journal of Engineering Sciences & Research Technology. Concept about work: Access control system forms a vital link in a security chain. The Fingerprint and password based security system presented here is an access control system that allows only authorized persons to access a restricted area. We have implemented a locker security system based on fingerprint, password andGSM technology containing door locking system which can activate, authenticate and validate the user and unlock thedoor in real time for locker secure[4]. Advantages: It will provide strong authentication key. Limitations: It is time consuming. Name of the author: Mary Lourde R and Dushyant Khosla Title: Fingerprint Identification in Biometric Security Systems. Publication: International Journal of Computer and Electrical Engineering Concept about work: They says Perhaps the most important application of accurate personal identification is securing limited access systems from malicious attacks. Among all the presently employed biometric techniques, fingerprint identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics. This paper deals with the issue of selection of an optimal algorithm for fingerprint matching in order to design a system that matches required specifications in performance and accuracy[5]. Advantages: Fingerprint identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics Limitations: Only one biometric fingerprint authentication is used. Name of the author: Pramila D Kamble and Dr. Bharti W. Gawali Title: Fingerprint Verification of ATM Security System by Using Biometric and hybridization Publication: International Journal of Scientific and Research Publications Concept about work: The biometrics, fingerprint recognition is one of the most reliable and promising personal identification technologies. Fingerprints are the most widely used biometric feature for person identification and verification. But in this paper we proposed that fingerprint verification of ATM (Automatic Teller Machine) security system using the biometric with hybridization. The fingerprint trait is chosen, because of its availability, reliability and high accuracy[6]. Advantages: Security system using the biometric with hybridization. The fingerprint trait is chosen, because of its availability, reliability and high accuracy.

CHAPTER 4

COMPONENTS SPECIFICATION

4.1 HARDWARE COMPONENTS

4.1.1 ARDUINO

The Arduino is a family of microcontroller boards to simplify electronic design, prototyping and experimenting for artists, hackers, hobbyists, but also many professionals. People use it as brains for their robots, to build new digital music instruments, or to build a system that lets your house plants tweet you when they're dry. Arduinos (we use the standard Arduino Uno) are built around an ATmegamicrocontroller — essentially a complete computer with CPU, RAM, Flash memory, and input/outputpins, all on a single chip. Unlike, say, a Raspberry Pi, it's designed to attach all kinds of sensors, LEDs,small motors and speakers, servos, etc. directly to these pins, which can read in or output digital or analog voltages between 0 and 5 volts. The Arduino connects to your computer via USB, where you program it in a simple language (C/C++, similar to Java) from inside the free Arduino IDE by uploadingyour compiled code to the board. Once programmed, the Arduino can run with the USB link back to your computer, or stand-alone without it — no keyboard or screen needed, just power.

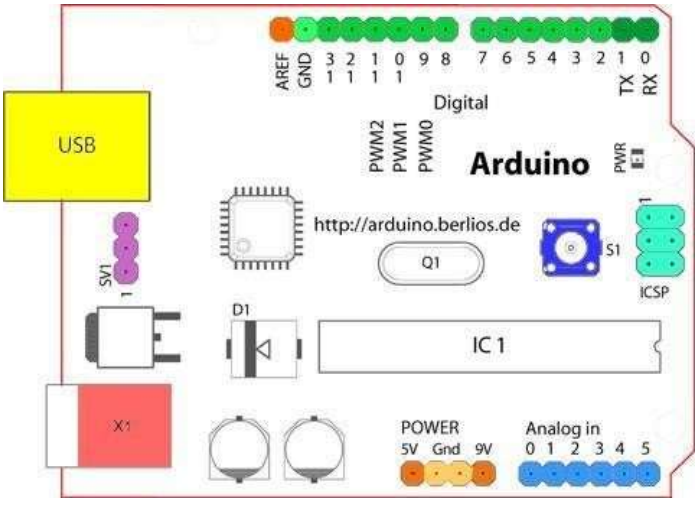

Fig 1. Structure of Arduino Board

Digital Pins

In addition to the specific functions listed below, the digital pins on an Arduino board can be used for general purpose input and output via the pin Mode(), Digital Read(), and Digital Write() commands. Each pin has an internal pull-up resistor which can be turned on and off using digital Write() (w/a valueof HIGH or LOW, respectively) when the pin is configured as an input. The maximum current per pinis 40mA.

Analog Pins

In addition to the specific functions listed below, the analog input pins support 10-bit analog-to-digitalconversion (ADC) using the analog Read() function. Most of the analog inputs can also be used as digital

Power Pins

VIN (sometimes labeled "9V"): The input voltage to the Arduino board when it's using an external power source (as opposed to 5 volts from the USB connection or other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin. Also note that the Lily Pad has no VIN pin and accepts only a regulated input.

GND: Ground pins.

Other Pins:

AREF: Reference voltage for the analog inputs. Used with analog Reference().

Reset: (Diecimila-only) Bring this line LOW to reset the microcontroller. Typically used to add a resetbutton to shields which block the one on the board.

Controller (ATMEGA328):

Controller is heart of our system. This controller following features: 32Kbytes of in-system programmable flash with read-while write capabilities, two 8-bit Timer/Counters, 23 programmable I/O Lines, and operating Voltage is 1.8 - 5.5V, Temperature Range -40°C to 105°C, three flexible Timer/Counters.Pin configuration of ATmega328 IC consists of 28 pins.There is Port B, Port C & Port D an 8-bit bi-directional I/O port with internal pull-up resistors.

Pin Diagram

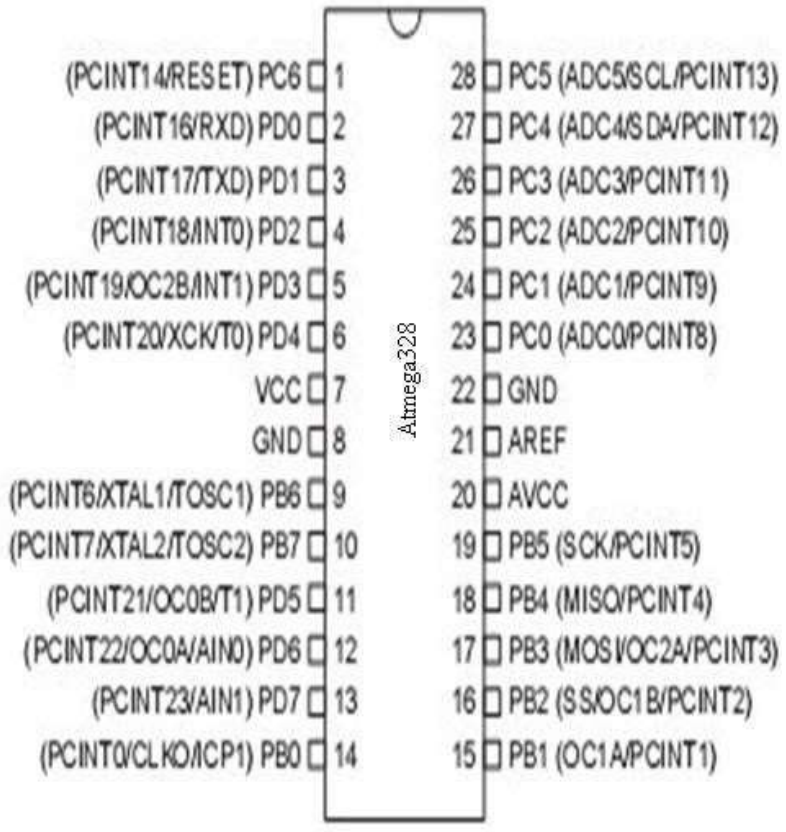

Fig 2. Pin Configuration of Atmega328

Pin Description

VCC: Digital supply voltage. GND: Ground.

Port A (PA7-PA0): Port A serves as the analog inputs to the A/D Converter. Port A also serves as an 8-bit bi-directional I/O port, if the A/D Converter is not used. Port pins can provide internal pull-up resistors (selected for each bit). The Port A output buffers have symmetrical drive characteristics with both high sink and source capability. When pins PA0 to PA7 are used as inputs and are externally pulledlow, they will source current if the internal pull-up resistors are activated. The Port A pins are tri-statedwhen a reset condition becomes active, even if the clock is not running.

Port B (PB7-PB0): Port B is an 8-bit bi-directional I/O port with internal pull-up resistors (selected foreach bit). The Port B output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port B pins that are externally pulled low will source current if the pull-upresistors are activated. The Port B pins are tri-stated when a reset condition becomes active, even if theclock is not running. Port B also serves the functions of various special features of the ATmega32.

Port C (PC7-PC0): Port C is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port C output buffers have symmetrical drive characteristics with both high sink andsource capability. As inputs, Port C pins that are externally pulled low will source current if the pull-upresistors are activated. The Port C pins are tri-stated when a reset condition becomes active, even if theclock is not running. If the JTAG interface is enabled, the pull-up resistors on pins PC5(TDI), PC3(TMS) and PC2(TCK) will be activated even if a reset occurs. The TD0 pin is tri-stated unless TAPstates that shift out data are entered. Port C also serves the functions of the JTAG interface.

Port D (PD7-PD0): Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port D output buffers have symmetrical drive characteristics with both high sink andsource capability.

Reset (Reset Input): A low level on this pin for longer than the minimum pulse length will generate areset, even if the clock is not running. Shorter pulses are not guaranteed to generate a reset.

XTAL1: Input to the inverting Oscillator amplifier and input to the internal clock operating circuit.

XTAL2: Output from the inverting Oscillator amplifier.

AVCC: AVCC is the supply voltage pin for Port A and the A/D Converter. 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 through a low-pass filter.

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

FEATURES :

- 1.8-5.5V operating range
- Up to 20MHz
- Part: ATMEGA328P-AU
- 32kB Flash program memory
- 1kB EEPROM
- 2kB Internal SRAM
- 2 8-bit Timer/Counters
- 16-bit Timer/Counter
- RTC with separate oscillator
- 6 PWM Channels
- 8 Channel 10-bit ADC
- Serial USART
- Master/Slave SPI interface
- 2-wire (I2C) interface
- Watchdog timer
- Analog comparator

Arduino Characteristics

The power pins are as follows:

- VIN: The input voltage to the Arduino board when it's using an external power source (as opposedto 5 volts from the USB connection or other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin.
- 5V: This pin outputs a regulated 5V from the regulator on the board. The board can be suppliedwith power either from the DC power jack (7 - 12V), the USB connector (5V), or the VIN pin of the board (7-12V). Supplying voltage via the 5V or 3.3V pins bypasses the regulator, and can damage your board. We don't advise it.
- 3V3. A 3.3 volt supply generated by the on-board regulator. Maximum current draw is 50 mA.
- GND. Ground pins.

4.1.2 LCD (Liquid Cristal Display)

Introduction:

A liquid crystal display (LCD) is a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector. Each pixel consists of a column of liquid crystal molecules suspended between two transparent electrodes, and two polarizing filters, the axes of polarity of which are perpendicular to each other. Without the liquid crystals between them, light passing through one would be blocked by the other. The liquid crystal twists the polarization of light entering one filter to allow it to pass through the other.A program must interact with the outside world using input and output devices that communicate directly with a human being. One of the most common devices attached to an controller is an LCD display. Some of the most common LCDs connected to the contollers are 16X1, 16x2 and 20x2 displays. This means 16 characters per line by 1 line 16 characters per line by 2 lines and 20 characters per line by 2 lines, respectively.

Shapes and S available. Line lengths of 8, 16, 20, 24, 32 and 40 characters are all standard, in one, two.

Many microcontroller devices use 'smart LCD' displays to output visual information. LCD displays designed around LCD NT-C1611 module, are inexpensive, easy to use, and it is even possible to produce a readout using the 5X7 dots plus cursor of the display. They have a standard ASCII set of characters and mathematical symbols. For an 8-bit data bus, the display requires a +5V supply plus 10I/O lines (RS RW D7 D6 D5 D4 D3 D2 D1 D0). For a 4-bit data bus it only requires the supply linesplus 6 extra lines(RS RW D7 D6 D5 D4). When the LCD display is not enabled, data lines are tri-stateand they do not interfere with the operation of the microcontroller.

Features:

(1) Interface with either 4-bit or 8-bit microprocessor.

(2) Display data RAM

(3) 80x □8 bits (80 characters).

(4) Character generator ROM

(5) 160 different 5 7 dot-matrix character patterns.

(6) Character generator RAM

(7) 8 different user programmed 5 7 dot-matrix patterns.

(8) Display data RAM and character generator RAM may be Accessed by the microprocessor.

(9) Numerous instructions

(10) Clear Display,Cursor Home, Display ON/OFF, Cursor ON/OFF, Blink Character, Cursor, Display Shift.

(11). Built-in reset circuit is triggered at power ON.(12). Built-in oscillator.

.

Data can be placed at any location on the LCD. For 16×1 LCD, the address locations are:

POSITION		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ADDRESS	LINE1	00	01	02	03	04	05	06	07	40	41	42	43	44	45	46	47

Table 4.1 Address locations for a 1x16 line LCD

Shapes and sizes:

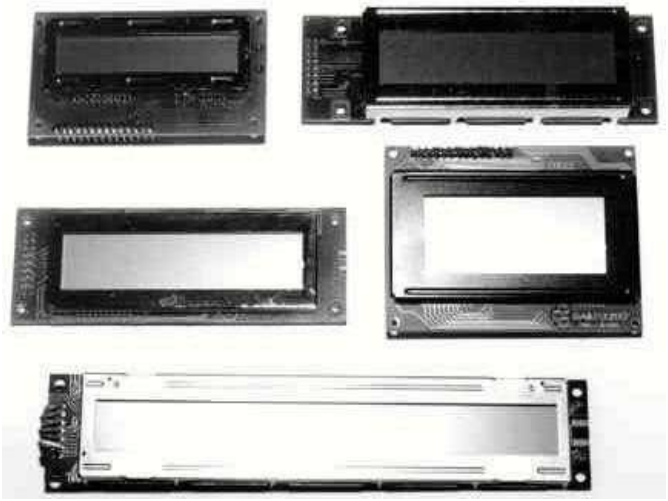

Fig 3. LCD Display

Even limited to character based modules, there is still a wide variety of shapes and sizes available. Linelengths of 8,16,20,24,32 and 40 characters are all standard, in one, two and four line versions.

Several different LC technologies exists. “super-twist” types, for example, offer Improved contrast andviewing angle over the older “twisted nematic” types. Some modules are available with back lighting, so so that they can be viewed in dimly-lit conditions. The back lighting may be either “elector- luminescent”, requiring a high voltage inverter circuit, or simple LED illumination.

PIN DESCRIPTION:

Most LCD's with 1 controller has 14 Pins and LCD's with 2 controller has 16 Pins (two pins are extra in both for back-light LED connections).

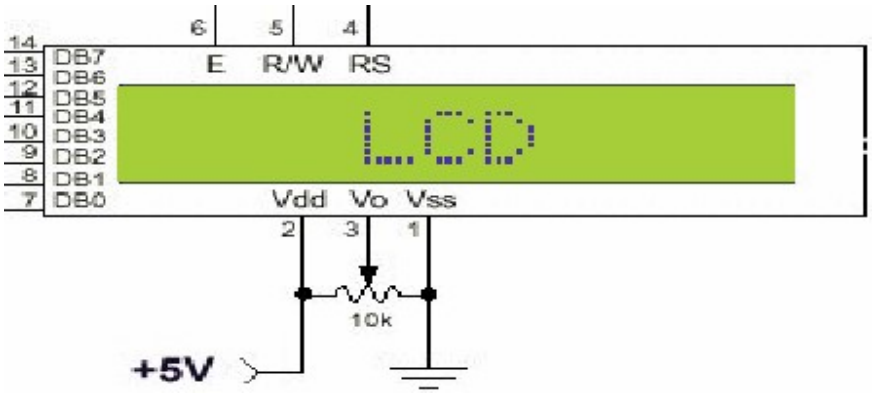

Fig 4.Pin diagram of 1x16 lines lcd

PIN	SYMBOL	FUNCTION
1	Vss	Power Supply(GND)
2	Vdd	Power Supply(+5V)
3	Vo	Contrast Adjust
4	RS	Instruction/Data Register Select
5	R/W	Data Bus Line
6	E	Enable Signal
7-14	DB0-DB7	Data Bus Line
15	A	Power Supply for LED B/L(+)
16	K	Power Supply for LED B/L(-)

Table 4.2 Pin symbols and functions

4.1.3 REGULATED POWER SUPPLY:

Introduction:

Power supply is a supply of electrical power. A device or system that supplies electrical or other typesof energy to an output load or group of loads is called a power supply unit or PSU. The term is most commonly applied to electrical energy supplies, less often to mechanical ones, and rarely to others. A

power supply may include a power distribution system as well as primary or secondary sources of energy such as

Conversion of one form of electrical power to another desired form and voltage, typically involving converting AC line voltage to a well-regulated lower-voltage DC for electronic devices. Low voltage, low power DC power supply units are commonly integrated with the devices they supply, suchas computers and household electronics.

Batteries.

Chemical fuel cells and other forms of energy storage

systems.Solar power.

Generators or
alternators.

Block Diagram:

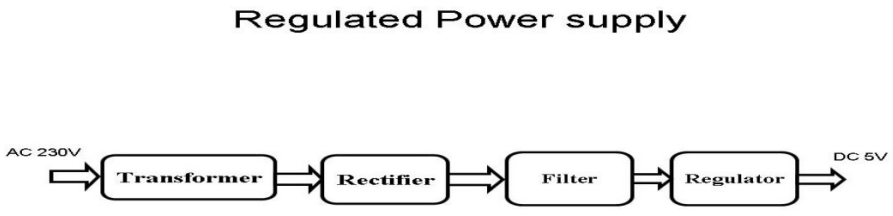

Fig 5. Regulated Power Supply

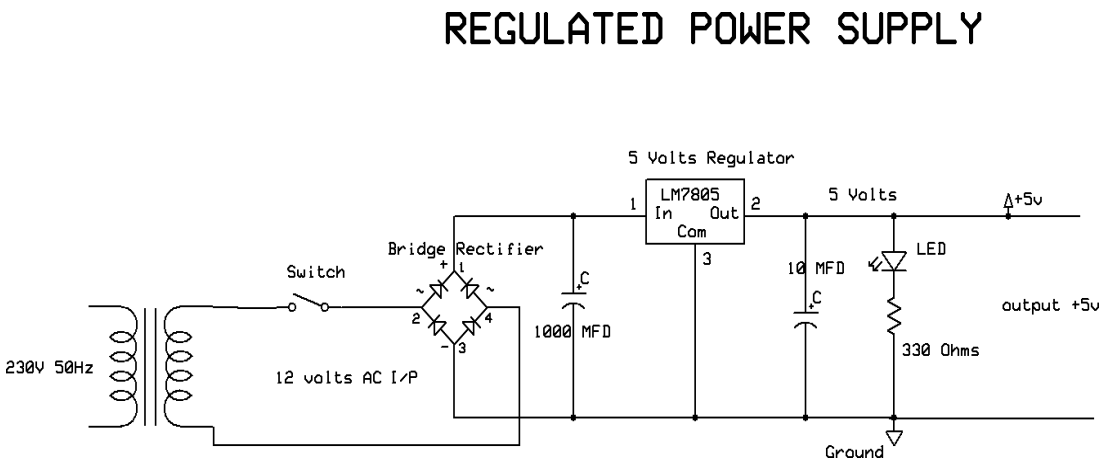

Fig 6.Circuit diagram of Regulated Power Supply with Led connection

The components mainly used in above figure are

- 230V AC MAINS
- TRANSFORMER
- BRIDGE RECTIFIER(DIODES)
- CAPACITOR
- VOLTAGE REGULATOR(IC 7805)
- RESISTOR
- LED(LIGHT EMITTING DIODE)

4.1.4 Battery power supply:

A battery is a type of linear power supply that offers benefits that traditional line-operated power supplies lack: mobility, portability and reliability. A battery consists of multiple electrochemical cells connected to provide the voltage desired. Hi-Watt 9V battery.

Fig 7 Hi-Watt 9V Battery

The most commonly used dry-cell battery is the carbon-zinc dry cell battery. Dry-cell batteries are made by stacking a carbon plate, a layer of electrolyte paste, and a zinc plate alternately until the desiredtotal voltage is achieved. The most common dry-cell batteries have one of the following voltages: 1.5,3, 6, 9, 22.5, 45, and 90. During the discharge of a carbon-zinc battery, the zinc metal is converted to azinc salt in the electrolyte, and magnesium dioxide is reduced at the carbon electrode. These actions establish a voltage of approximately 1.5 V.

The lead-acid storage battery may be used. This battery is rechargeable; it consists of lead and lead/dioxide electrodes which are immersed in sulfuric acid. When fully charged, this type of battery has a 2.06-2.14 V potential (A 12 volt car battery uses 6 cells in series). During discharge, the lead is converted to lead sulfate and the sulfuric acid is converted to water. When the battery is charging, the lead sulfate is converted back to lead and lead dioxide A nickel-cadmium battery has become more popular in recent years. This battery cell is completely sealed and rechargeable. The electrolyte is not involved in the electrode reaction, making the voltage constant over the span of the batteries long service life. During the charging process, nickel oxide is oxidized to its higher oxidation state and cadmium oxide is reduced. The nickel-cadmium batteries have many benefits. They can be stored bothcharged and uncharged. They have a long service life, high current availabilities, constant voltage, andthe ability to be recharged. Fig: 3.3.5 shows pencil battery of 1.5V.

Hi-Waote 9V Battery is the most commonly used and portable 9V battery. It is non-rechargeable and is a high capacity and low-cost solution for many electronic devices. It is based on Zinc Carbon Chemistry and can be used easily replaced if discharged just like any standard AA and AAA batteries.

4.1.5 LED

A light-emitting diode (LED) is a semiconductor light source. LEDs are used as indicator lamps in many devices, and are increasingly used for lighting. Introduced as a practical electronic component in1962, early LEDs emitted low-intensity red light, but modern versions are available across the visible,ultraviolet and infrared wavelengths, with very high brightness. The internal structure and parts of a ledare shown below.

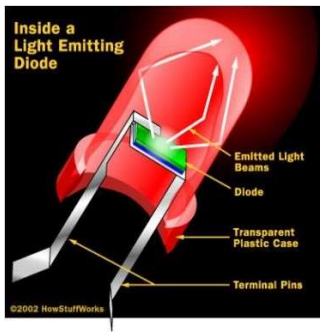

Fig 8. Inside a LED

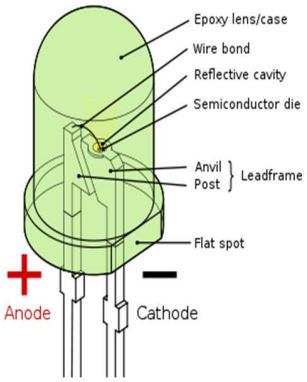

Fig 9. Parts of a LED

Working:

The structure of the LED light is completely different than that of the light bulb. Amazingly, the LED has a simple and strong structure. The light-emitting semiconductor material is what determines the LED's color. The LED is based on the semiconductor diode. When a diode is forward biased (switchedon), electrons are able to recombine with holes within the device, releasing energy in the form of photons. This effect is called electroluminescence and the color of the light (corresponding to the energyof the photon) is determined by the energy gap of the semiconductor. An LED is usually small in area (less than 1 mm2), and integrated optical components are used to shape its radiation pattern and assist in reflection. LEDs present many advantages over incandescent light sources including lower energy consumption, longer lifetime, improved robustness, smaller size, faster switching, and greater durabilityand reliability. However, they are relatively expensive and require more precise current and heat management than traditional light sources. Current LED products for general lighting are moreexpensive to buy than fluorescent lamp sources of comparable output. They also enjoy use in applications as diverse as replacements for traditional light sources in automotive lighting (particularly indicators) and in traffic signals.

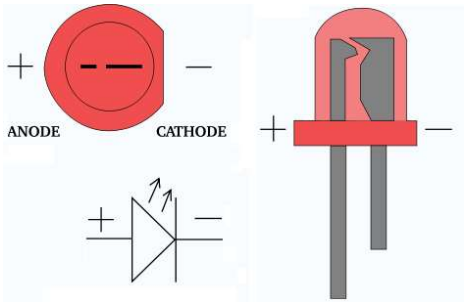

Fig 10. Electrical Symbol & Polarities of LED

LED lights have a variety of advantages over other light sources:
High-levels of brightness and
intensityHigh-efficiency
Low-voltage and current
requirementsLow radiated heat

High reliability (resistant to shock and
vibration)No UV Rays
Long source life
Can be easily controlled and programmed

4.1.6 PIR SENSOR

PIR Sensor is short for passive infrared sensor, which applies for projects that need to detect human orparticle movement in a certain range, and it can also be referred as PIR(motion) sensor, or IR sensor. Since its powerful function and low-cost advantages, it has been adopted in tons of projects and widely accepted by the open-source hardware community for projects related to Arduino and raspberry pi. Allthis can help the beginners learn about PIR sensor more easily

PIR sensors allow you to sense motion, almost always used to detect whether a human has moved in or out of the sensors range. They are small, inexpensive, low-power, easy to use and don't wear out. For that reason they are commonly found in appliances and gadgets used in homes or businesses. They are often referred to as PIR, "Passive Infrared", "Pyroelectric", or "IR motion" sensors.

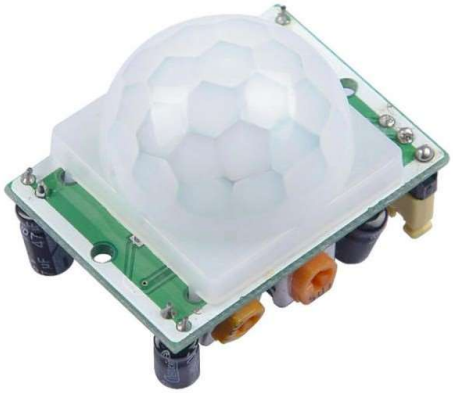

Fig 11 .PIR Motion Sensor – Large Lens version

In this article, I will introduce PIR Sensor with the following 7 sections and compare different PIR sensors that you can find at our online store. Hope it can help you understand PIRs better and pick thesuitable PIR sensor for your projects.

1. What is PIR Sensor?

A passive infrared sensor is an electronic sensor that measures infrared light radiating from objects in its field of view. They are most often used in PIR-based motion detectors. PIR sensors are commonly used in security alarms and automatic lighting applications.Technically, PIR is made of a pyroelectric sensor, which is able to detect different levels of infrared radiation. For example, Everything emits varied level radiation and the level of radiation will increase with the increase of the object's temperature.

2. What does a PIR sensor detect?

As we all know that PIR sensors can be also refer to PID, which is short for passive infrared detectors. As you have learned about the technical term in the first part, PIR sensor can detect infrared radiation which is emitted by particles.

Generally, PIR can detect animal/human movement in a requirement range, which is determined by the spec of the specific sensor. The detector itself does not emit any energy but passively receives it, detects infrared radiation from the environment. Once there is infrared radiation from the human body/ particle with temperature, focusing on the optical system causes the pyroelectric device to generate a sudden electrical signal and an alarm is issued.

3. How does PIRs work?

The passive infrared alarm does not radiate energy to space but relies on receiving infrared radiation from the human body to make an alarm. Any object with temperature is constantly radiating infrared rays to the outside world. The surface temperature of the human body is 36-27 ° C, and most of its radiant energy is concentrated in the wavelength range of 8-12 um.

Passive infrared alarms can be classified into infrared detectors (infrared probes) and alarm control sections. The most widely used infrared detector is a pyroelectric detector, which is used as a sensor for converting human infrared radiation into electricity. If the human infrared radiation is directly

irradiated on the detector, it will, of course, cause a temperature change to output a signal, but in doing so, the detection distance will not be far. In order to lengthen the detection distance of the detector, an optical system must be added to collect the infrared radiation, usually using a plastic optical reflection system or a Fresnel lens made of plastic as a focusing system for infrared radiation.

In the detection area, the infrared radiation energy of the human body through the clothing is received by the lens of the detector and focused on the pyroelectric sensor. When the human body (intruder) moves in this surveillance mode, it enters a certain field of view in sequence and then walks out of the field of view. The pyroelectric sensor sees the moving human body for a while and then does not see it, so the human body The infrared radiation constantly changes the temperature of the pyroelectric material so that it outputs a corresponding signal, which is the alarm signal

1. The Range of PIR Sensor?

Indoor passive infrared: Detection distances range from 25 cm to 20 m. Indoor curtain type: The detection distance ranges from 25 cm to 20 m.

Outdoor passive infrared: The detection distance ranges from 10 meters to 150 meters. Outdoor passive infrared curtain detector: distance from 10 meters to 150 meters

2. What is the difference between PIR sensor and motion sensor?

The motion sensor is a device that can detect the movement of people or objects. In most applications, these sensors are mainly used to detect human activities in a specific area.

As it is capable of converting the motion it senses into electrical signals, the sensor either emits stimuli and monitors any changes reflected back, or acquires signals from the moving object itself. Some motion sensors will alarm when people or other objects invade and break the normal state, while others will alarm when they return to normal state after the invasion. Security systems all over the world rely on motion sensors to trigger alarms and/or automatic lighting switches, which are usually placed in relatively easy access to buildings, such as windows and gates.

4.1.7 BUZZERS

In common parlance a Buzzer is a signaling device that is not a loudspeaker. It can be mechanical, electromechanical, or electronic (a piezo transducer). BeStar produces Buzzers in every available configuration for a wide variety of applications. A Piezo transducer can produce the sound for panel mount buzzers, household goods, medical devices and even very loud sirens. When a lower frequencyis required an electromagnetic buzzer can fill the need. These are very common in automotive chimes and higher end clinical diagnostic devices. The BeStar buzzer range includes self drive units with theirown drive circuitry (indicators), or external drive units, which allow the designer the flexibility to createtheir own sound patterns.

BeStar buzzers, whether a piezo buzzer, or an electro-magnetic buzzer, self (indicator) or non-self (transducer) drive are available with a variety of mounting methods, such as surface mount, thru hole, flange, wire leads or panel mounting. Sealed, high temp, very loud, weather resistant; whatever your application requirement is, BeStar has a piezo buzzer that will meet your design criteria.

Browse our selection on the site and you can also browse several catalogs found under the Resources Tab: Electromagnetic, Surface Mount, Piezo Surface Mount, and Automotive. Typical piezoelectric buzzer frequencies range from 2000-4000Hz and an electromagnetic buzzer provides good sound output starting at 800Hz. Operating voltage range for self drive units is 3-28Vdc, units are available in110 or 230Vac and for non-self drive units 1-60Vp-p.

BeStar buzzers achieve strong, clear sound pressure and reliable performance, that is why we havebeen chosen by important global companies like Whirlpool, Visteon, Bosch-Siemens, and Roche Diagnostics to name a few. Buzzers are a wide product area, so for convenience we have broken it up into four categories: Indicators, Transducers, Panel Mount Buzzers and Junction Box Buzzers. If you need application assistance, please contact a BeStar representative.

ACTIVE PASSIVE BUZZER

Fig 12 Active Passive Buzzer

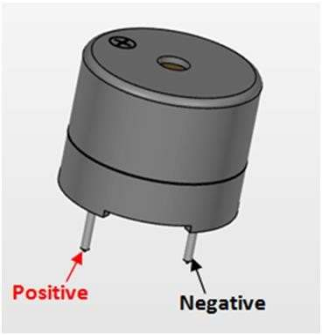

Fig 13 Active Passive Buzzer Pinout

Pin Number	Pin Name	Description
1	Positive	Identified by (+) symbol or longer terminal lead. Can be powered by 6V DC
2	Negative	Identified by short terminal lead. Typically connected to the ground of the circuit

Table 4.3 Buzzer Pin Configuration

- Buzzer Features and Specifications
- Rated Voltage: 6V DC
- Operating Voltage: 4-8V DC
- Rated current: <30mA
- Sound Type: Continuous Beep
- Resonant Frequency: ~2300 Hz
- Small and neat sealed package
- Breadboard and Perf board friendly
- Equivalents for Passive Buzzer
- Piezo Electric buzzer, Speaker, Active Passive Buzzer with Module

How to use a Buzzer

A buzzer is a small yet efficient component to add sound features to our project/system. It is very smalland compact 2-pin structure hence can be easily used on breadboard, Perf Board and even on PCBs which makes this a widely used component in most electronic applications.

There are two types are buzzers that are commonly available. The one shown here is a simple buzzer which when powered will make a Continuous Beeeeeeppp. sound, the other type is called a readymade

buzzer which will look bulkier than this and will produce a Beep. Beep. Beep. Sound due to the internaloscillating circuit present inside it. But, the one shown here is most widely used because it can be customised with help of other circuits to fit easily in our application.

This buzzer can be used by simply powering it using a DC power supply ranging from 4V to 9V. A simple 9V battery can also be used, but it is recommended to use a regulated +5V or +6V DC supply. The buzzer is normally associated with a switching circuit to turn ON or turn OFF the buzzer at requiredtime and require interval.

Applications of Buzzer

- Alarming Circuits, where the user has to be alarmed about something
- Communication equipments
- Automobile electronics
- Portable equipments, due to its compact size

4.1.8 GSM (Global System for Mobile communications)

Introduction:

GSM (Global System for Mobile communications) is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800 MHz bands. Some countries in the Americas use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated.

The rarer 400 and 450 MHz frequency bands are assigned in some countries, where these frequencies were previously used for first-generation systems.

GSM-900 uses 890–915 MHz to send information from the mobile station to the base station (uplink) and 935–960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz. Duplex spacing of 45 MHz is used. In some countries the GSM-900 band has been extended to cover a larger frequency range. This 'extended GSM', E-GSM, uses 880–915 MHz(uplink) and 925–960 MHz (downlink), adding 50 channels (channel numbers 975 to 1023 and 0) to the original GSM-900 band. Half rate channels use alternate frames in the sametimeslot. The channel data rate is 270.833 kbit/s, and the frame duration is 4.615 ms.

GSM Advantages:

GSM also pioneered a low-cost, to the network carrier, alternative to voice calls, the Short t message service (SMS, also called "text messaging"), which is now supported on other mobile standards as well. Another advantage is that the standard includes one worldwide Emergency telephone number, 112. Thismakes it easier for international travelers to connect to emergency services without knowing the local emergency number.

The GSM Network:

GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but do not address the hardware. The GSM network is divided into threemajor systems: the switching system (SS), the base station system (BSS), and the operation and supportsystem (OSS).

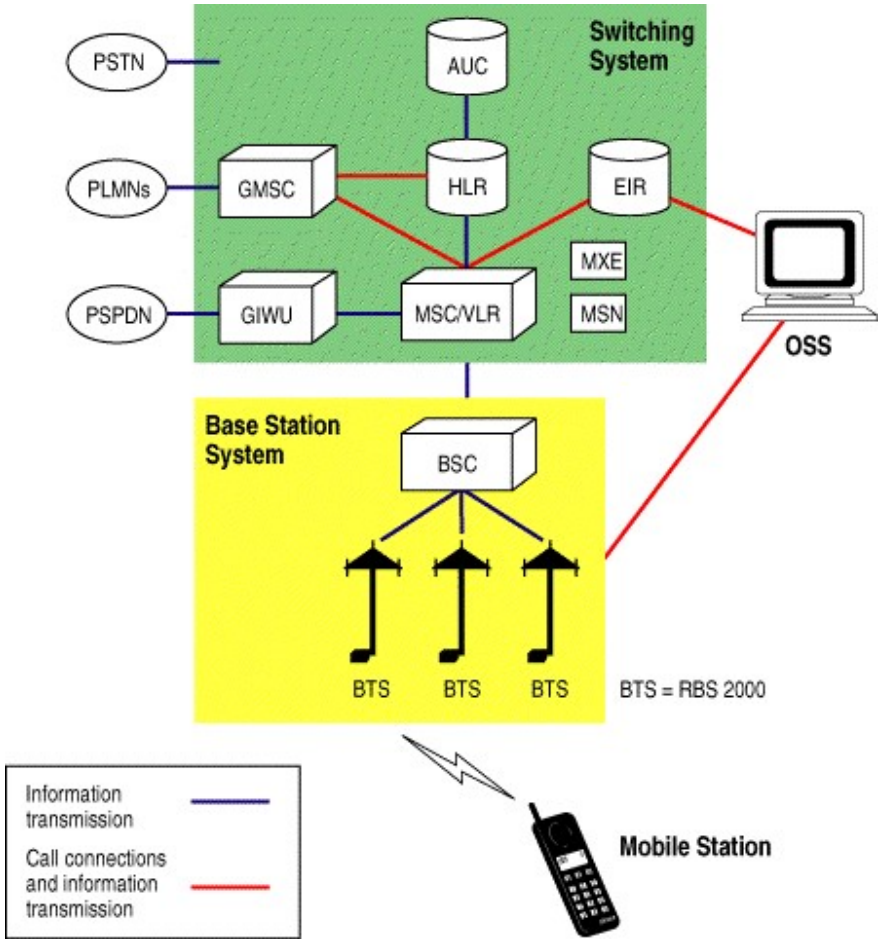

Fig 14. GSM working

The Switching System:

The switching system (SS) is responsible for performing call processing and subscriber-related functions. The switching system includes the following functional units.

Home location register (HLR): The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When anindividual buys a subscription from one of the PCS operators, he or she is registered in the HLR of thatoperator.

Mobile services switching center (MSC): The MSC performs the telephony switching functions of the system. It controls calls to and from other telephone and data systems. It also performs such functions as toll ticketing, network interfacing, common channel signaling, and others.

Visitor location register (VLR): The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes acall, the VLR will have the information needed for call setup without having to interrogate the HLR each time.

Authentication center (AUC): A unit called the AUC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The AUC protectsnetwork operators from different types of fraud found in today's cellular world.

Equipment identity register (EIR): The EIR is a database that contains information about the identity ofmobile equipment that prevents calls from stolen, unauthorized, or defective mobile stations. The AUCand EIR are implemented as stand-alone nodes or as a combined AUC/EIR node.

The Base Station System (BSS): All radio-related functions are performed in the BSS, which consistsof base station controllers (BSCs) and the base transceiver stations (BTSs).

BSC: The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control ofradio frequency (RF) power levels in base transceiver stations. A number of BSCs are served by an MSC.

BTS: The BTS handles the radio interface to the mobile station. The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTSs are controlledby a BSC.

The Operation and Support System:

The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS). The OSS is the functional entity from which operator monitors and controls the system.

The purpose of OSS is to offer the customer cost-effective support for centralized, regional and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation andmaintenance organizations.

Additional Functional Elements

Message center (MXE): The MXE is a node that provides integrated voice, fax, and data messaging.Specifically, the MXE handles short message service, cell broadcast, voice mail, fax mail, e-mail, and notification.

Mobile service node (MSN): The MSN is the node that handles the mobile intelligent network (IN) services.

Gateway mobile services switching center (GMSC): A gateway is a node used to interconnect twonetworks. The gateway is often implemented in an MSC. The MSC is then referred to as the GMSC. GSM inter-working unit (GIWU): The GIWU consists of both hardware and software that provides aninterface to various networks for data communications. Through the GIWU, users can alternate betweenspeech and data during the same call. The GIWU hardware equipment is physically located at theMSC/VLR.

GSM Network Areas:

The GSM network is made up of geographic areas. As shown in bellow figure, these areas include cells,location areas (LAs), MSC/VLR service areas, and public land mobile network (PLMN) areas.

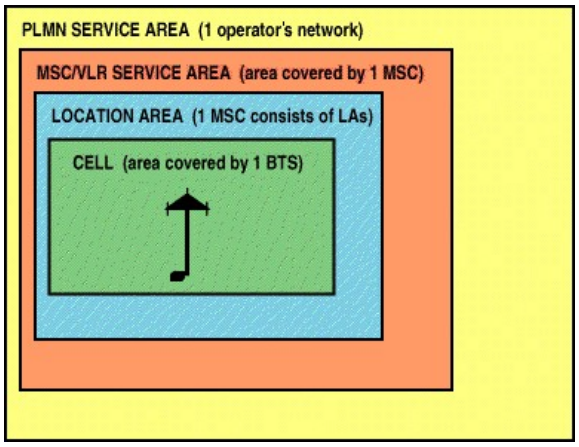

Fig 15.GSM network access

Location Areas:

The cell is the area given radio coverage by one base transceiver station. The GSM network identifies each cell via the cell global identity (CGI) number assigned to each cell. The location area is a group ofcells. It is the area in which the subscriber is paged. Each LA is served by one or more base station controllers, yet only by a single MSC Each LA is assigned a location area identity (LAI) number.

MSC/VLR service areas:

An MSC/VLR service area represents the part of the GSM network that is covered by one MSC and which is reachable, as it is registered in the VLR of the MSC.

PLMN service areas:

The PLMN service area is an area served by one network operator.

GSM Specifications:

Specifications for different personal communication services (PCS) systems vary among the differentPCS networks. Listed below is a description of the specifications and characteristics for GSM. Frequency band: The frequency range specified for GSM is 1,850 to 1,990 MHz (mobile station tobase station).

Duplex distance: The duplex distance is 80 MHz. Duplex distance is the distance between the uplinkand downlink frequencies. A channel has two frequencies, 80 MHz apart.

Channel separation: The separation between adjacent carrier frequencies. In GSM, this is 200 kHz. Modulation: Modulation is the process of sending a signal by changing the characteristics of a carrierfrequency. This is done in GSM via Gaussian minimum shift keying (GMSK).

Transmission rate: GSM is a digital system with an over-the-air bit rate of 270 kbps.

Access method: GSM utilizes the time division multiple access (TDMA) concept. TDMA is a technique in which several different calls may share the same carrier. Each call is assigned a particulartime slot.

Speech coder: GSM uses linear predictive coding (LPC). The purpose of LPC is to reduce the bit rate.The LPC provides parameters for a filter that mimics the vocal tract. The signal passes through this filter, leaving behind a residual signal. Speech is encoded at 13 kbps.

GSM Subscriber Services:

Dual-tone multi frequency (DTMF): DTMF is a tone signaling scheme often used for various controlpurposes via the telephone network, such as remote control of an answering machine. GSM supports full-originating DTMF.

Facsimile group III—GSM supports CCITT Group 3 facsimile. As standard fax machines are designedto be connected to a telephone using analog signals, a special fax converter connected to the exchangeis used in the GSM system. This enables a GSM–connected fax to communicate with any analog fax inthe network.

Short message services: A convenient facility of the GSM network is the short message service. A message consisting of a maximum of 160 alphanumeric characters can be sent to or from a mobilestation. This service can be viewed as an advanced form of alphanumeric paging with a number ofadvantages. If the subscriber's mobile unit is powered off or has left the coverage area, the message isstored and offered back to the subscriber when the mobile is powered on or has reentered the coveragearea of the network. This function ensures that the message will be received.

Cell broadcast: A variation of the short message service is the cell broadcast facility. A message of amaximum of 93 characters can be broadcast to all mobile subscribers in a certain geographic area. Typical applications include traffic congestion warnings and reports on accidents.

Voice mail: This service is actually an answering machine within the network, which is controlled bythe subscriber. Calls can be forwarded to the subscriber's voice-mail box and the subscriber checks formessages via a personal security code.

Fax mail: With this service, the subscriber can receive fax messages at any fax machine. The messagesare stored in a service center from which they can be retrieved by the subscriber via a personal securitycode to the desired fax number

Supplementary Services: GSM supports a comprehensive set of supplementary services that can complement and support both telephony and data services.

Call forwarding: This service gives the subscriber the ability to forward incoming calls to another number if the called mobile unit is not reachable, if it is busy, if there is no reply, or if call forwardingis allowed unconditionally.

Barring of outgoing calls: This service makes it possible for a mobile subscriber to prevent all outgoing calls.

Barring of incoming calls: This function allows the subscriber to prevent incoming calls. The following two conditions for incoming call barring exist: baring of all incoming calls and barring of incoming calls when roaming outside the home PLMN.

Advice of charge (AoC): The AoC service provides the mobile subscriber with an estimate of the callcharges. There are two types of AoC information: one that provides the subscriber with an estimate ofthe bill and one that can be used for immediate charging purposes. AoC for data calls is provided on the basis of time measurements.

Call hold: This service enables the subscriber to interrupt an ongoing call and then subsequently reestablish the call. The call hold service is only applicable to normal telephony.

Call waiting: This service enables the mobile subscriber to be notified of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call. Call waiting is applicableto all GSM telecommunications services using a circuit-switched connection.

Multiparty service: The multiparty service enables a mobile subscriber to establish a multiparty conversation—that is, a simultaneous conversation between three and six subscribers. This service is only applicable to normal telephony.

Calling line identification presentation/restriction: These services supply the called party with the integrated services digital network (ISDN) number of the calling party. The restriction service enables the calling party to restrict the presentation. The restriction overrides the presentation.

Closed user groups (CUGs): CUGs are generally comparable to a PBX. They are a group of subscribers who are capable of only calling themselves and certain numbers

Main AT commands: "AT command set for GSM Mobile Equipment" describes the Main AT commands to communicate via a serial interface with the GSM subsystem of the phone.

AT commands are instructions used to control a modem. AT is the abbreviation of Attention. Every command line starts with "AT" or "at". That's why modem commands are called AT commands. Manyof the commands that are used to control wired dial-up modems, such as ATD (Dial), ATA (Answer), ATH (Hook control) and ATO (Return to online data state), are also supported by GSM/GPRS modemsand mobile phones. Besides this common AT command set, GSM/GPRS modems and mobile phones support an AT command set that is specific to the GSM technology, which includes SMS-related commands like AT+CMGS (Send SMS message), AT+CMSS (Send

Note that the starting "AT" is the prefix that informs the modem about the start of a command line. Itis not part of the AT command name. For example, D is the actual AT command name in ATD and

+CMGS is the actual AT command name in AT+CMGS. However, some books and web sites use theminterchangeably as the name of an AT command.

Here are some of the tasks that can be done using AT commands with a GSM/GPRS modem or **mobilephone:** Get basic information about the mobile phone or GSM/GPRS modem. For example, name of manufacturer (AT+CGMI), model number (AT+CGMM), IMEI number (International Mobile Equipment Identity) (AT+CGSN) and software version (AT+CGMR).

Get basic information about the subscriber. For example, MSISDN (AT+CNUM) and IMSI number (International Mobile Subscriber Identity) (AT+CIMI).

Get the current status of the mobile phone or GSM/GPRS modem. For example, mobile phone activity status (AT+CPAS), mobile network registration status (AT+CREG), radio signal strength (AT+CSQ),battery charge level and battery charging status (AT+CBC).

Establish a data connection or voice connection to a remote modem (ATD, ATA,

etc).Send and receive fax (ATD, ATA, AT+F*).

Send (AT+CMGS, AT+CMSS), read (AT+CMGR, AT+CMGL), write (AT+CMGW) or delete (AT+CMGD) SMS messages and obtain notifications of newly received SMS messages (AT+CNMI).Read (AT+CPBR), write (AT+CPBW) or search (AT+CPBF) phonebook entries.

Perform security-related tasks, such as opening or closing facility locks (AT+CLCK), checking whethera facility is locked (AT+CLCK) and changing passwords (AT+CPWD).

(Facility lock examples: SIM lock [a password must be given to the SIM card every time the mobile phone is switched on] and PH-SIM lock [a certain SIM card is associated with the mobile phone. To use other SIM cards with the mobile phone, a password must be entered.])

Control the presentation of result codes / error messages of AT commands. For example, you can controlwhether to enable certain error messages (AT+CMEE) and whether error messages should be displayedin numeric format or verbose format (AT+CMEE=1 or AT+CMEE=2).

4.1.9 Motor

Motors can be found practically everywhere. This guide will help you learn the basics of electric motors,available types and how to choose the correct motor. The basic questions to answer while deciding which motor is most appropriate for an application are which type should I choose and whichspecifications matter.

How do motors work?

Electric motors work by converting electrical energy to mechanical energy in order to create motion. Force is generated within the motor through the interaction between a magnetic field and winding alternating (AC) or direct (DC) current. As the strength of a current increases so does the strength of the magnetic field. Keep Ohm's law (V = I*R) in mind; voltage must increase in order to maintain the same current as resistance increases.

Electric Motors have an array of applications. Conventional industrial uses include blowers, machine and power tools, fans and pumps. Hobbyists generally use motors in smaller applications requiring movement such as robotics or modules with wheels.

Fig 16. Motor

4.1.10 Relay

This is where relay modules come into play. These well-contained modules are inexpensive, simple toconnect, and ideal for home-brew projects that require switching modest amounts of AC or DC power.The only downside is that, because these are elector-mechanical devices, they are more prone to wear and tear over time.

This tutorial will walk you through setting up the relay module to turn on a lamp or other device, but first, a quick primer on relays.

How Do Relays Work?

At the core of a relay is an electromagnet (a wire coil that becomes a temporary magnet when electricityis passed through it). A relay can be thought of as an electric lever; you turn it on with a relatively smallcurrent, and it turns on another device with a much larger current.

Relay Basics

Here's a small animation showing how a relay links two circuits together.

To illustrate, think about two simple circuits: one with an electromagnet and a switch or sensor, and theother with a magnetic switch and a light bulb.

Initially, both circuits are open, with no current flowing through them.

When a small current flows through the first circuit, the electromagnet is energized, creating a magneticfield around it. The energized electromagnet attracts the second circuit's contact, closing the switch andallowing a large current to flow.

When the current in the first circuit stops flowing, the contact returns to its original position, reopeningthe second circuit.

Relay Operation

A relay typically has five pins, three of which are high voltage terminals (NC, COM, and NO) thatconnect to the device being controlled.

The device is connected between the COM (common) terminal and either the NC (normally closed) orNO (normally open) terminal, depending on whether the device should remain normally on or off.

Between the remaining two pins (coil1 and coil2) is a coil that acts as an electromagnet.

Normally (initial position), the COM terminal is connected to the NC terminal and the NO terminal is open.

When current flows through the coil, the electromagnet becomes energized, causing the switch's internal contact to move. The COM then connects to the NO terminal, disconnecting from the NC terminal.

When the current stops flowing through the coil, the internal contact is returned to its initial position, re-connecting the NC terminal to the COM and re-opening the NO terminal.

To put it another way, the relay functions as a single-pole-double-throw switch (SPDT).

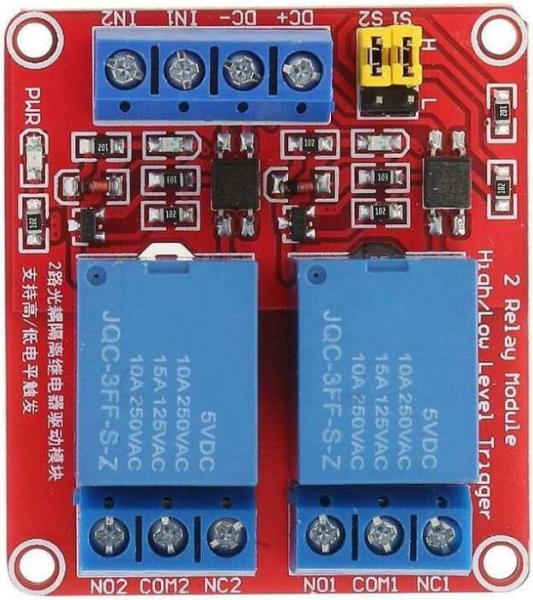

Fig 17. relay module

4.2 SOFTWARE TOOLS

4.2.1 ARDUINO SOFTWARE

The Arduino is a family of microcontroller boards to simplify electronic design, prototyping and experimenting for artists, hackers, hobbyists, but also many professionals. People use it as brains for their robots, to build new digital music instruments, or to build a system that lets your house plants tweet you when they're dry. Arduinos (we use the standard Arduino Uno) are built around an ATmegamicrocontroller — essentially a complete computer with CPU, RAM, Flash memory, and input/output

What you will need:
A computer (Windows, Mac, or Linux)
An Arduino-compatible microcontroller (anything from this guide should work)
A USB A-to-B cable, or another appropriate way to connect your Arduino-compatible microcontrollerto your computer (check out this USB buying guide if you're not sure which cable to get).

Fig 18. Arduino Uno

fig 19. Arduino cable

An Arduino Uno

Windows 7, Vista,

and XP

Installing the Drivers for the Arduino Uno (from Arduino.cc)

Plug in your board and wait for Windows to begin it's driver installation process After a few moments,the process will fail, despite its best efforts.

Click on the Start Menu, and open up the Control Panel

If there is no COM & LPT section, look under 'Other Devices' for 'Unknown Device

Right click on the "Arduino UNO (COMxx)" or "Unknown Device" port and choose the "UpdateDriver Software" opti Next, choose the "Browse my computer for Driver software" option

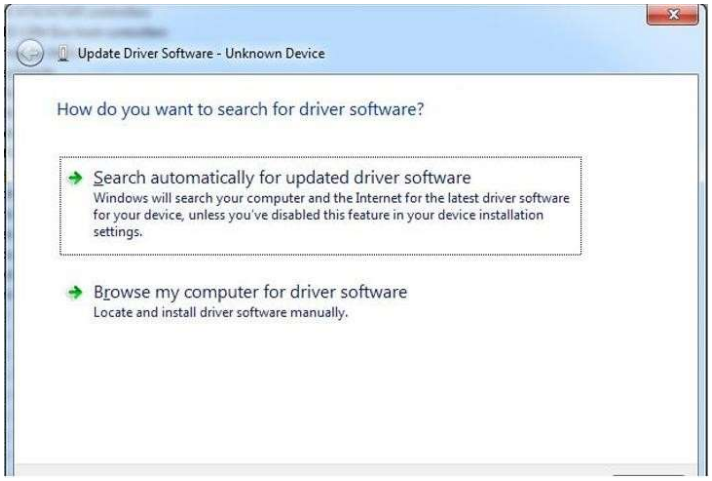

Fig 20 . search for drivers

Finally, navigate to and select the Uno's driver file, named "ArduinoUNO.inf", located in the "Drivers"folder of the Arduino Software download (not the "FTDI USB Drivers" sub-directory). If you cannot see the .inf file, it is probably just hidden. You can select the 'drivers' folder with the 'search sub- folders' option selected instead. Windows will finish up the driver installation

LAUNCH AND BLINK!

After following the appropriate steps for your software install, we are now ready to test your firstprogram with your Arduino board!

Launch the Arduino application

If you disconnected your board, plug it back in

Open the Blink example sketch by going to: File > Examples > 1.Basics > Blink

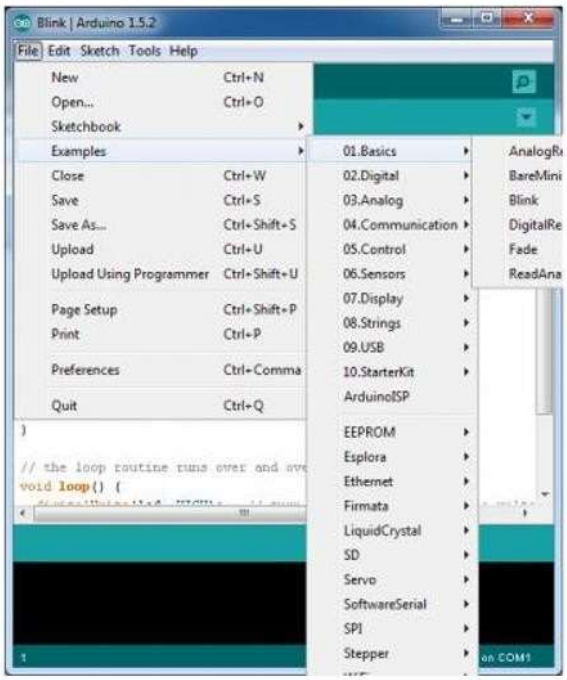

Fig 21. blink

Select the type of Arduino board you're using: Tools > Board > your board type

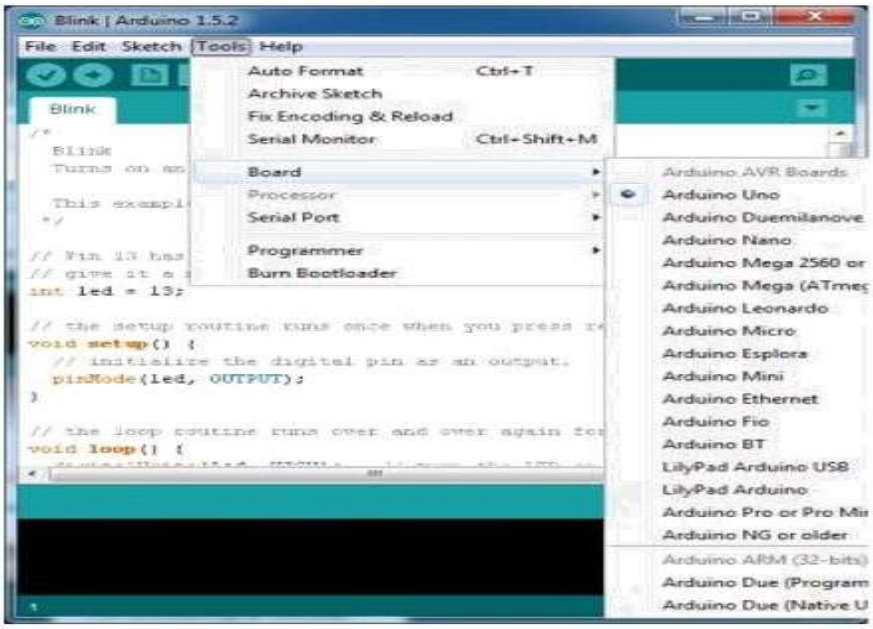

Fig 22 . select board

Select the serial/COM port that your Arduino is attached to: Tools > Port > COMxx

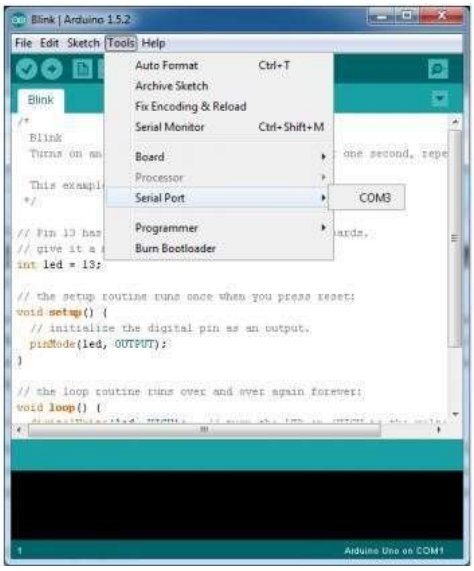

Fig 23. select serial port

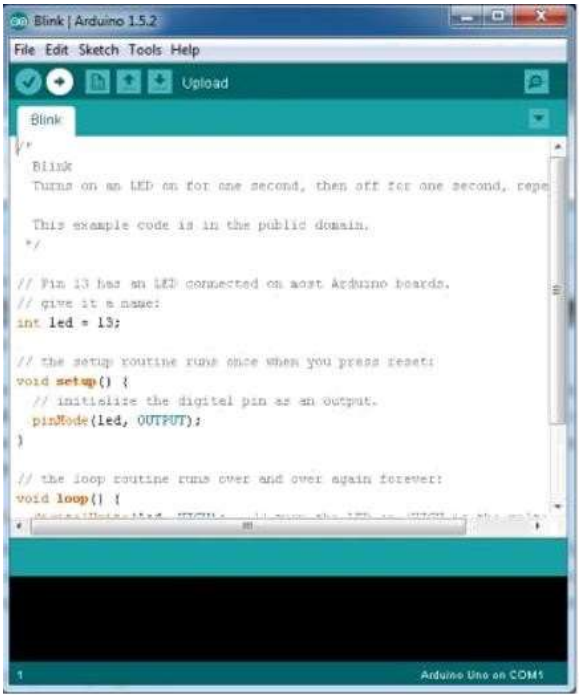

Fig 24. blink code

If you're not sure which serial device is your Arduino, take a look at the available ports, then unplugyour Arduino and look again. The one that disappeared is your Arduino.

With your Arduino board connected, and the Blink sketch open, press the 'Upload' button

After a second, you should see some LEDs flashing on your Arduino, followed by the message 'DoneUploading' in the status bar of the Blink sketch.

If everything worked, the onboard LED on your Arduino should now be blinking! You just programmedyour first Arduino!

CHAPTER 5
DESIGN AND IMPLEMENTATION

5.1 Block Diagram

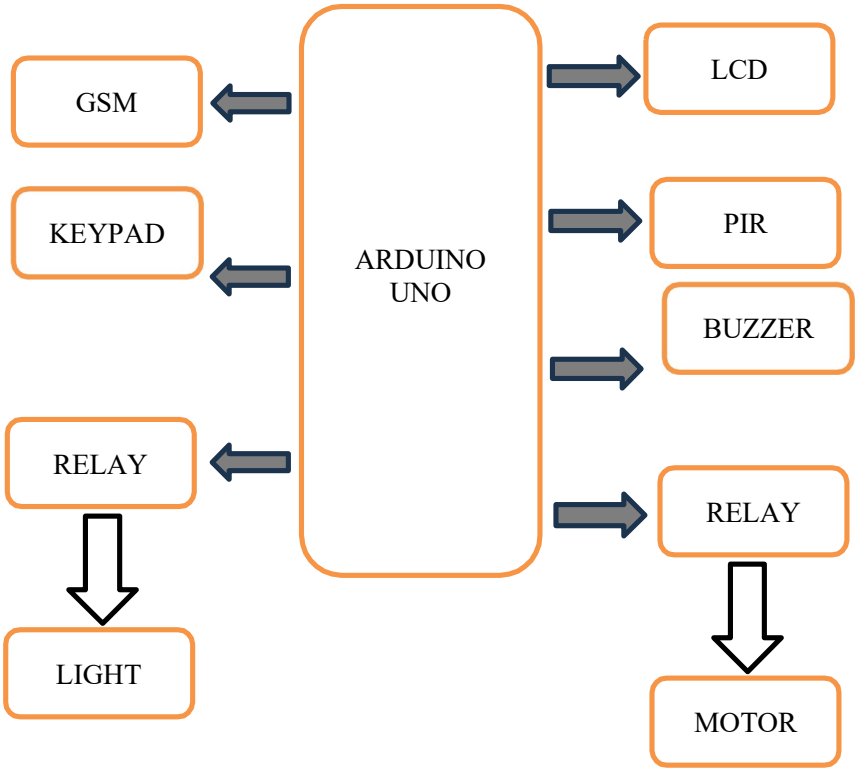

Fig 25. Block diagram

Block diagram Description

Various important blocks of system are:

1. Arduino UNO:

This is the CPU (central processing unit) of our project. An Arduino uno is being used here. Thevarious functions like:

I. Reading the digital input from Keypad

II. Sending this data to LCD so that the person operating this project should read the password

III. Sensing the password using keypad and to check whether it is a correct password or a wrongpassword and rotate the stepper motor if the password entered is a correct password.

IV. Sending the data to the GSM modem using serial port. This data consists of the status of enteredpassword (Correct/wrong)

2. LCD:

We are going to use 16x2 alphanumeric Liquid Crystal Display (LCD) which means it can displayalphabets along with numbers on 2 lines each containing 16 characters.

3. Buzzer:

The buzzer is to indicate the wrong password to open the door.

4. Keypad:

User will enter the password using the keypad. Various keys of keypad are as following,E for Enter
I for
Increment
D for
Decreme
nt

5. PIR SENSOR:

Here we use PIR sensor for motion detection

6.GSM modem:

User need to send various messages to the owner of bank locker. GSM modem is chosen for thispurpose.

7. DC Motor:

It is used to show demo of locker opening.

8. RELAY

This is used to turn on light and buzzer

5.2 FLOW CHART

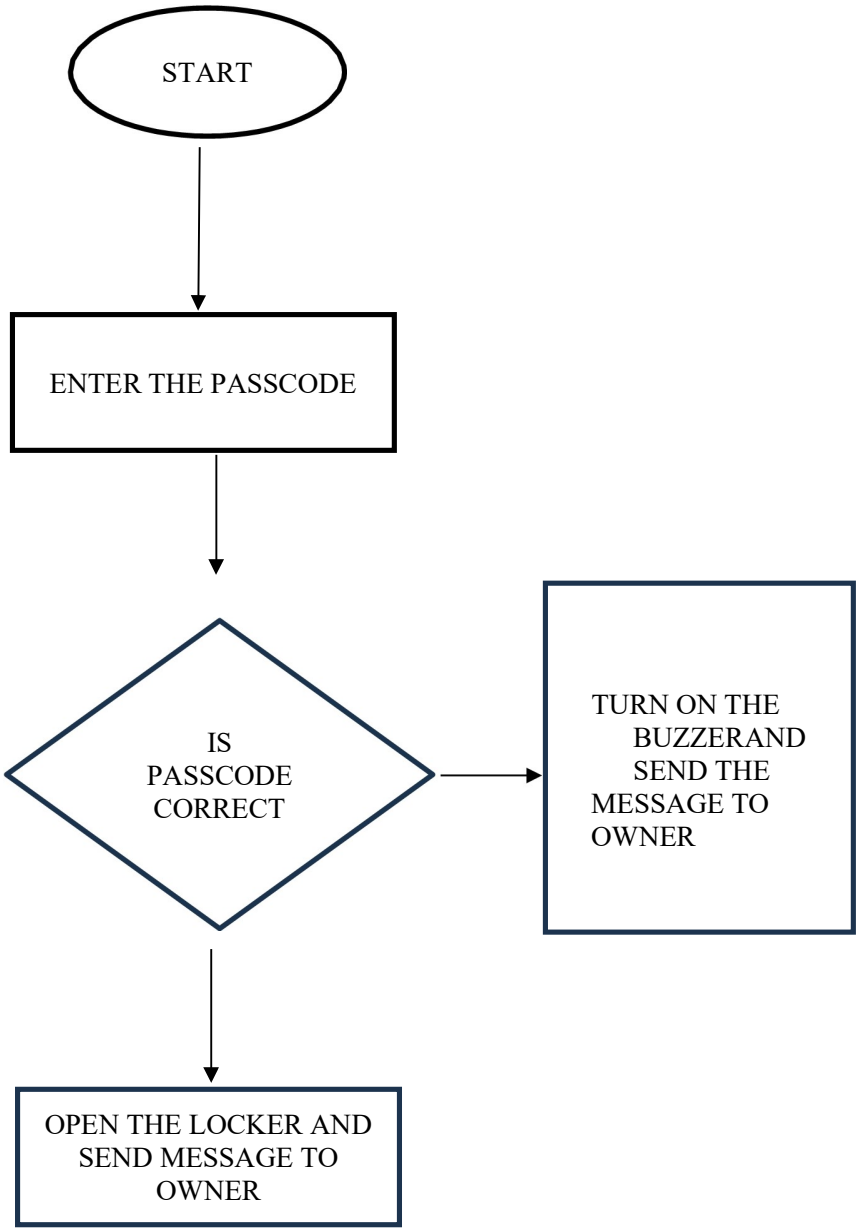

Fig 26. Flow Chart

Steps of Process Flow

1. Start the process

Connect the components according to block diagram. And give the power supply to the project.

2. Initialize the Arduino UNO and GSM Module

Now upload required code into the arduino.

Now insert sim into the gsm.

Now we need to register the sim number to gsm using message to get required information to it.

3. detecting the motion

Pir sensor is used to detect the moving object and send sms to registered mobile number.

4.Enter the Password Through Keypad

5.UNO verifies the first password using stored data.

6.right password/otp .

If the entered password is correct and verified by UNO then a message saying access granted isdisplayed on LCD display and the DC motor is turned on showing the opening of the locker.

7.wrong password/otp.

When the entered password is incorrect buzzer will be turned and message is sent to the owner.

8.Stop.

5.3 ADVANTAGES

Eliminates the continuously monitoring, it facilitates 24 hours a day, 365 days in year communicationbetween system and user.

- Easy to install & simple in operation.
- Low cost, high reliability & flexibility.

5.4 LIMITATIONS

If the GSM network used in mobile does not have any coverage then the operation can not beperformed.

5.5APPLICATIONS

The proposed system can be efficiently used in banks and industries, offices including othercommercial organizations too.

CHAPTER 6
RESULTS AND DISCUSSIONS

6.1 RESULT

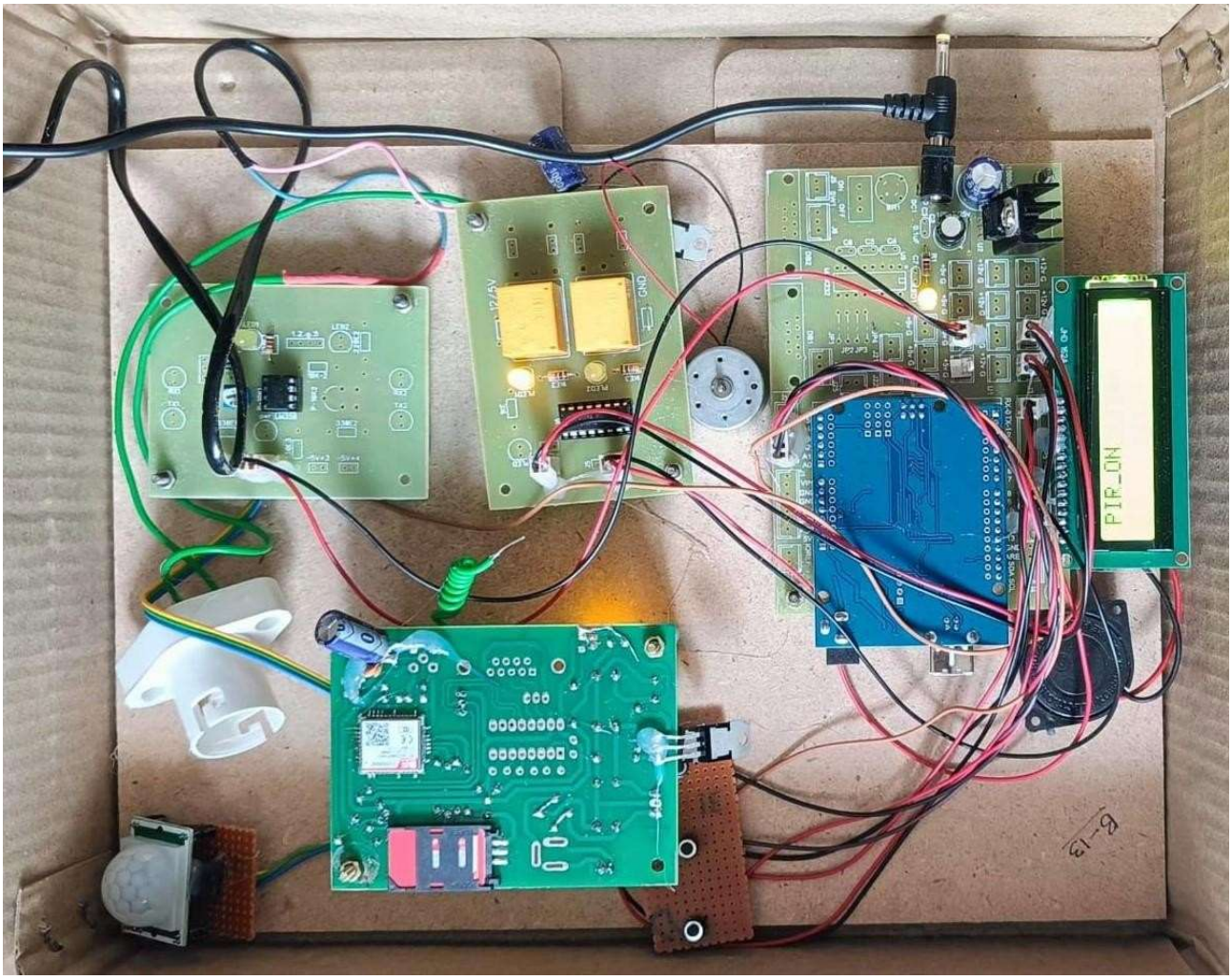

Fig 27. SMS BASED BANKING SECURIY SYSTEM

Output received to mobile while entering wrong and correct password

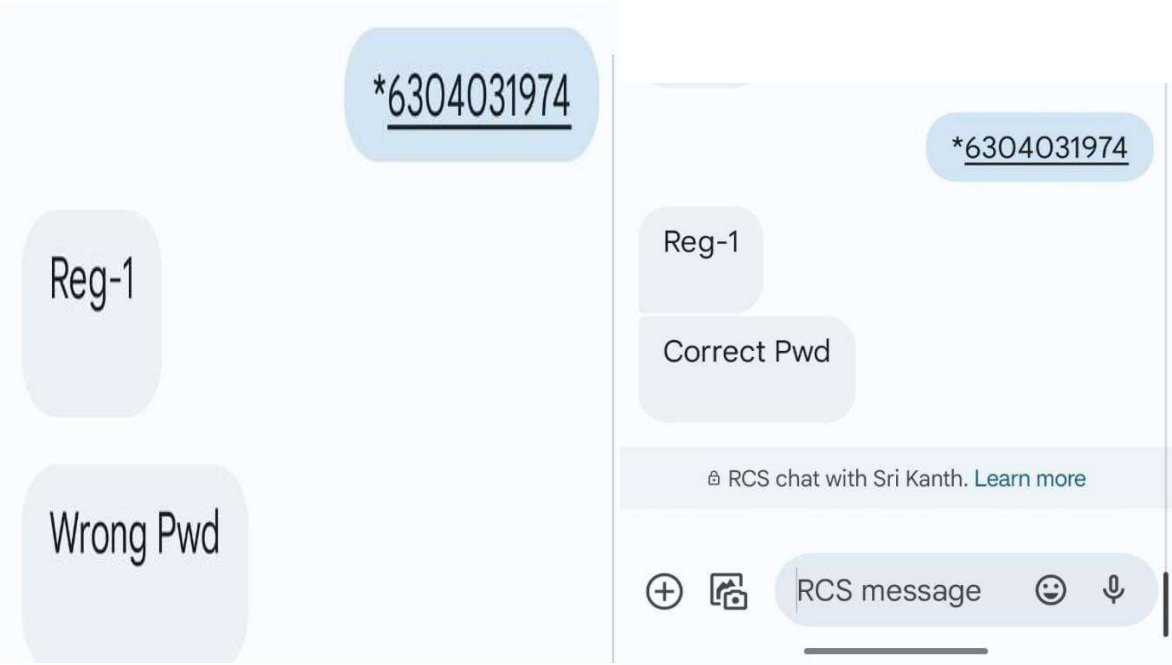

Fig 28. Result with Wrong password and Correct password

6.2 CONCLUSION

With the knowledge of emerging new techniques in 'electronics" the lives of people are moresheltered and safe. One such application of electronics is used in "GSM based bank locker security system" The approach to be followed is explained thoroughly which makes us to achieve the target efficiently satisfying user's needs and requirements.

GSM based bank locker security system is automatic and very versatile system. It can beimplemented in commercial organizations, firms and homes. It provides flexibility and system reliability with low cost as well as less maintenance,

It provides remote access to the system to deliver service at any time of the day without any hassles and providing us sufficient information of the security of the locker and situation. With the implementation of this system one can not only protect their prized possessions but also can control and monitor the devices at remote locations which makes it even more structured, systematic and efficient to use.

6.3 FUTURE SCOPE

The future scope of the project is to develop a smart bank locker security system using facial, iris and retina scanning for virtual identification; in addition a voice feedback system can be provided which would further increase the efficiency and security. Fire sensors and wind sensors can be added to the current design for increased safety from external damages.

6.4 REFERENCES

[1] Sagar S. Palsodkar, Prof S.13. Patil, "Review: Biometric and GSM Security for Lockers"Int. Journal of Engineering Research and Applications, Vol. 4, Issue 12(Part 6), December 2014.

[2] R.Ramani, S. Selvaraju, S. Valarmathy, P.Niranjan, "Bank Locker Security System basedon RFID and GSM Technology", International Journal of Computer Applications (0975-8887)Volume 57-No.18, November 2012.

[3] P. Sugapriya, K. Amsavalli, "Smart Banking Security System Using PatternAnalyzer", International Journal of Innovative Research in Computer and Communication Engineering Vol.3, Special Issue 8, October 2015.

[4] M. Sai Divya, M. Nagabhushan Rao, "Centralized Authentication Smart Locking System using RFID, Fingerprint, Password and GSM", International Journal of Engineering &Technology, July 2018.

[5] Subhash H. Jadhav, S. S. Agrawal, "Smart Bank Locker Security System Using BiometricFingerprint and GSM Technology", International Journal of Science and Research (2319- 7064), Volume 5, 10, October 2016.

[6] Ashish M. Jaiswal and MahipBartere, "Enhancing ATM Security Using Fingerprint And GSM Technology", International Journal of Computing Science and Mobile Computing Vol.3, Issue. 4, April 2014.

[7] Vaijanath R. Shintre, Mukesh D. Patil, "Banking Security System Using PSoC". International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015.

[8] Tarief M. F. Elshafiey, "Design and Implementation of a museum and bank security systemusing antenna as IR proximity sensor and PSoC Technology", IEEE symposium on wireless technology and applications, September 25-28 Malaysia 2011.

[9] Pramila D Kamble and Dr. Bharti W. Gawali "Fingerprint Verification of ATM Security System by Using Biometric and Hybridization" International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.

[10] SanalMalhotra, "Banking Locker System With Odor Identification & Security Question Using RFID GSM Technology". International Journal of Advances in Electronics Engineering - JAEE Volume 4: Issue 3.