INDEX

CHAPTER-1

CHAPTER-2

CHAPTER-3

CHAPTER-4

CHAPTER-5

ABSTRACT

Safety locks play an important role in protecting valuable materials for a person or a group of people.Safety locks vary from being simple to complex Simple in design are easy to use and often easy to break through as well, while complex locks are difficult to penetrate but laborious to use Advanced locking systems are expensive and difficult to install. This paper aims to build secure and easy to use security system based on incorporating Android smartphone in controlling the locking operation System hardwired is implemented using Arduino, SIM 900, servo motor and LCD screen. System software was implemented using two software. The first one is used to build the controlling statements of the system in Arduino controller using "ARDUINO IDE" software, while second one "MIT APP INVENTPR" which is used to build a GUI for interfacing between user and the system .System testing gives good performance by giving high level of security.

CHAPTER – 1

INTRODUCTION

1.1 Introduction to Project

A smart lock is an electromechanical lock that is designed to perform locking unlocking operations on a door when it receives a prompt via an electronic keypad, biometric sensor, access card, Bluetooth, or Wi-Fi from a registered mobile device.

These locks are called smart locks because they use advanced technology. Internet communication to enable easier access for users and enhanced security from the main components of the smart lock which can be controlled system to the major access and send alerts in response to the different events it monitors as well as other events related to the status of the device. Smart locks can be considered part of a smart most smart locks are installed on mechanical locks (simple types of locks, including and ordinary lock. Recently, smart locking controllers have also appeared at the market.

Smart locks, like the traditional locks, need two main parts to work the lock and In the case of these electronic locks, the key is not a physical key but or a special configured explicitly for this purpose which wirelessly performs the authentication needed to automatically unlock the door.

Fig:1.1:Sensor Lock

Smart locks allow users to grant access to a third party by means of a virtual key. This key can besent to the recipient smartphone over standard messaging protocols such as email or wifi.Certain smart locks include a built-in Wi-Fi connection that allows for monitoringfeatures such as access notifications or cameras to show the person requesting access. Some smart locks

work with to allow the user to see who and when someone is at a door. Many smart locks now also feature biometric features such as fingerprint sensors. Biometrics are becoming increasingly popular because they offer more security than passwords alone. This is because they use unique physical characteristics rather than stored information.

Smart locks may us Bluetooth energy and SSI to communicate, encrypting communications. Industrial smart locks are a branch of the smart lock field. They are an iterative product of mechanical locks like smart locks. However, the application areas of industrial smart locks are not smart homes, but fields that have extremely high requirements for key management, such as communications, power utilities, water utilities, public safety, transportation, data centers, etc.Industry smart locks mainly have three components: locks and keys, and management systems.

Similarly, the key is no longer a physical key, but a special electronic key. When unlocking, the unlocking authority needs to be assigned before.Through the management system, the administrator needs to set the user, unlock date and time period for the key. Whenever the user unlocks or locks the lock, the unlock record will be saved in the key. The unlocking record can betracked through the management software.

1.2 Introduction to Embedded System

An **embedded system** is a computer system that is designed to perform a specific task or set of tasks. It is a combination of computer hardware and software that is integrated into a larger system. Embedded systems are used in various applications such as home appliances, transportation, healthcare, business sector & offices, defence sector, aerospace, and agricultural sector. The three main components of an embedded system are hardware, software, and firmware. Hardware refers to the physical components of the system such as microprocessors or microcontrollers.

Software refers to the programs that run on the hardware. Firmware is a type of software that is embedded in the hardware and is responsible for controlling the system. An Embedded system is a special- purpose system in which the computer is completely encapsulated by or dedicated to the device or system it controls. Unlike a general-purpose computer, such as a personal computer, an Embedded System performs one or few predefined Tasks usually with very specific requirements. Since the system is dedicated to specified tasks, design engineers can

optimize it, reducing the size and cost of the product. Embedded Systems are often mass-produced, benefiting from economies of scale.

Characteristics of Embedded System:

- An embedded System is any computer system hidden inside a product other than a computer.
- Throughput – Our system may need to handle a lot of data in short period of time.
- Response – Our system may need to react to events quickly.
- Test ability- Setting up equipment to test embedded software can be difficult.
- Debug ability- Without a screen or a keyboard, finding out what the software is doing wrong is a troublesome problem.
- Reliability – Embedded Systems must be able to handle any situation without human intervention.
- Memory Space - Memory is limited on Embedded Systems, and you must make the software and the data fit into whatever memory exists.
- Power Consumption – Portable systems must run on battery power, and the software in these systems must conserve power.
- Processor hogs- Computing that requires large amounts of CPU time can complicate the response problem.

1.3 Introduction to IOT

INTERNET OF THINGS (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order tocommunicate Interaction amongst each other or with respect to the external environment. In the upcoming years, IoT-based technology will offer advanced levels of services and practically away people lead their daily lives. Advancements in medicine, power, gene therapy agriculture, smart cities, and smart homes are just a very few of the categorical example where IoT is strongly established.

IoT is network of interconnected computing devices which are embedded in everyday objects, enabling them to send and receive data. With more than 7 billion connected IOT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025. Oracle has a network of device partners.

The most important features of IoT on which it works are connectivity, integrating, active engagement, and many more. Connectivity refers to establish a proper connection between all the things of IoT platform it may be server or cloud. After connecting the IoT devices, it needs a highspeed messaging between the devices and cloud to enable reliable, secure and bi-directional communication. IoT makes things smart and enhances life through the use of data. For example, if we have a coffee machine whose beans have going to end, then the coffee machine it orders the coffee beans of your choice from the retailer.The most important features of IoT on which it works are connectivity,analysing, integrating, active engagement, and many more. Some of them are listed below:

Connectivity: Connectivity refers to establish a proper connection between all the things of IoT platform it may be server or cloud. After connecting the IoT devices, it needs a high speed messaging between the devices and cloud to enable reliable,secure and bi-directional communication.

Analysing: After connecting all the relevant things, it comes to real-time analysing the data collected and use them to build effective business intelligence. If we have a good insight into data gathered from all these things, then we call our system has a smart system.

Integrating: IoT integrating the various models to improve the user experience as well.

Artificial Intelligence: IoT makes things smart and enhances life through the use of data. For example, if we have a coffee machine whose beans have going to end, then the coffee machine it orders the coffee beans of your choice from the retailer.

Sensing: The sensor devices used in IoT technologies detect and measure any change in the environment and report on their status. IoT technology brings passive networks to active networks. Without sensors,there could not hold an effective or true Iot environment.

Active Engagement: IoT makes the connected technology, product, or services to active engagement between each other.

Endpoint Management: It is important to be the endpoint management of all the IoT system otherwise,it makes the complete failure of the system. For example, if a coffee machine itself order the coffee beans when it goes to end but what happens when it orders the beans from a retailer and we are not present at home for a few days, it leads to the failure of the IoT system.

1.4 Need of IoT

The Internet of Things (IoT) stands as a transformative force, reshaping our interactions with the world and revolutionizing diverse aspects of our daily lives. At its core, IoT thrives on connectivity, fostering seamless communication between devices and promoting interoperability.. Through automation, IoT enhances efficiency by enabling devices to operate autonomously based on predefined conditions or real-time data, reducing the need for constant human intervention. In the realm of smart cities, IoT contributes to urban development by introducing intelligent transportation systems, energy management, and sustainable practices, thereby enhancing overall quality of life.

Health care benefits from IoT through wearables and remote monitoring tools, offering personalized insights and timely interventions. Industries leverage Industrial IoT (IIoT) to optimize manufacturing processes, monitor equipment health, and implement predictive maintenance strategies, leading to increased productivity and cost savings. From smart homes with connected appliances to environmental monitoring and supply chain optimization, IoT's impact is far-reaching, creating a more connected, efficient, and intelligent world across various domain

CHAPTER -2

LITERATURE SURVEY

2.1 Introduction:

There are many automated advanced door locking system has been developed and it's popularly used in commercial buildings and organization. Some of these automated doors locking system are based on RFID (Radio Frequency Identification). The RFID cards are used as a key. The RFID card reader detects and validates the user accessibility. When the card is brought near the reader, it identifies the radio frequency of the card and thus verifies the key.

However these systems are expensive. Various control systems have been designed over the years to prevent access to unauthorized user. The main aim for providing locks for our home, school, office, and building is for security of our lives and property. It is therefore important to have convenient way of achieving this goal. Automatic door locking system has become a standard feature on many different types of buildings and homes.

1.Smart Door Lock System using Android Applications

It also provides real-time notifications for door opening with the door lock, forced door opening, overheating detection, and battery condition . Another resource I found is an article that presents a method of locking the door of a smart home using an Android app. The app uses Bluetooth to connect to the lock and allows you to lock and unlock the door using voice commands . A third resource I found is a list of the top-rated smartphone door locks, which includes the Tinxy app that can operate on the Android platform as well as iPhones. The app allows you to unlock your door from anywhere on a variety of devices, check if the door is locked or not with your phone, and get notified when family members open the house's doors

2.How Smart Door lock System using Voice Recognition

One of the resources I found is a project by Jithin Sanal that uses Amazon's Alexa skill to automatically secure a custom door locking mechanism without the need for Bluetooth or a fingerprint. The project is based around a Nano RP2040 Connect and can talk with the Arduino

Cloud . Another resource I found is an article that presents two methods of locking the door of a smart home: using voice commands (lock and unlock the door) and controlling the lock by facial recognition using an Android app .

A third resource I found is a chapter from a book that describes how the use of Internet of things (IoT) allows transformation of a conventional door locking into an automated door locking system that leads to smart security system at home. The IoT-based door locking system can detect home user, monitors for authentication, manage locking/unlocking the door, and alert home users if any intruder is identified . Finally, I found a tutorial on how to make a door lock which can be controlled with voice commands. The tutorial uses a Voice Recognition Module V3, which is trained first and then gives voice recognition results. The Voice Recognition Module is a compact and easy-control speaking recognition board .

3.Smart Door Lock System based on Gesture Human Machine Interface

I found a few resources that might be helpful in answering your question. One of the resources I found is a paper that describes a smart door lock system with fingerprint interface. The system uses a fingerprint sensor, a GSM module, a motor driver, a motor, and some other hardware devices to create a smart and affordable door lock. The fingerprint sensor is integrated into the door panel, facing the outer side of the door, so that people can't have access to the controlling system from outside. The latches will be fixed inside the door panel, so that the thickness of the door can help the latch's strength. The system will also go into a secure state where it will continue to buzz the buzzer to alert the neighbors that something is wrong. The system will be reset once a known print will be entered .

Another resource I found is a paper that presents a low-cost smart door locking system capable of making decisions based on facial recognition technology. The system operates through a combination of Arduino UNO and Android-based smartphone.

Some of the side benefits that come here are ease of opening the door lock without using keys, avoiding inconvenience caused by losing keys, no problem even in case of forgetting to carry keys. The purpose of the study was to look at the characteristics and drawbacks of the existing door lock systems that are utilized for security related objectives. The remaining section of this paper is as follows. The literature review includes the related systems of smart door locks

that have been done so far in the security domain. The discussion section includes an idea about the experience level of using these systems. Moreover, the discussion includes the technologies and features used in existing systems. Finally, the paper includes a conclusion and further work.

Door lock security systems are classified based on technology used as 1) Password based, 2) Biometric based, 3) GSM based, 4) smart card based, 5) RFID based, 5) Door phone based, 6) Bluetooth based, 7) Social networking sites based, 8) OTP based, 9) Motion detector based, 10) VB based, 11) Combined system.

2.2 Password Based Systems

The programmable electronic code lock device is programmed in such a way that it will operates only with the correct entry of predefined digits. It is also called an integrated combinational type lock

Based on the programmable electronic code lock, the reprogrammable digital door locks were invented in that the password can change any time as it stored in PROM. For operating the device, GSM/CDMA module can be used. When any person calls up from his phone, the call will be received by the system. And the door will opens only if the call is from specified user.: Password Protected Door Locking System based on Cell Phone A cellphone controlled password protected door lock system which was proposed to open the door with the help of cell phone device by entering a specific code. The user can make a call to a systems number. This call is responsible for opening or closing of the entry with the use of correct password. In latest password based system, a more advanced system develops which communicates the owner of the office or house, when any unauthorized person tries to open the code, by giving correct code as well. While closing the door of office/home, the owner has to press the 0 key available on the hex keypad and leave the system. The system developed by Annie P. Oommen et.allows for changing the password. To open the lock, the entered password must matches with the changed one. In some systems the security dial-up enables through the GSM modem , when the unauthorized person enters an invalid password then the controller informs to the owner through GSM modem. Latest security system is designed where the locking security system can be enhanced with the help of RF and GSM wireless technology by using a 4 digit password which provides the authentication.

2.3 Biometric Based System

The palmtop recognition is the next step for fingerprint recognition. It operates on the image of palmtop. Firstly system takes an image of the palmtop then it works on that image by partitioning it and process is required. At the end, verify the right person. Hence, it reduces the chances of error in other human recognition methods and clarifies the problems which were faced in the fingerprint recognition. The biometric technique is very useful in bank lockers. Except fingerprint recognition the vein detector and iris scanner gives best and accurate result so, in the bank security system , microcontroller continuously monitors the Vein Detector and Iris Scanner through keypad authenticated codes. During night the wireless motion detector will be active, if any variation occurs in its output, it will be sensed by the controller and alert sounds will be given by it. Recently, the fast based principal component analysis approach is proposed in which the modification of principal component analysis approach for the face recognition and face detection process is done. The image is captured by the web camera and it gets matched with the image stored in the database. New advanced door lock security systems are available based on the pattern of the human iris for providing a high level of security. And to make the system more efficient n reliable the simulation is done in MATLAB .

2.4 GSM Based Systems

In many door lock security systems, GSM is used for communication purpose. The purpose of a work cultivated by utilization of a circuits like a GSM module which gets activated by a controller for sending SMS in emergency to proprietor and for sending corresponding services of security at the time of break in. For detecting obstacles, the system requires various sensors. It gathers data from the sensors and settles on a choice. With the help of GSM module, sends SMS to a respective number. A recently created model for security of door easily controlled like remote control operations by a GSM hand set acts as the transmitter and the other GSM phone set with the DTMF associated with the motor attached to door with the use of DTMF decoder, a stepper motor and microcontroller unit. Nowadays people want to be secure though they are away from home so, the work proposed by Jayashri Bangali et. When the owner is not at his home, security of home and important things is the big issue in front of all. Two frameworks were created which depends on GSM based technology. For detection of the gate-crashes, it takes place by capturing image through web camera. When peoples are not at their homes, the system sends notification in terms of SMS to the crisis number. A novel administrator based system can login without any

stretch to the system and can see guests record and listen their recorded messages and also automatically lock the door using mobile communication technology.

2.5 Smart Card Based System

A model entryway security framework is intended to permit an authorized person for getting a safe (without need of any key) entryway where valid card of smart RFID is necessary for ensuring the pass of the door. Total control activity is performed by the microcontroller.

2.6 RFID Based Systems

These types of security systems used for digital door lock are utilizing inactive RFID tags (passive). With the help of this, it ensures that only valid person can get entry. Such systems are working in real time basic for opening the door in which user have to place the tag in contact with RFID detector, then the entryway gets opens and in the central server the registration data is stored with necessary data of the users. Attendance and person tracking is possible by using such type of system. RFID Based Gate Access Security System which points out authorized peoples and permits just them was effectively created by K.Srinivasa et. al. . This system ought to have the capacity to minimize the trained or specialized human error during secured door access. Latest RFID based door lock security system are based on arduino platfor with audio acknowledgement at the point when card put close to the RFID module, it peruses International Journal of Computer Applications (0975 – 8887) Volume 153 – No2, November 2016 15 the card data and it matches with the data stored in the program memory and shows authorize/unauthorized entry. Arduino is also used by many other applications for example A specific Arduino ATMEL processor can be used for sensing and recognition of person another example like ECG Parameter Identification and Monitoring as they have open source platform.

2.7 Door Phone Based System

The earlier system, a specific system in which identification of a visitant is done for the most part by direct communication with the set of the housing estate concerned . A dialling up to the sets over the handsfree telephone is created by the framework at the entryway. Visitors enter inside through the gate by controlling the gate with the help of the telephone set. The latest system is based on video door phone surveillance which is used to identify the visitors, developed by Chau-Huang Wei et. al. The work utilized a novel powerline communication chip for build up a digital networked video door phone. Moreover, they exchanged audio and visual information and upgraded the passageway guarding capacities.

2.8 Bluetooth Based Systems

Bluetooth based system is a bit like sarvy house innovations that utilizes Bluetooth function available in smart devices . The framework using Bluetooth turns out to be more simple and productive for proper utilization. Such systems are generally based on Arduino platform. The hardware of such framework is the combo of android smart phone and Bluetooth module. Arduino microcontroller here is acting as a controller and solenoid can be acting as output of locking system.

2.9 Social Networking Sites Based Systems

A specific work the digitalization and safety perspectives were accomplished by utilizing the phone device and web camera. The model can empower a pin to close and open a door from allotted region using SMS from a (social networking site) like Facebook, Whatsapp etc. Digital Door Lock model based on Internet of Things Recently, a new digital door lock system get designed which detects the unknown physical contact of a visitant then immediately informs to the owner through the smart phone. At the moment, if wrong password gets detected more than the specified times, the system catches the picture of the unknown visitant and sends it to the owner through smart device. In this manner, increases the strength of the security function. With help of latest advanced technology, demonstration of an intelligent door system using Internet of Things is given by S. Nazeem Basha et. The system provides notification of intrusion by sending out email notification to the owner. It logs all the intrusion data into Google spread sheet of owner‟s Google drive account. ADXL345 accelerometer detects the change in motion of the door and raspberry pi reads the sensor intrusion data and to communicate to the Amazon Web Services Internet of Things (AWS IoT) console. Similar to the Ardiuno, Raspberry Pi module used mostly as It is an inexpensive computer that uses Linux-based operating system . It is also having open source platform for using devices like GPIO, HDMI, 10/100 Ethernet and USB port etc. It is also having slots for SD cards in which Linux raspberry package can be stored . It has large scope in research and development in the field of automatic door lock systems

2.10 OTP Based Systems

The proposed method in latest work does not need administrator‟s help to access the facility if the user knows OTP technique and has a registered mobile phone. Likewise the OTP is generated and sent to the proprietor‟s mobile phone whenever user requests to access facility. Then the OTP should enter through keypad on the door the door will open. In case if the mobile is not available or off then the option to open the door is to answer the security question ask by system.

2.11 Motion Detector Based System

The Motion Detector System working is based on the principle of amount of light falling on the photodiode. At the point when the laser light is falling constantly on the photodiode, its reading is 255 in decimals. But when it‟s hindered by deterrent, the voltage falls less than 50 in decimals. This flames the alarm and gives notification to the owner about the break in. And automatic lock can be activated.

2.12 VB Based System

Electronic eye represents the model for capturing the door images with the help of microcontroller to ensure the safety for offices and houses. In this system, the image gets captured when the door is opened and these images are displayed by using VB application on computing system.

2.13 Combined System

The locker security system is as shown in view of RFID, FINGERPRINT, PASSWORD and GSM technology containing door locking frameworks which can be without much of a stretch, initiated, authenticated and validated by the authorized person. It unlocks the locker door in real time manner.

II. LITERATURE REVIEW

Among the existing smart door lock systems, designed using different technologies, a few selected systems are discussed below, along with their features. As soon as a person is detected, the door would open, and they would be welcomed.

A. Smart IoT-based Facial Recognition Door Lock System

A smart IoT-based facial recognition system is a proactive approach that can take immediate action upon a security threat. The system recognizes the face of that person nearby the door and compares it with the faces uploaded to the database. A message and email with an intruder image will be sent to the owner in the event that an unknown person enters the building. This system uses Raspberry Pi, a Pi camera that is installed near the door to recognize an intruder's face, Direct Current (DC) motors connected through relays to open the door, Light-Emitting Diodes (LED) to indicate whether the door is open, and a GSM module is used to send texts to the registered mobile number.

B. Microcontroller-based Password Enabled Door Lock System

Microcontroller-based Password Enabled Door Lock System is an electronic security system that can detect an intruder and report it to the security personnel. The construction of an electronic digital lock using a microcontroller based on security information using a four-digit pass key. This operation involves opening the door, closing the door, changing the password, and alerting when entering the wrong password. The research objectives are achieved by using a micro-controller that interfaces the ATMEGA328P microprocessor with all the other components in the circuit. In the end, the circuit has activated by the relay and triggers the alarm. The password-protected lock system is designed previously using a microcontroller known as an 8051, accompanied by a 4*3 keypad for entering the password. A comparison is made between the entered password and the predefined password. If the password is correct, the door will be unlocked by rotating the door motor and the status of the door will be displayed on Liquid Crystal Display (LCD). On the other hand, when the password is incorrect, the door remains locked and a message appears on the LCD that reads "Password incorrect". The information will be stored in the database. However, when the correct password is received, the DC motor performs the action of unlocking the door as per the instructions of the controller. The door lock system is secured with the user's password. A door lock can only be opened if the correct password is entered. However, the option to change the password appears to be more secure since only authorized persons have access to it.

C. Knock-pattern using Arduino and GSM Communication

This technique uses a 'Secret Knocking Pattern,' which is only known by the owner of the safe, luggage, or other object or item on which the device is installed. It is necessary to apply the knocking pattern only at a specific spot known only by the owner in order to open the lock. Changing the secret pattern is only possible after unlocking the secret knock. Duplication cannot be done using this method because there is no key to copy.

D. Fingerprint Door Locking System

Fingerprints are widely considered as a unique identification of a person and the fastest and easiest method of biometric identification. Due to the fact that they are so unique and don't change for one in a lifetime, they are so secure and reliable to use. As long as the minutiae

matching technique is used appropriately, fingerprint recognition can be cheap, reliable, and accurate. A minutiae matching approach is used in this thesis work for fingerprint matching. The main difference between this algorithm and other conventional minutiae matching algorithms is the fact that it takes account of region and line structures between minutiae pairs. More structural information about the fingerprint should be accounted for to increase the certainty of matching minutiae. Most of the region analysis is pre-processed, so the algorithm does not become slower as a result.

E. RFID-Based Digital Door Locking System

As part of the RFID-Based Digital Door Locking System process, an image of the use is also captured. This image is scanned and compared against the database for matching. Depending on the card Unified Information Devices (UID) and capture image match, access is granted or denied, alerting the system for security purposes. This system is a significant entrance monitoring controller and exit monitoring controller, which can be installed at entrances and exits. This system can be used in hostels for security purposes. With a controller process and real time images and controller processes, this technology can improve response time. Figure 2. RFID-Based Digital Door Lock System

F. The Five-Button Door Lock System

These locks are called simplex locks. Combination numbers in simplex locks are related to Stirling numbers of the second kind and Mahler's algorithm for writing polynomials. Has the result that the number of combinations using all the buttons equals the number of combinations using fewer than all the buttons. It is common for schools, hospitals, and office buildings to have programmable door locks like the one in the figure that provides selective security and entry to a variety of rooms and spaces. Figure 3. The Five-Button Door Lock System

G. Colour Image Edge Detection

In this method, the amount of information required to complete facial recognition on a user is reduced by reducing the amount of data that needs to be stored every time. Using this technique, it is possible to create a CV on both greyscales or coloured images differently to provide sharp edges to the person, thus using less data traffic to transfer information between the accessor and the primary user, who will receive all notifications and images related to each

activity. The process of entering details of a new user, while the primary user is located at a remote location, is faster, more accurate (because the image reconstruction and edging are performed by the primary user), and more feasible. Despite the fact that this system is more data friendly, the accuracy of edge defining may not be a proper condition

CHAPTER-3

DESIGNED SYSTEM

3.1 Introduction

A smart door lock is a device that allows you to lock and unlock your door using a mobile app on your smartphone. It is a convenient and secure way to manage access to your home or office.One such example of a smart door lock system is the Android-Based Smart Door Locking System**.** This system is designed to prevent unauthorized access, trespassing, and intrusion.

Another example is the Secure Smart Door Lock System based on Arduino and Smartphone App. This system allows you to lock and unlock the door using voice commands or facial recognition using an Android app .There are many other smart door lock systems available in the market. You can choose one that suits your needs and budget.

This smart Lock is the secure, simple, and easy to manage your home's lock. This lock needs no keys and the lock is attached inside the door and you can control it from outside the door using Bluetooth. As the lock is inside the door there is no way to break the door by a thief. An android application is required to open and close the lock and I will explain the details how you can develop an android app in the later part of the tutorial. A password is sent to the lock using Android app and if the password is matched to your preset-lock password then the lock will be open and sent a feedback to your phone like the lock is open.

3.2 Objectives

The objectives of a smart door lock system using a mobile app typically include**:**
Enable users to lock and unlock doors remotely using their mobile devices for added convenience.

- Security: Implement secure authentication methods to ensure that only authorized users can control the smart door lock.
- Remote Monitoring :Allow users to monitor the status of the door (locked or unlocked) from anywhere using the mobile app.
- User Access Management: Provide features for managing and granting access rights to specific individuals, such as family members, friends, or service providers.

- Integration with Smart Homes: Integrate the smart door lock with other smart home devices, allowing users to create automation scenarios or receive alerts based on door activity.
- Audit Trail: Maintain a log or audit trail of door activities, including who locked or unlocked the door and when, for security and accountability.
- Emergency Access: Include mechanisms for emergency access, ensuring that authorized personnel can enter in critical situations.
- Energy Efficiency: Implement power-saving features to optimize energy consumption, especially in battery-operated smart locks.
- Notification System: Send real-time notifications to users when the door is accessed, providing immediate awareness.
- Tamper Detection: Incorporate sensors or features to detect and alert users in case of any tampering or unauthorized attempts to manipulate the lock.
- Firmware Updates: Allow for remote firmware updates to enhance security and add new features to the smart lock system.
- User-Friendly Interface: Design an intuitive and user-friendly interface for the mobile app, ensuring easy navigation and accessibility.
- Compatibility: Ensure compatibility with various mobile devices and operating systems to cater to a broad user base.
- Privacy Protection: Implement measures to protect user privacy, particularly regarding personal data and access logs.

3.3 Block Diagram

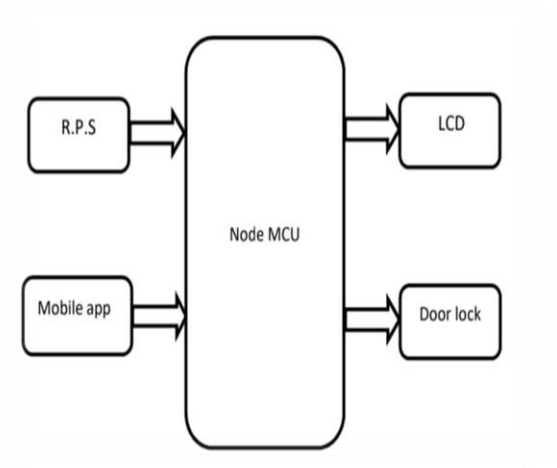

Fig 3.1:Block Diagram

3.4 Tools Required

3.4.1 Hardware Components

- Power Supply
- Node MCU
- Mobile app
- Lcd

3.4.2 Soft Ware Requirements

- Arduino IDE
- Proetus
- Code develops through Embedded C

3.4.3 Techniques Used

- IOT technology

From the block diagram we notice that we use hardware and software components. Each component will do their related work. Servomotor is used for rotating or shifting the in gate and exit gate. Esp332s is used for taking the inputs and outputs. We use software app for searching the slots and parking their vehicle in that app we done the payment also. Ultrasonic sensors are used for detecting the distance and give the information to the micro controller. Here we give the power supply.

The Internet of Things (IoT) is a revolutionary technological paradigm that involves linking everyday objects to the internet, enabling them to exchange data. These objects, equipped with sensors and actuators, form a network of interconnected devices known as the "Internet of Things." This connectivity allows devices to communicate with each other and centralized systems, fostering a wide array of applications across various domains.

Key components include the integration of devices with sensors, diverse connectivity protocols such as Wi-Fi and Bluetooth, data processing capabilities either locally or in the cloud, and the critical role of cloud computing for data storage and analysis. Ensuring the

security of IoT devices and the data they generate is a paramount concern, addressed through encryption, authentication, and secure communication protocols. IoT applications span from smart homes and healthcare to industrial automation, showcasing its capacity to enhance efficiency, provide real-time insights, and improve overall quality of life. Interoperability and standardization are essential for seamless collaboration among different IoT devices, regardless of their manufacturers. Despite its transformative potential, challenges such as security, privacy, and the establishment of industry standards continue to shape the evolving landscape of IoT.

3.5 WORKING

Creating a smart door lock system through a mobile device involves several steps. Below is a generalized procedure:

1. Select Smart Door Lock System:

Choose a smart door lock that is compatible with mobile connectivity. This could be a Bluetooth-enabled lock, a Wi-Fi-connected lock, or one that integrates with a specific smart home platform.

2. Purchase and Install the Smart Lock:

Purchase the selected smart door lock and follow the manufacturer's instructions for installation. This may involve replacing an existing lock or retrofitting the smart lock onto the current door.

3. Download and Install Mobile App:

Download the mobile app provided by the smart lock manufacturer. This app will serve as the interface for controlling and monitoring the lock.

4. Create User Accounts:

Register for an account within the mobile app. This account is essential for managing and controlling the smart lock. Depending on the lock system, you may also need to create user accounts for others who will have access.

5. Pair Mobile Device with Smart Lock:

Follow the pairing instructions provided by the lock manufacturer to connect your mobile device to the smart lock. This could involve Bluetooth pairing, Wi-Fi setup, or other connectivity methods.

6. Configure Lock Settings:

Use the mobile app to configure the settings for the smart lock. This may include setting up passcodes, defining access schedules, and configuring security preferences.

7. Test the Smart Lock:

Test the smart lock to ensure that it responds correctly to commands from the mobile app. Check if you can lock and unlock the door remotely.

8. Enable Additional Features (Optional):

Depending on the smart lock system, you may have additional features such as integration with voice assistants (e.g., Amazon Alexa, Google Assistant) or compatibility with other smart home devices. Enable these features if desired.

9. Share Access (Optional):

If the smart lock supports it, use the mobile app to share access with other users. This is useful for granting temporary access to guests or service providers.

10. Regular Maintenance and Updates:

Keep the mobile app and smart lock firmware up to date by installing any available updates. Regularly check and replace batteries if the lock is battery-powered.

ADVANTAGES

1. Convenient Access Control:

- Mobile-controlled smart door locks provide convenient access control, allowing users to lock or unlock doors remotely. This is particularly useful for granting access to guests or service providers without physical keys.

2. Keyless Entry:

- Eliminating the need for traditional keys, mobile-controlled smart locks offer keyless entry through the use of smartphones. This enhances security by reducing the risk of lost or stolen keys.

3. Remote Monitoring:

- Users can remotely monitor the status of their doors in real-time through the mobile app. This feature provides peace of mind by allowing homeowners to check if doors are securely locked when away from home.

4. Customized Access Permissions:

- Mobile apps associated with smart locks often allow users to set customized access permissions. This includes creating temporary access codes for guests or service personnel, enhancing flexibility and security.

5. Integration with Smart Home Systems:

- Many smart door locks integrate with broader smart home ecosystems. Users can link them to home automation systems, voice assistants, or security cameras for a more comprehensive and interconnected home setup.

6. Audit Trail and Activity Logs:

- Smart door locks often maintain an audit trail or activity log. Users can review these logs within the mobile app to see who accessed the door and when, providing enhanced security and accountability.

7. Increased Security Features:

- Mobile-controlled smart locks frequently incorporate advanced security features such as biometric authentication, two-factor authentication, and encryption, making them more resilient against unauthorized access.

8. Lost Key Replacement:

- In traditional lock systems, losing keys could pose security risks and require the replacement of locks. With mobile-controlled smart locks, access credentials can be easily deactivated and reissued without changing physical hardware.

9. Integration with Geofencing:

- Some smart locks support geofencing, automatically unlocking or locking doors based on the user's proximity. This feature adds an extra layer of automation and convenience.

10. Emergency Access:

- In the event of an emergency, authorized users can remotely grant access to emergency responders or trusted individuals through the mobile app, facilitating a quick response.

CHAPTER-4

HARDWARE IMPLEMENTATION

4.1 Node MCU ESP8266

4.1.1 Description

Node MCU ESP8266 Description Node MCU is an open-source firmware for which open-source prototyping board designs are available. The name “Node MCU” combines “node” and “MCU” (micro-controller unit). The term “Node MCU” strictly speaking refers to the firmware rather than the associated development kits. Both the firmware and prototyping board designs are open source. Node MCU ESP8266 and Node MCU ESP32 are becoming very popular and are almost used in more than 50% IoT based projects today.

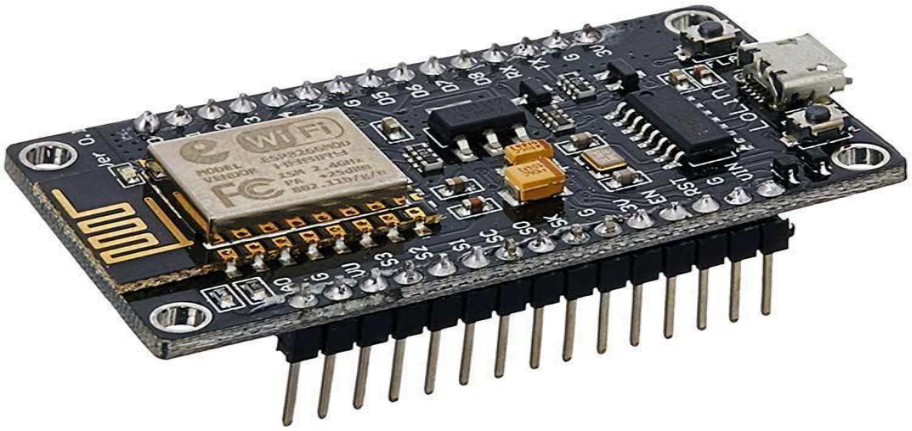

Fig 4.1: Node MCU

The firmware uses the Lua scripting language. The firmware is based on the eLua project and built on the Espressif Non-OS SDK for ESP8266. It uses many open-source projects, such as luacjson and SPIFFS. Due to resource constraints, users need to select the modules relevant for their project and build a firmware tailored to their needs. Support for the 32-bit ESP32 has also been implemented. The prototyping hardware typically used is a circuit board functioning as a dual in-line package (DIP) which integrates a USB controller with a smaller surface-mounted board containing the MCU and antenna. The choice of the DIP format allows for easy prototyping on breadboards.

The design was initially was based on the ESP-12 module of the ESP8266, which is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT applications.

About the Node MCU ESP8266 Pinout:

Node MCU ESP8266 Wi-Fi Module is an open-source Lua based firmware and development board specially targeted for IoT based applications. It includes firmware that runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module.

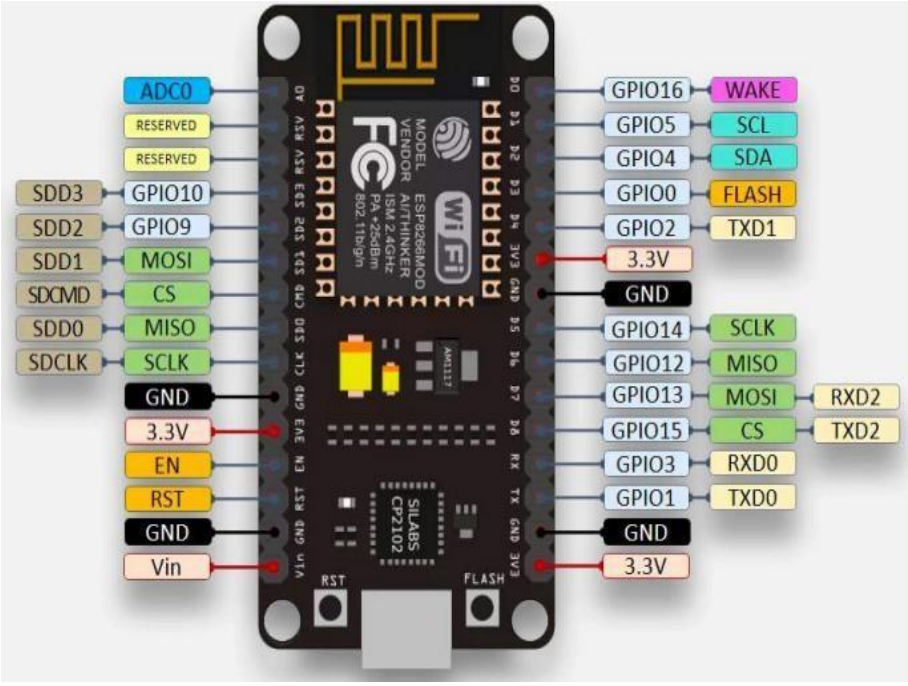

Fig 4.2 Pin Diagram of Node MCU

4.1.2 Node MCU ESP8266 Features:

Microcontroller: Tensilica 32-bit RISC CPU Xtensa LX106

Operating Voltage: 3.3V

Input Voltage: 7-12V

Digital I/O Pins (DIO): 16

Analog Input Pins (ADC): 1

UARTs: 1

SPIs: 1

I2Cs: 1

Flash Memory: 4 MB

SRAM: 64 KB

Clock Speed: 80 MHz

USB-TTL based on CP2102 is included onboard, Enabling Plug n Play PCB

Antenna Small Sized module to fit smartly inside your IoT projects

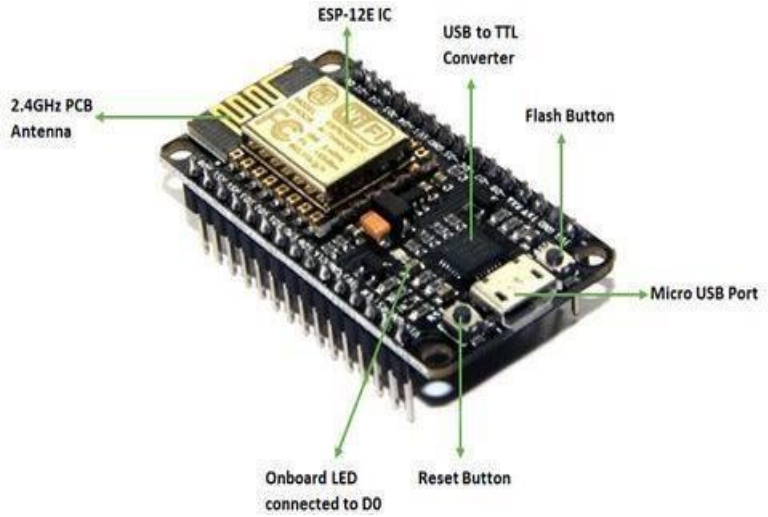

Fig 4.3: Layout of the Node MCU

4.1.3 Node MCU ESP8266 Pinout:

For practical purposes ESP8266 Node MCU V2 and V3 boards present identical pinouts. While working on the Node MCU based projects we are interested in the following pins.

Power pins (3.3 V).

Ground pins (GND).

Analog pins (A0).

Digital pins (D0 – D8, SD2, SD3, RX, and TX – GPIO XX)

Most ESP8266 Node MCU boards have one input voltage pin (Vin), three power pins (3.3v), four ground pins (GND), one analog pin (A0), and several digital pins (GPIO XX).

Pin Code Arduino alias

A0 A0 A0

D0 GPIO 16 16

D1 GPIO 5 5

D2 GPIO 4 4

D3 GPIO 0 0

D4 GPIO 2 2

D5 GPIO 14 14

D6 GPIO 12 12

D7 GPIO 13 13

D8 GPIO 15 15SD2 GPIO 9 9

SD3 GPIO 10 10

RX GPIO 3 3

TX GPIO 1 1

4.2 Relay

A relay is an electrical switch that is operated by an electromagnet. It is used to control high-voltage or high-current circuits using a low-voltage or low-current control signal. Here's a brief description and working principle of a relay:

4.2.1 Description

Electromagnetic Switch: A relay consists of an electromagnetic coil and a set of contacts (switches). These contacts can be either normally open (NO) or normally closed (NC)

.Coil and Contacts: When a voltage is applied to the coil, it generates a magnetic field, which causes the contacts to move and make or break an electrical connection.

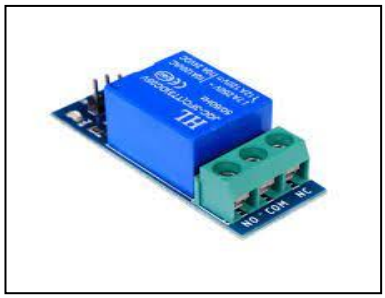

Fig 4.4: Relay

1. Types of Relays: There are various types of relays, including electro mechanical relays, solid-state relays (SSRs), and reed relays, each with specific applications and characteristics.

4.2.2 Working Principle

1.Normally Closed (NC): In its resting state, the NC contacts are closed, allowing current to flow through the circuit.

2.Normally Open (NO): In its resting state, the NO contacts are open, interrupting the current flow in the circuit.

3.Energizing the Coil: When a low-voltage control signal is applied to the relay coil, it creates a magnetic field, which either attracts or repels the contacts depending on the relay type.

4.Switching Operation: If it's an NC relay, applying the control signal opens the contacts, breaking the circuit. If it's an NO relay, applying the control signal closes the contacts, completing the circuit.

5. Isolation and Protection: Relays provide electrical isolation between the control circuit and the high-voltage/high-current circuit, which helps protect sensitive control electronics from potential damage.

Fig 4.5: Layout of Relay

4.2.3 Features

1.Voltage/Current Amplification: Relays allow small control signals, such as those from microcontrollers or sensors, to control larger loads like motors, heaters, or lights.

2.Electrical Isolation: They provide isolation between the control circuit and the load, enhancing safety and preventing interference.

3.Versatility: Relays are used in a wide range of applications, from home automation to industrial control systems.

4.Longevity: Electro mechanical relays can have a long operational life, making them suitable for many industrial applications.

4.Solid-State Relays (SSRs): These relays use semiconductor components (no moving parts) and are often used for high-speed switching, with the advantage of silent operation and faster response times.

4.3 Mems Sensor

Micro-electromechanical systems (MEMS) is a process technology used to create tiny integrated devices or systems that combine mechanical and electrical components. They are fabricated using integrated circuit (IC) batch processing techniques and can range in size from a few micro meters to milli meters.

4.3.1 Working Principle

MEMS is a chip-based technology, known as a Micro Electro-Mechanical System. Sensors are composed of a suspended mass between a pair of capacitive plates. When tilt is applied to the sensor, the suspended mass creates a difference in electric potential. The difference is measured as a change in capacitance.

A MEMS sensor provides the convenient features available with any other sensor line, but you don't need to concern yourself with space constraints. MEMS utilizes very compact micro machine components so small that each sensor can fit into the palm of your hand. They have an IP67 seal and since the operating temperature range is -40° to +85°C, they will withstand some intense conditions. While electrolytic sensors have much higher accuracy, some of them can be sensitive to temperature.

These sensors are great solutions to applications that do not demand the highest accuracy such as industrial automation, platform levelling, position control, and pitch and roll measurement. Since they are low cost, you can even save some money.

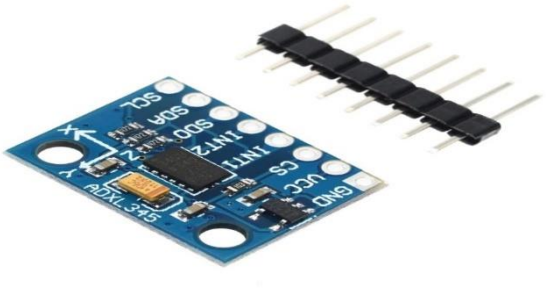

Fig 4.6: MEMS sensor (ADXL 345)

ADXL345 works on the principle of capacitive. ADXL345 is a capacitive accelerometer. It works on the principle that when the acceleration is applied to the sensor, the capacitance inside the sensor changes. This change in capacitance is then used to measure the acceleration of the object.

4.3.2Types

1. Accelerometers
2. MEMS microphone

Accelerometers

An accelerometer is a device that measures the vibration, or acceleration of motion, of a structure. The force caused by vibration or a change in motion (acceleration) causes the mass to "squeeze" the piezoelectric material which produces an electrical charge that is proportional to the force exerted upon it. Since the charge is proportional to the force, and the mass is constant, then the charge is also proportional to the acceleration. These sensors are used in a variety of ways – from space stations to handheld devices – and there's a good chance you already own a device with an accelerometer in it. For example, almost all smartphones today house an accelerometer. They help the phone know whether it undergoes acceleration in any direction, and it's the reason why your phone's display switches on when you flip it. In an industrial setting, accelerometers help engineers understand a machine's stability and enable them to monitor for any unwanted forces/vibrations.

Mems microphones

MEMS microphones extract audio pressure changes as electrical signals. However, MEMS microphones boast a reliable monolithic structure and far more compact form factor, which significantly lowers mechanical vibration, power consumption, and noise interference. They also offer a better signal-to-noise ratio (SNR) and support a wide operating temperature range. MEMS microphones, also known as silicon microphones, are now commonly used in smartphones, tablets, laptops, hearing aids, voice biometric, digital voice assistants, and more.

4.3.3: ADXL345 working principle

ADXL345 works on the principle of capacitive. ADXL345 is a capacitive accelerometer. It works on the principle that when the acceleration is applied to the sensor, the capacitance inside the sensor changes. This change in capacitance is then used to measure the acceleration of the object.

4.3.4: ADXL345 pinout:

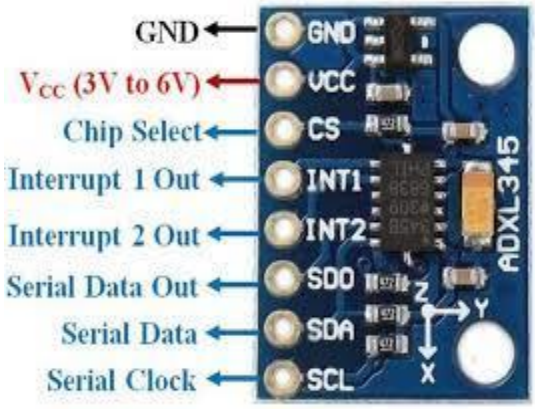

Fig 4.7: Pin Diagram of ADXL345

ADXL345 Pinout Configuration

- VCC: Power supply pin (3v to 6v)
- CS: Chip Select pin
- INT1: Interrupt 1 Out
- INT2: Interrupt 2 Out
- SDO: Serial Data Out
- SDA: Serial Data Input and Output
- SDC: Serial Communication Clock
- GND: Ground

4.4 Power Supply

4.4.1 Description

A regulated power supply is an embedded circuit; it converts unregulated AC (alternating current) into a constant DC. With the help of a rectifier, it converts AC supply into DC. Its function is to supply a stable voltage (or less often current), to a circuit or device that must be operated within certain power supply limits. The output from the regulated power supply may be alternating or unidirectional, but is nearly always DC (direct current). The type of stabilization used may be restricted to ensuring that the output remains within certain limits under various load conditions, or it may also include compensation for variations in its own supply source. The latter is much more common today.

4.4.2 Working Principle

The **Regulated power supply (RPS)** is one kind of electronic circuit, designed to provide the stable DC voltage of fixed value across load terminals irrespective of load variations. The main function of the regulated power supply is to convert an unregulated alternating current (AC) to a steady direct current (DC). The RPS is used to confirm that if the input changes, then the output will be stable. This power supply is also called a linear power supply, and this will allow an AC input as well as provides steady DC output.

4.4.3 Block Diagram

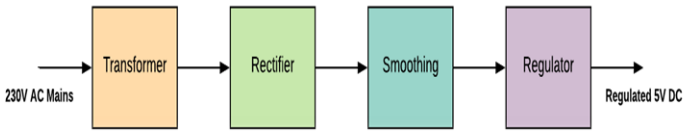

Fig 4.8: R.P.S Block Diagram

4.4.4 Features

1. Load Regulation: The load regulation, abbreviated LR (also called the **load effect**), is the change in regulated output voltage when the load current changes from minimum to maximum value

2. Minimum Load Resistance: Another characteristic of regulated power supply is load resistance, at which a power supply delivers its full-load rated current at rated voltage is referred to as a minimum load resistance, $R_{L\,(min)}$.

3. Source or Line Regulation: The input line voltage has a nominal value of 230 V but in practice, there are considerable variations in ac supply mains voltage. Since this ac supply mains voltage is the input to the ordinary power supply, the filtered output of the bridge rectifier is almost directly proportional to the ac mains voltage. Filtered output of the bridge rectifier is the input to the voltage regulating device.

4. Output Impedance: A regulated power supply is a very stiff dc voltage source. This means that the output resistance is very small (in milliohms). Even though the external load resistanceis

varies, almost no change is seen in the load voltage. An ideal voltage source has an output impedance of zero. Modern regulated power supplies approach ideal voltage sources.

5. Ripple Rejection: Voltage regulators stabilize the output voltage against variations in input voltage. Ripple is equivalent to a periodic variation in the input voltage. Thus, a voltage regulator attenuates the ripple that comes in with the unregulated input voltage. Since a voltage regulator uses negative feedback, the distortion is reduced by the same factor as the gain. Ripple rejection is a measure of a power supply's ability to reject ripple voltages and is usually expressed in decibels.

4.5 Liquid Crystal Display

A liquid-crystal display (LCD) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals combined with polarizers. Liquid crystals do not emit light directly but instead use a backlight or reflector to produce images in colour or monochrome.

4.5.1 Description

A **liquid-crystal display** (**LCD**) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals combined with polarizers. Liquid crystals do not emit light directly but instead use a backlight or reflector to produce images in colour or monochrome. LCDs are available to display arbitrary images (as in a general-purpose computer display) or fixed images with low information content, which can be displayed or hidden: preset words, digits, and seven-segment displays (as in a digital clock) are all examples of devices with these displays. They use the same basic technology, except that arbitrary images are made from a matrix of small pixels, while other displays have larger elements. LCDs can either be normally on (positive) or off (negative), depending on the polarizer arrangement.

Fig 4.9: Liquid Crystal Display

LCDs are used in a wide range of applications, including LCD televisions, computer monitors, instrument panels, aircraft cockpit displays, and indoor and outdoor signage. Small LCD screens are common in LCD projectors and portable devices such as digital cameras, watches, calculators, and mobile telephones, including smartphones. LCD screens have replaced heavy, bulky and less energy-efficient cathode-ray tube (CRT) displays in nearly all applications. The phosphorus used in CRTs make them vulnerable to image burn-in when a static image is displayed on a screen for a long time, e.g., the table frame for an airline flight schedule on an indoor sign. LCDs do not have this weakness, but are still susceptible to image persistence.

4.5.2 Working

An LCD panel is made of many layers. These consist of a polariser, polarised glass, LCD fluid, conductive connections etc. Polarisation is a process in which the vibration of light waves is restricted to a single plane, resulting in the formation of light waves known as polarised light. Since liquid crystals do not produce light of their own, they need an external light source to work. An LCD panel has sets of polarised glass consisting of liquid crystal materials in between them. When the external light passes through one of the polarised glasses and electric current is applied on the liquid crystal molecules, they align themselves in such a way that polarised light travels from the first layer to the second polarised glass, causing an image to appear on the screen.

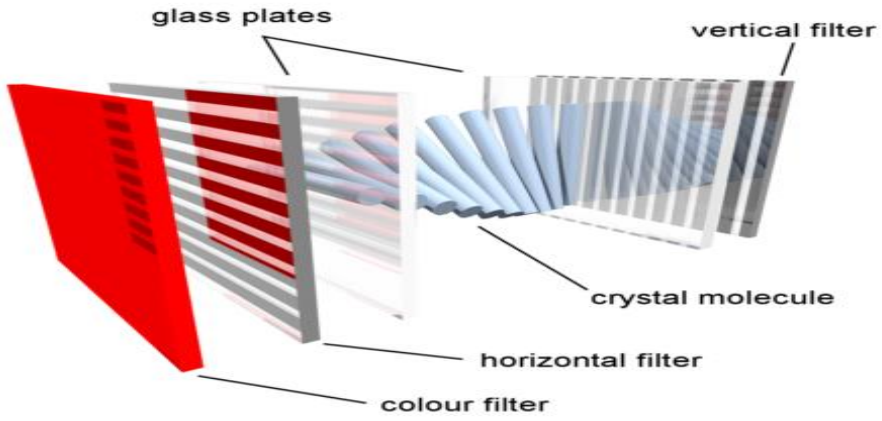

Fig 4.10: Internal Blocks of LCD

4.5.3 Types of LCD

Reflective: This type of LCD has a mirror layer. When a light ray within an LCD is reflected by the mirror layer, then visible patterns are produced on the LCD.

Transmissive: Here the LCD has a backlight, which passes through the LCD polarised glass to produce visible pattern. But because it uses backlight for working, the images displayed in such LCD types appear very dim when used under bright sunlight.

CHAPTER-5

SOFTWARE IMPLEMENTATION

5.1 Arduino IDE

5.1.1 Introduction to Arduino IDE

IDE stands for Integrated Development Environment - An official software introduced by Arduino.cc that is mainly used for writing, compiling and uploading the code in almost all Arduino modules/boards. Arduino IDE is open-source software and is easily available to download & install from Arduino Official Site.

In this post, I'll take you through the brief Introduction of the Software, how you can install it, and make it ready for your required Arduino module.
Let's dive in and get down to the nitty-gritty of this Software.

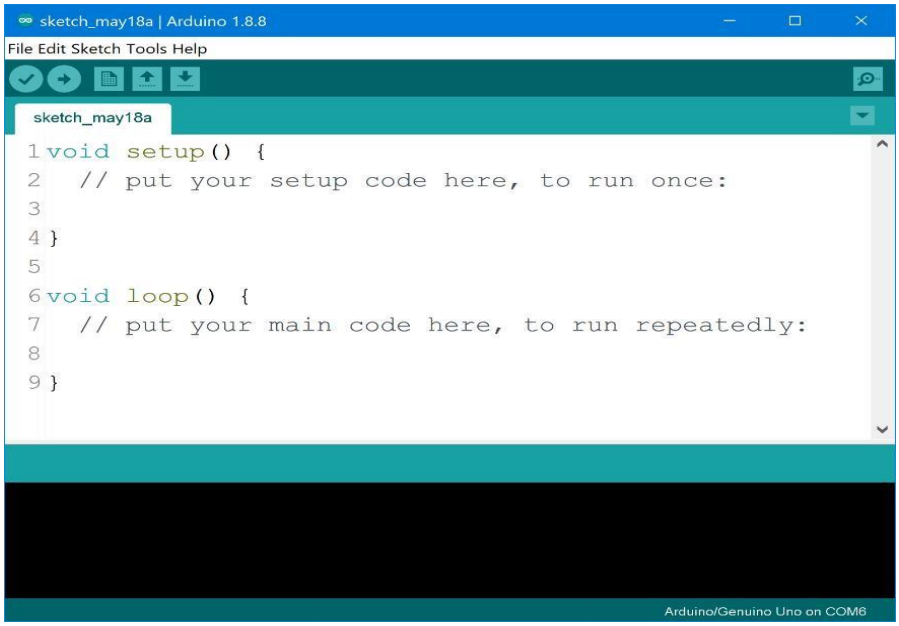

Fig 5.1: Arduino IDE Editor page

Arduino IDE is an open-source software, designed by Arduino.cc and mainly used for writing, compiling & uploading code to almost all Arduino Modules.

It is an official Arduino software, making code compilation too easy that even a common person with no prior technical knowledge can get their feet wet with the learning process.It is available for all operating systems i.e., MAC, Windows, Linux and runs on the Java Platform that comes with inbuilt functions and commands that play a vital role in debugging, editing and compiling the code.A range of Arduino modules available including Arduino Uno, Arduino Mega, Arduino Leonardo, Arduino Micro and many more.Each of them contains a microcontroller on the board that is actually programmed and accepts the information in the form of code.The main code, also known as a sketch, created on the IDE platform will ultimately generate a Hex File which is then transferred and uploaded in the controller on the board.The IDE environment mainly contains two basic parts: Editor and Compiler where former is used for writing the required code and later is used for compiling and uploading the code into the given Arduino Module.

This environment supports both C and C++ languages.

5.1.2 How to Download Arduino IDE

You can download the Software from Arduino main website. As I said earlier, the software is available for common operating systems like Linux, Windows, and MAX, so make sure you are downloading the correct software version that is easily compatible with your operating system.

8.1 or Windows 10, as the app version is not compatible with Windows 7 or older version of this operating system.

You can download the latest version of Arduino IDE for Windows (Non admin standalone version), by clicking below button:

Arduino IDE Download

The IDE environment is mainly distributed into three sections.

1.Menu Bar

2.Text Editor

3.Output Pane

As you download and open the IDE software, it will appear like an image below:

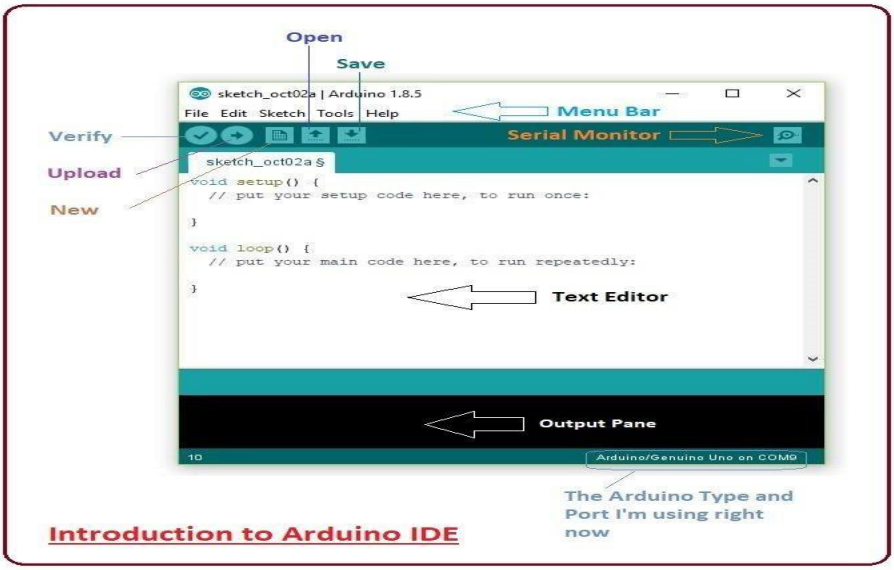

Fig 5.2: Introduction to Arduino IDE

The bar appearing on top is called Menu Bar that comes with five different options as

 File - You can open a new window for writing the code or open an existing one. The following table shows number of further subdivisions the file option is categorized into:

File	
New	This is used to open new text editor window to write your code
Open	Used for opening the existing written code
Open Recent	The option reserved for opening recently closed program
Sketchbook	It stores the list of codes you have written for your project
Examples	Default examples already stored in the IDE software
Close	Used for closing the main screen window of recent tab. If two tabs are open, it will ask you again as you aim to close the second tab
Save	It is used for saving the recent program
Save as	It will allow you to save the recent program in your desired folder
Page setup	Page setup is used for modifying the page with portrait and landscape options. Some default page options are already given from which you can select the page you intend to work on
Print	It is used for printing purpose and will send the command to the printer
Preferences	It is page with number of preferences you aim to setup for your text editor page
Quit	It will quit the whole software all at once

Fig 5.3: File subdivisions in Arduino IDE

 As you go to the preference section and check the compilation section, the Output Pane will show the code compilation as you click the upload button.

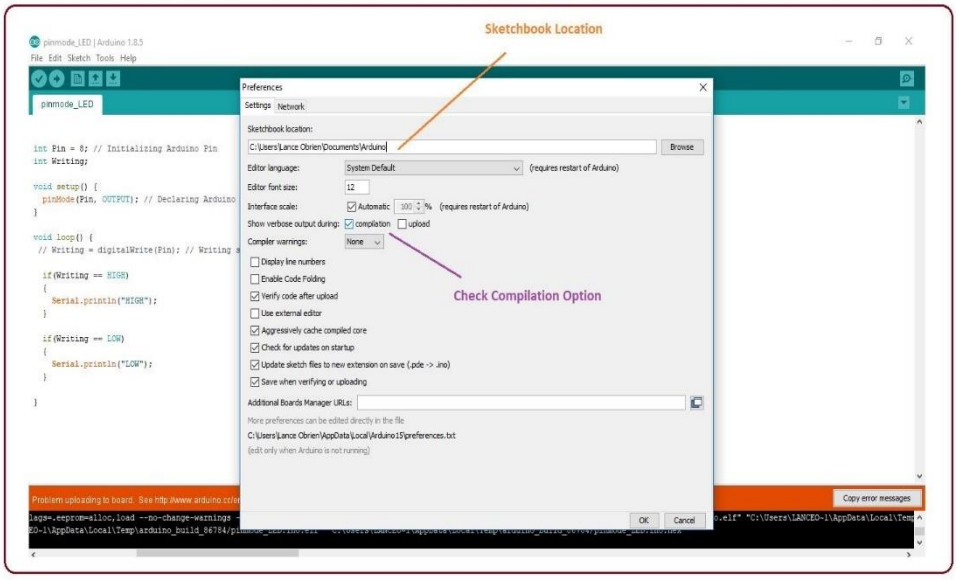

Fig 5.4: Selection of compilation

 And at the end of the compilation, it will show you the hex file it has generated for the recent sketch that will send to the Arduino Board for the specific task you aim to achieve.

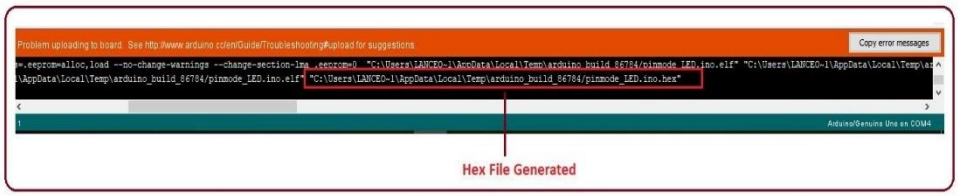

Fig 5.5: Hex file generation

- Sketch - For compiling and programming
- Tools - Mainly used for testing projects. The Programmer section in this panel is used for burning a boot loader to the new microcontroller.
- Help - In case you are feeling Edit - Used for copying and pasting the code with further modification for font
- sceptical about software, complete help is available from getting started to troubleshooting.
- The Six Buttons appearing under the Menu tab are connected with the running program as follows.

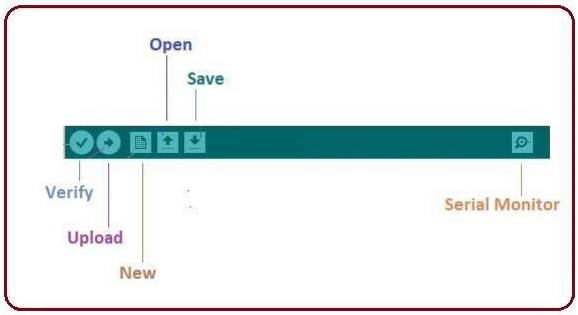

Fig 5.6: Serial monitor

- The check mark appearing in the circular button is used to verify the code. Click this once you have written your code.
- The arrow key will upload and transfer the required code to the Arduino board.
- The dotted paper is used for creating a new file.
- The upward arrow is reserved for opening an existing Arduino project.
- The downward arrow is used to save the current running code.
- The button appearing on the top right corner is a Serial Monitor - A separate pop-up window that acts as an independent terminal and plays a vital role in sending and receiving the Serial Data. You can also go to the Tools panel and select Serial Monitor, or pressing Ctrl+Shift+M all at once will open it instantly. The Serial Monitor will actually help to debug the written Sketches where you can get a hold of how your program is operating. Your Arduino Module should be connected to your computer by USB cable in order to activate the Serial Monitor.
- You need to select the baud rate of the Arduino Board you are using right now. For my Arduino Uno Baud Rate is 9600, Monitor, the output will show as the image below.

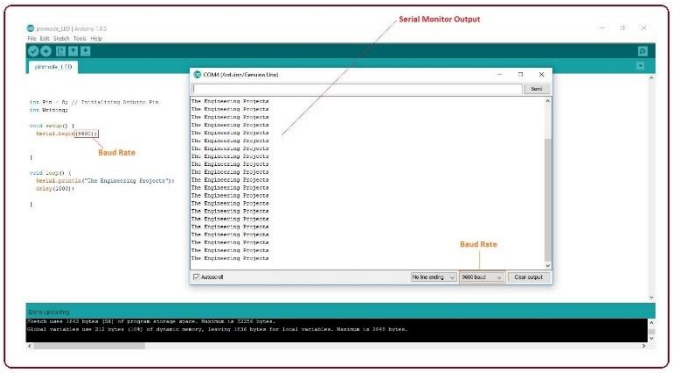

Fig 5.7: output of the serial monitor

 The main screen below the Menu bard is known as a simple text editor used for writing the required code.

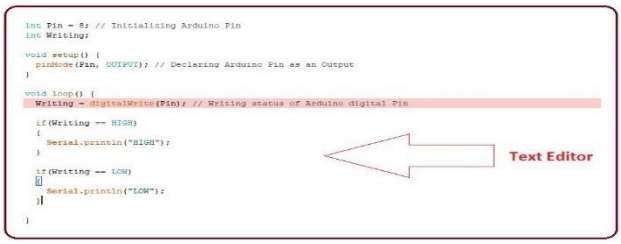

Fig 5.8: Text editor

 Output Pane that mainly highlights the compilation status of the running code: the memory used by the code, and errors that occurred in the program. You need to fix the bottom of the main screen is described as those errors before you intend to upload the hex file into your Arduino Module.

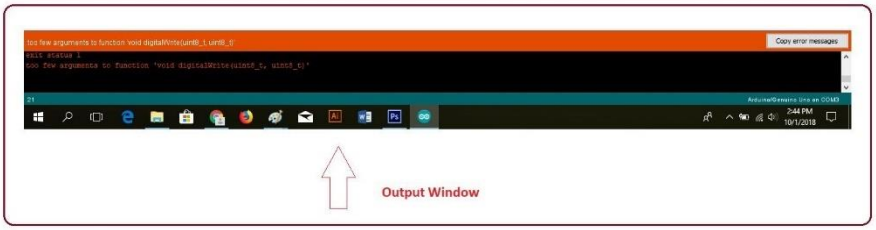

Fig 5.9: output window

 More or less, Arduino C language works similar to the regular C language used for any embedded system microcontroller, however, there are some dedicated libraries used for calling and executing specific functions on the board.

5.1.3 Libraries

- Libraries are very useful for adding extra functionality into the Arduino Module.
- There is a list of libraries you can check by clicking the Sketch button in the menu bar and going to Include Library.
- As you click the Include Library and Add the respective library it will be on the top of the sketch with a #include sign. Suppose, I Include the Liquid
  Crystal library, it will appear on the text editor as

#include <Liquid Crystal. h>

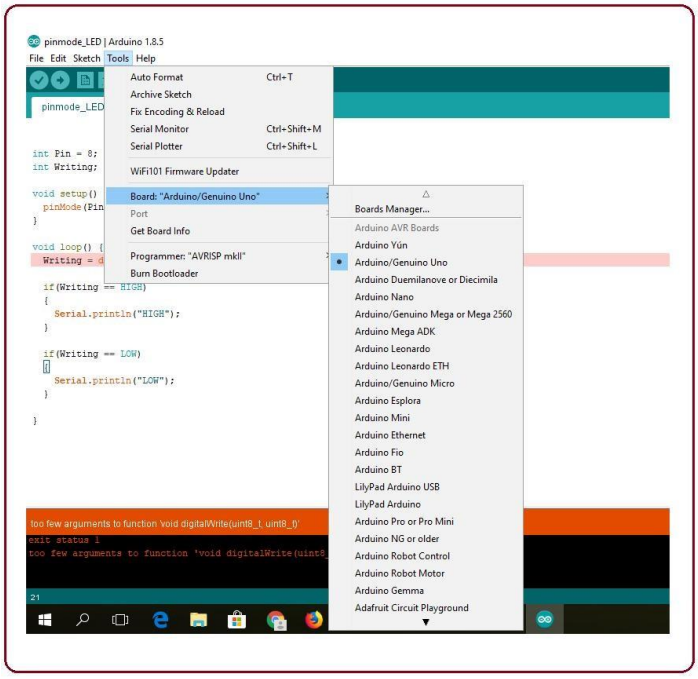

Fig 5.10: Selection of tools

- As you click the Include Library and Add the respective library it will be on the top of the sketch with a #include sign. Suppose, I Include the Liquid
  Crystal library, it will appear on the text editor as

  #include <Liquid Crystal.h>

- Most of the libraries are preinstalled and come with the Arduino software.
  However, you can also download them from external sources.

5.1.4 Making Pins Input or Output.

The digitalRead and digitalWrite commands are used for addressing and making the Arduino pins as an input and output respectively. These commands are text sensitive i.e., you need to write them down the exact way they are given like digitalWrite starting with small "d" and write with capital "W". Writing it down with DigitalWrite or digitalWrite won't be calling or addressing any function.

5.1.5 How to Select the Board

- In order to upload the sketch, you need to select the relevant board you are using and the ports for that operating system.
- As you click the Tools on the menu, it will open like the figure below:

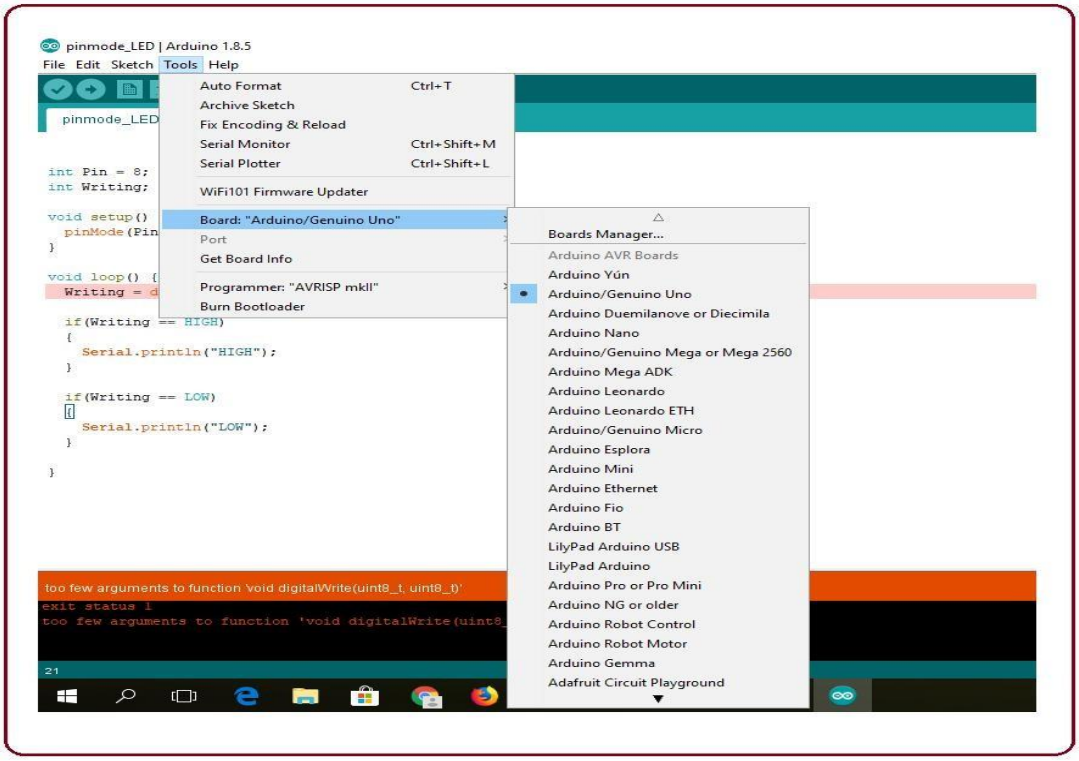

Fig 5.11: Selection of board manager

- Just go to the "Board" section and select the board you aim to work on. Similarly, COM1, COM2, COM4, COM5, COM7 or higher are reserved for the serial and USB board. You can look for the USB serial device in the port section of the Windows Device Manager.
- The following figure shows the COM4 that I have used for my project, indicating the Arduino Uno with the COM4 port at the right bottom corner of the screen.
- After correct selection of both Board and Serial Port, click the verify and then upload button appearing in the upper left corner of the six-button section or you can go to the Sketch section and press verify/compile and then upload.
- The sketch is written in the text editor and is then saved with the file extension into. It is important to note that the recent Arduino Modules will reset automatically as you compile and press the

upload button the IDE software, however, the older versions may require the physical reset on the board.

- Once you upload the code, TX and RX LEDs will blink on the board, indicating the desired program is running successfully.

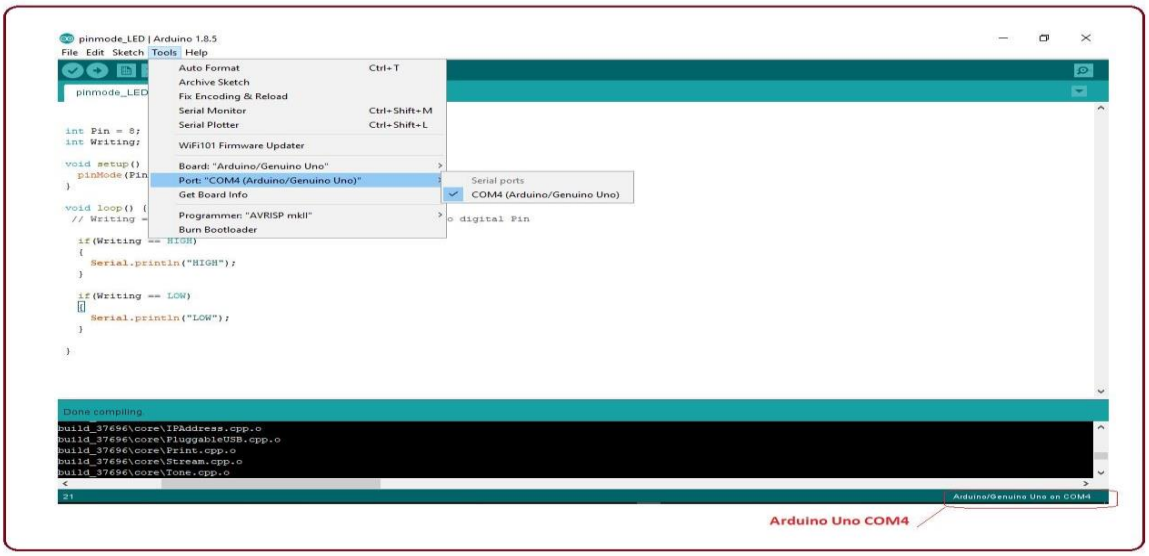

Fig 5.12: Selection of port

Note: The port selection criteria mentioned above are dedicated to Windows operating system only, you can check this Guide if you are using MAC or
Linux.

The amazing thing about this software is that no prior arrangement or bulk of the mess is required to install this software, you will be writing your first program within 2 minutes after the installation of the IDE environment.

5.1.6 Uploading

After writing your code, click on the upload button which is above the window and the code will be directly uploaded into the Node MCU with a cable wire connector.

CHAPTER – 6

RESULT

Smart door locks integrated with mobile technology have become a cornerstone in modern home automation. These locks typically connect to a mobile app, allowing users to remotely control access to their homes. Users can grant temporary or permanent access to individuals by sending virtual keys through the app, eliminating the need for physical keys. Advanced security features like two-factor authentication, fingerprint recognition, or facial recognition enhance the overall safety of these systems.

Moreover, many smart door locks offer compatibility with virtual assistants like Amazon Alexa or Google Assistant, enabling voice control for added convenience. Some models also support geofencing, automatically unlocking the door when the user approaches and locking it when they leave. This geo-aware functionality adds another layer of automation to the system.

The ability to receive real-time notifications on the mobile device, such as alerts for unauthorized access attempts or successful entries, ensures users stay informed about the security status of their homes. Additionally, integration with other smart home devices allows for creating custom automation scenarios, such as adjusting lights or thermostats upon unlocking the door.

Fig 6.1:Circuit Diagram

Fig 6.2: Door Open

Fig 6.3: Door Closed

CONCLUSION

In conclusion, the future of smart door locks through mobile devices holds tremendous potential for innovation and heightened security. With advancements in biometrics, AI integration, and the use of technologies like blockchain, these locks are poised to offer robust access control mechanisms. The advent of 5G connectivity and edge computing will enhance responsiveness and efficiency, while seamless integration into broader smart home ecosystems promises a more interconnected living experience. The incorporation of augmented reality for user-friendly interactions, environmental sensors for added functionalities, and ongoing emphasis on cybersecurity measures underscore a commitment to user safety and convenience. As the industry continues to evolve, the focus on improving energy efficiency, adhering to interoperability standards, and ensuring global compatibility will contribute to shaping a sophisticated and user-centric landscape for smart door locks through mobile devices.

FUTURE SCOPE

The future scope of smart door locks through mobile devices is promising, with anticipated advancements in technology. Biometric authentication methods are likely to become more sophisticated, incorporating advanced techniques like vein recognition and gait analysis. Artificial Intelligence (AI) integration could enhance security by adapting to user behaviors. The adoption of blockchain technology might provide increased transparency and security for access logs and permissions. With the rollout of 5G networks, faster and more reliable connectivity will enable quicker remote access and control. Edge computing may play a role in processing tasks locally on the smart lock, reducing latency. Expect deeper integration with smart home ecosystems, allowing for seamless automation and coordination. Augmented Reality (AR) features in mobile apps could simplify installation and troubleshooting. Environmental sensors may be integrated for additional functionalities, and cybersecurity measures will remain a priority to safeguard user privacy. The industry will likely focus on improving user experiences, refining voice control, and adhering to interoperability standards. Furthermore, advancements in energy-efficient components and global compatibility are expected to contribute to the evolution of smart door lock technology.

SOURCE CODE

```
 #include <ESP8266WiFi.h>
WiFi Client client;
WiFi Server server (80);
const char* ssid = "purple";
const char* password = "1234567890";
String command =""; // Command received from Android device
 // Set Motor Control Pins
int rightMotor2 = D3;
 void setup ()
{
  Serial. begin(115200);
 Pin Mode (rightMotor2, OUTPUT);
  digital Write (rightMotor2, HIGH);
   connect WiFi ();
  server. Begin ();
}
void loop ()
{
    client = server. Available ();
    if (! client) return;
    command = check Client ();
        if (command == "door%20open" ||command == "door%201%20open" || command ==
"VOICE1"          || command == "a frente") VOICE1();
    else if (command == "door%20close" ||command == "door%20one%20close"|| command
== "relay%20one%20of"|| command == "voltar") VOICE2();

   Serial. Println (command);
    Send Back Echo(command); // send command echo back to android device
    command = "";
}
```

```
/* command motor forward */
void VOICE1(void)

{
  Digital Write (rightMotor2, LOW);
}
void VOICE2(void)
{
  Digital Write (rightMotor2, HIGH);
}
/* command motor stop */
void stop Motor(void)
{

  Digital Write(rightMotor2,HIGH);
}

/* connecting WiFi */
void connect WiFi ()
{
  Serial .println ("Connecting to WIFI");
  WiFi.begin (ssid, password);
  while ((!(WiFi.status() == WL_CONNECTED)))
  {
    Delay (300);
    Serial.print("..");
  }
  Serial.println(" ");
  Serial.println("WiFi connected");
  Serial.println("NodeMCU L
ocal IP is : ");
```

```
  Serial.print((WiFi.localIP()));
}

/* check command received from Android Device */
String checkClient (void)
{
  while(!client.available()) delay(1);
  String request = client.readStringUntil('\r');
  request.remove(0, 5);
  request.remove (request.length()-9,9);
  return request;
}

/* send command echo back to android device */
void send Back Echo (String echo)
{
  Client .println ("HTTP/1.1 200 OK");
  client. Println("Content-Type: text/html");
  client. println("");
  client. println("<!DOCTYPE HTML>");
  client .println("<html>");
  client .println(echo);
  client .println("</html>");
  client .stop();
  delay (1);
}
```

REFERENCES

[1] Oke Alice O., Adigun Adebisi A., Falohun Adeleye S., and Alamu F. O. , "DEVELOPMENT OF A PROGRAMMABLE ELECTRONIC DIGITAL CODE LOCK SYSTEM" , International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 02– Issue 01, January 2013

[2] Mohammad Amanullah "MICROCONTROLLER BASED REPROGRAMMABLE DIGITAL DOOR LOCK SECURITY SYSTEM BY USING KEYPAD TECHNOLOGY", IOSR Journal of Electrical and Electronics Engineering (IOSR - JEEE), Volume 4, Issue 6 (Mar. - Apr. 2013).

[3] Ashish Jadhav, Mahesh Kumbhar, Mahesh Walunjkar, ", PASSWORD PROTECTED DOOR LOCKING SYSTEM" , International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 6, August 2013.

[4] P. K. Gaikwad, "DEVELOPMENT OF FPGA AND GSM BASED ADVANCED DIGITAL LOCKER SYSTEM", International Journal of Computer Science and Mobile Applications, Vol.1 Issue. 3, September2013. [5] Annie P. Oommen, Rahul A P, Pranav V, Ponni S, Renjith Nadeshan,

[6] Arpita Mishra, Siddharth Sharma, Sachin Dubey, S.K.Dubey, "PASSWORD BASED SECURITY LOCK SYSTEM", International Journal of Advanced Technology in Engineering and Science, Volume No.02, Issue No. 05, May 2014.

[7] E.Supraja, K.V.Goutham, N.Subramanyam, A.Dasthagiraiah, Dr.H.K.P.Prasad, "ENHANCED WIRELESS SECURITY SYSTEM WITH DIGITAL CODE LOCK USING RF &GSM TECHNOLOGY", International Journal of Computational Engineering Research, Vol 04, Issue 7, July – 2014.