ABSTRACT

This project presents the overall design of Home Automation System (HAS) with low cost and wireless system. It specifically focuses on the development of an IOT based home automation system that is able to control various components via internet or be automatically programmed to operate from ambient conditions. In this project, we design the development of a firmware for smart control which can successfully be automated minimizing human interaction to preserve the integrity within whole electrical devices in the home. We used Node MCU, a popular open source IOT platform, to execute the process of automation. Different components of the system will use different transmission mode that will be implemented to communicate the control of the devices by the user through Node MCU to the actual appliance. The main control system implements wireless technology to provide remote access from smart phone. We are using a cloud server-based communication that would add to the practicality of the project by enabling unrestricted access of the appliances to the user irrespective of the distance factor. We provided a data transmission network to create a stronger automation. The system intended to control electrical appliances and devices in house with relatively low-cost design, user-friendly interface and ease of installation. The status of the appliance would be available, along with the control on an android platform. This system is designed to assist and provide support in order to 1fulfil the needs of elderly and disabled in home. Also, the smart home concept in the system improves the standard living at home.

PREFACE

In an era where technology continues to evolve at an unprecedented pace, the integration of Artificial Intelligence (AI) into various facets of our lives has become more prevalent than ever. From the comfort of our homes to the complexities of industrial landscapes, AI smart automation stands at the forefront, reshaping the way we interact with and perceive the world around us.

This document delves into the multifaceted realm of AI smart automation, exploring its applications, benefits, challenges, and transformative potential across different sectors. Whether you are a technology enthusiast, industry professional, or curious observer, this guide aims to provide a comprehensive overview, shedding light on the intricacies and innovations driving the AI revolution.

As we embark on this journey through the realms of AI and automation, I invite you to delve deeper, question the norms, and envision the possibilities that lie ahead. Together, let us explore the boundless horizons of AI smart automation and embrace the opportunities it presents in shaping a smarter, more connected future.

Welcome to the world of AI smart automation—a world where technology transcends boundaries, fosters innovation, and paves the way for a brighter tomorrow.

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

Internet of Things (IOT) is a concept where each device is assigned to an IP address and through that IP address anyone makes that device identifiable on internet. The mechanical and digital machines are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Basically, it started as the "Internet of Computers." Research studies have forecast an explosive growth in the number of "things" or devices that will be connected to the Internet. The resulting network is called the "Internet of Things" (IoT). The recent developments in technology which permit the use of wireless controlling environments like, Bluetooth and Wi-Fi that have enabled different devices to have capabilities of connecting with each other. Using a WIFI shield to act as a Micro web server for the Arduino which eliminates the need for wired connections between the Arduino board and computer which reduces cost and enables it to work as a standalone device. The Wi-Fi shield needs connection to the internet from a wireless router or wireless hotspot and this would act as the gateway for the Arduino to communicate with the internet. With this in mind, an internet-based home automation system for remote control and observing the status of home appliances is designed.

Due to the advancement of wireless technology, there are several different types of connections are introduced such as GSM, WIFI, and BT. Each of the connection has their own unique specifications and applications. Among the four popular wireless connections that often implemented in HAS project, WIFI is being chosen with its suitable capability. The capabilities of WIFI are more than enough to be implemented in the design. Also, most of the current laptop/notebook or Smartphone come with built-in WIFI adapter. It will indirectly reduce the cost of this system.

1.2 BACKGROUND

The concept of "Home Automation" has been in existence for several years. "Smart Home", "Intelligent Home" are terms that followed and is been used to introduce the concept of networking appliance within the house. Home Automation Systems (HASs) includes centralized control and distance status monitoring of lighting, security system, and other appliances and systems within a house. HASs enables energy efficiency, improves the security systems, and certainly the comfort and ease of users. In the present emerging market, HASs is gaining popularity and has attracted the interests of many users. HASs comes with its own challenges. Mainly being, in the present day, end users especially elderly and disabled, even though hugely benefited, aren't seen to accept the system due to the complexity and cost factors.

1.3 PROJECT-OBJECTIVES

- **Design of an independent HAS**
  To formulate the design of an interconnected network of home appliance to be integrated into the HAS. The objective to account for every appliance and its control to be automated and integrated into the network further formulated into the HAS.
- **Wireless control of home appliances (Switch and Voice mode)**
  To develop the application that would include features of switch and/or voice modes to control the applications
- **Monitoring status of appliances**
  Being able to view the status of home appliances on the application, in order have a better HAS.
- **Secure connection channels between application and Node MCU**
  Use of secure protocols over Wi-Fi so that other devices are prevented to achieve control over the HAS. Secure connections are obtained by SSL over TCP, SSH.
- **Controlled by any device capable of Wi-Fi (Android, iOS, PC)**
  To achieve flexibility in control of the home appliances, and device capable of Wi-Fi connectivity will be able to obtain a secure control on the HAS.

- **Extensible platform for future enhancement**
  With a strong existing possibility of adding and integrating more features and appliances to the system, the designed system needs to be highly extensible in nature.

1.4 SCOPE

The aim is to design a prototype that establishes wireless remote control over a network of home appliances. The application is designed to run on android device providing features like, switch mode control, voice command control and a provision to view the status of the devices on the application itself. Considering its wide range of application, following are the scope of this prototype.

The system can be implemented in homes, small offices and malls as well, being in-charge of control of the electrical appliances.

For remote access of appliances in internet or intranet. The appliances in the above-mentioned environment can be controlled in intra-network or can be accessed via internet.

The development of technology friendly environment. The system incorporates the use of technology and making HAS. By the use of day-to-day gadgets, we can utilize them for a different perspective.

1.5 PROJECT-MANAGEMENT

Management of any project can be briefly disintegrated into several phases. Our project has been decomposed into the following phases:

1. ENVISIONED PHASE	• Information Gathering • Project Initiation
2. PLANNING PHASE	• Hardware & software estimation • Scheduling and distribution of task
3. MODELLING PHASE	• Analysis of project • Design and architecture of project
4. CONSTRUCTION PHASE	• Coding and hardware assembly • Testing and debugging
5. DEPLOYMENT PHASE	• Delivery of project • Feedback

Fig1: Model of phases in project management.

Experimentation

This phase involved discussions regarding necessary equipment regarding the project. The study of related already existing projects, gathering required theoretical learning. It also included figuring out the coding part, by developing simple algorithms and flowcharts to design the whole process

Design

This phase was, designing layout of the application, and the necessary features to be included. This involved the complete hardware assembly and installing the code to Node MCU. The power strip was designed to connect the home appliances that can be controlled via GPIO pins.

Development and testing

This phase had the development of the application. The android device was connected to the Node MCU via wireless network (WiFi) and the whole prototype was tested for identification and removal of bugs.

Real world testing

The prototype was ready to be tested into the real world and integrated with various real time electrical appliances.

1.6 OVERVIEW & BENEFITS

The benefits of an established wireless remote switching system of home appliances include:

- **No legal issues**
  Obtaining access to or traversing properties with hard lines is extremely difficult.
- **Reduced wiring issues**
  Considering the increase in price of copper, thus increases the possibility of the wire to be stolen. The use of a wireless remote system to control home appliances means no wire for thieves to steal.
- **Extended range**
  As the system establishes control over Wi-Fi, it was a generally considered descent range. That is 150 feet indoors. Outdoors it can be extended to 300 feet, but since the application is of a HAS, an indoor range is considered.
- **Security**
  As the connection of the control of the HAS is established over a secure network the system ensures security to the maximum extent.
- **Integrable and extensive nature**
  The prototype designed can be integrated to a larger scale. Also, it has an extensive nature being able to add or remove the appliances under control according to application.

1.7 ORGANIZATION OF THESIS

The thesis is organized into seven chapters including the introduction. Each chapter is unique on its own and is described with necessary theory to comprehend it.

Chapter 2 deals with Literature Review, this chapter reflects a comprehended form of the existing projects related to the topic. It credits the projects along with a brief paragraph of summery about the project. This reflects the various people worked on this area, how different and advanced each project is from one another.

Chapter 3 has the Theory that has been acquired to commence the project work. This discussed about IOT, the advantages, disadvantages the network topologies and communication protocols. This chapter also briefs about the main microcontroller unit of the prototype, Node MCU. Its pin configuration, various functional units of the development board and the installation process of the device. The chapter further giver a brief overview of the project, a block diagram of the system and the circuit diagram.

Chapter 4 describes the Hardware Modelling and setup of the project. The chapter points the main features of the prototype, gives a layout of the project, lists the components requires. It briefly describes the various setup processes involved with the project, including hardware interfacing and software installation and setup according to our requirement. It finally gives the hardware assembly involved.

Chapter 5 is the Logic and operation of the project. A flow chart presents the actions describe the working process of the prototype. It discussed the principle of operation of the system with the advantages and disadvantages of the microcontroller unit. It describes Blynk and IFTTT application and the wireless network established to attain remote control over the system. It describes the process of voice control mode and gives an overall cost estimation of the project.

Chapter 6 is the conclusion and Future scope. This chapter includes the result of the project work carried, the limitations it possesses, the further enhancements and modification that can be integrated into the prototype and finally concludes the project work carried so far.

Chapter 7 lists the References that have been used for the commencement of the project work.

Appendix A & B individual hardware description of the prototype and associated data sheets.

CHAPTER 2
LIERATURE SURVEY

2.LIERATURE SURVEY

2.1“Smart Energy Efficient Home Automation System using IOT”, by Satyendra K. Vishwakarma, Prashant Upadhyaya, Babita Kumari, Arun Kumar Mishra.

This paper presents a step-by-step procedure of a smart home automation controller. It uses IOT to convert home appliances to smart and intelligent devices, with the help of design control. An energy efficient system is designed that accesses the smart home remotely using IOT connectivity. The proposed system mainly requires, Node MCU as the microcontroller unit, IFTTT to interpret voice commands, Adafruit a library that supports MQTT acts as an MQTT broker and Arduino IDE to code the microcontroller. This multimodal system uses Google Assistant along with a web-based application to control the smart home. The smart home is implemented with main controller unit that is connected with the 24-hour available Wi-Fi network. To ensure, that the Wi-Fi connection do not turn off, the main controller is programmed to establish automatic connection with the available network and connected to the auto power backup.

2.2“IOT Based Smart Security and Home Automation”, by Shardha Somani, Parikshit Solunke, Shaunak Oke, Parth Medhi, Prof. P. P. Laturkar.

This paper focuses on a system that provides features of Home Automation relying on IOT to operate easily, in addition to that it includes a camera module and provides home security. The android application basically converts Smartphone into a remote for all home appliances. Security is achieved with motion sensors if movement is sensed at the entrance of the house; a notification is sent that contains a photo of house entrance in real time. This notification will be received by the owner of the house via internet such that app can trigger a notification. So, owner can raise an alarm in case of any intrusion or he/she can toggle the appliances like opening the door if the person is a guest. The system uses Raspberry Pi, a small sized computer which acts as server for the system. The smart home consists two modules. Home automation that consists; fan light and door controller, and security module that consists; smoke sensor motion sensor and camera module.

2.3“A Dynamic Distributed Energy Management Algorithm of Home Sensor Network for Home Automation System”, by Tui-Yi Yang, Chu-Sing Yang, Tien-Wen Sung.

This paper proposes an optimization of home power consumption based on PLC (Power Line Communication) for an easy to access home energy consumption. This also proposes a Zigbee and PLC based renewable energy gateway to monitor the energy generation of renewable energies. ACS and DDEM algorithm are proposed for the design of an intelligent distribution of power management system to make sure ongoing power supply of home networks. To provide efficient power management the power supply models of home sensor network are classified groups viz. main supply only, main supply and backup battery, rechargeable battery power and non-rechargeable battery power. Devices with particular features are assigned to these groups. It targets to establish real time processing scheme to address variable sensor network topologies.

2.4“Enhance Smart Home Automation System based on Internet of Things”, by Tushar Churasia and Prashant Kumar Jain.

This paper proposes a system that develops a model to reduce the computation overhead in existing smart home solutions that uses various encryption technologies like AES, ECHD, hybrid, etc. these solutions use intermediate gateway for connecting various sensor devices. The proposed model provides a method for automation with sensor-based learning. The system uses temperature sensor for development but other sensors can also be used as per requirement. These smart home devices with sensors can configure themselves autonomously and can operate without human intervention.

This work minimizes encryption decryption and focuses on authentication and automation of smart home devices with learning. The system bypasses local gateway mentioned in existing system to provide better security for smart home devices and sensor data and save computation overhead. The real time broker cloud is directly connected with smart home and manages all incoming and outgoing request between users and devices. The main purpose to use real time broker cloud is save time of cryptographic operations.

2.5"Visual Machine Intelligence for Home Automation", by Suraj, Ish Kool, Dharmendra Kumar, Shovan Barman.

The paper presents a vision-based machine intelligence system to sense on/off state of common home appliance. The proposed method of sensing the state of appliances results on a novel home automation system. The accessibility of the suite of devices in the home over a remote network is facilitated by the IP Addressing methods in the IOT. This project uses two boards viz. Raspberry Pi and Intel Galileo Gen 2. The communication between the User devices, Raspberry Pi and the Intel Galileo boards happens over a wireless network. The UDP protocol is deployed to facilitate the wireless communication of the nodes present in the home automation network. A Pi Cam and a USB Logitech camera attached to the rotating shaft of two different servo motor capture snapshots that are passed as inputs to the Machine Learning based models trained using dlib-C++ to detect the state of the operation of the appliances. The proposed method uses visual modality to automate the appliances, as privacy concerns may emerge while using the images from some specific places, as a counter to this issue, an SPDT switch is added to the Raspberry Pi which when turned off ensures that even if the images are taken from the webcams, they are just passed as inputs to the machine learning models and are not displayed on the website when the users access the website on the server address obtained from Raspberry Pi.

2.6"A Low Cost Home Automation System Using Wi-Fi based Wireless Sensor Network Incorporating internet of Things", by Vikram.N, Harish.K.S, Nihaal.M.S, Raksha Umesh, Shetty Aashik Ashok Kumar.

This paper illustrates a methodology to provide a low cost Home Automation System (HAS) using Wireless Fidelity (Wi-Fi). This crystallizes the concept of internetworking of smart devices. A Wi-Fi based Wireless Sensor Network (WSN) is designed for the purpose of monitoring and controlling environmental, safety and electrical parameters of a smart interconnected home. The different sections of the HAS are; temperature and humidity sensor, gas leakage warning system, fire alarm system, burglar alarm system, rain sensing, switching and regulation of load & voltage and current sensing. The primary requirement of HAS to monitor and control of devices is accomplished using a Smartphone application. The application is developed using Android Studio based on JAVA platform and User Interface of those are exemplified. The primary focus of the paper is to develop a solution cost effective flexible in control of devices and implementing a wide range of sensors to to capture various parameters.

2.7"Voice Controlled Home Automation System using Natural Language Processing and Internet of Things", by Mrs. Paul Jasmin Rani, Jason Bakthakumar, Praveen Kumaar.B, Praveen Kumaar.U, Santhosh Kumar. The paper focuses on the construction of a fully functional voice based home automation system that uses Internet of Things, Artificial Intelligence and Natural Language Processing (NLP) to provide a cost-effective, efficient way to work together with home appliances using various technologies such as GSM, NFC, etc. it implements a seamless integration of all the appliances to a central console, i.e. the mobile device. The prototype uses Arduino MK1000, known as Genuine MK1000. The NLP in this project gives the user the freedom to interact with the home appliances with his/her own voice and normal language rather than complicated computer commands. The appliances are connected to the mobile device through an Arduino Board that establishes the concept of Internet of Things. The Arduino Boards are interfaced with the appliances and programmed in such a way that they respond to mobile inputs

CHAPTER 3
THEORY

3.THEORY

3.1 IOT (INTERNET OF THINGS)

IOT as a term has evolved long way as a result of convergence of multiple technologies, machine learning, embedded systems and commodity sensors. IOT is a system of interconnected devices assigned a UIDS, enabling data transfer and control of devices over a network. It reduced the necessity of actual interaction in order to control a device. IOT is an advanced automation and analytics system which exploits networking, sensing, big data, and artificial intelligence technology to deliver complete systems for a product or service. These systems allow greater transparency, control, and performance when applied to any industry or system.

3.1.1 Features of IOT

3.1.1.1 Intelligence

IOT comes with the combination of algorithms and computation, software & hardware that makes it smart. Ambient intelligence in IOT enhances its capabilities which facilitate the things to respond in an intelligent way to a particular situation and supports them in carrying out specific tasks. In spite of all the popularity of smart technologies, intelligence in IOT is only concerned as a means of interaction between devices, while user and device interaction are achieved by standard input methods and graphical user interface

3.1.1.2 Connectivity

Connectivity empowers the Internet of Things by bringing together everyday objects. Connectivity of these objects is pivotal because simple object level interactions contribute towards collective intelligence in the IOT network. It enables network accessibility and compatibility in the things. With this connectivity, new market opportunities for the Internet of things can be created by the networking of smart things and applications

3.1.1.3 Dynamic Nature

The primary activity of Internet of Things is to collect data from its environment, this is achieved with the dynamic changes that take place around the devices. The state of these devices changes dynamically, example sleeping and waking up, connected and/or disconnected as well as the context of devices including temperature, location and speed. In addition to the state of the device, the number of devices also changes dynamically with a person, place and time

3.1.1.4 Enormous Scale

The number of devices that need to be managed and that communicate with each other will be much larger than the devices connected to the current Internet. The management of data generated from these devices and their interpretation for application purposes becomes more critical. Gartner (2015) confirms the enormous scale of IOT in the estimated report where it stated that 5.5 million new things will get connected every day and 6.4 billion connected things will be in use worldwide in 2016, which is up by 30 percent from 2015. The report also forecasts that the number of connected devices will reach 20.8 billion by 2020

3.1.1.5 Sensing

IOT wouldn't be possible without sensors that will detect or measure any changes in the environment to generate data that can report on their status or even interact with the environment. Sensing technologies provide the means to create capabilities that reflect a true awareness of the physical world and the people in it. The sensing information is simply the analog input from the physical world, but it can provide a rich understanding of our complex world

3.1.1.6 Heterogeneity

Heterogeneity in Internet of Things as one of the key characteristics. Devices in IOT are based on different hardware platforms and networks and can interact with other devices or service platforms through different networks. IOT architecture should support direct network connectivity between heterogeneous networks. The key design requirements for heterogeneous things and their environments in IOT are scalabilities, modularity, extensibility and interoperability.

3.1.1.7 Security

IOT devices are naturally vulnerable to security threats. As we gain efficiencies, novel experiences, and other benefits from the IOT, it would be a mistake to forget about security concerns associated with it. There is a high level of transparency and privacy issues with IOT. It is important to secure the endpoints, the networks, and the data that is transferred across all of it means creating a security paradigm.

3.1.2 Advantages of IOT

3.1.2.1 Communication

IOT encourages the communication between devices, also famously known as Machine-to-Machine (M2M) communication. Because of this, the physical devices are able to stay connected and hence the total transparency is available with lesser inefficiencies and greater quality.

3.1.2.2 Automation and Control

Due to physical objects getting connected and controlled digitally and centrally with wireless infrastructure, there is a large amount of automation and control in the workings. Without human intervention, the machines are able to communicate with each other leading to faster and timely output.

3.1.2.3 Information

It is obvious that having more information helps making better decisions. Whether it is mundane decisions as needing to know what to buy at the grocery store or if your company has enough widgets and supplies, knowledge is power and more knowledge is better.

3.1.2.4 Monitor

The second most obvious advantage of IOT is monitoring. Knowing the exact quantity of supplies or the air quality in your home, can further provide more information that could not have previously been collected easily. For instance, knowing that you are low on milk or printer ink could save you another trip to the store in the near future. Furthermore, monitoring the expiration of products can and will improve safety.

3.1.2.5 Time

As hinted in the previous examples, the amount of time saved because of IOT could be quite large. And in today's modern life, we all could use more time.

3.1.2.6 Money

The biggest advantage of IOT is saving money. If the price of the tagging and monitoring equipment is less than the amount of money saved, then the Internet of Things will be very widely adopted. IOT fundamentally proves to be very helpful to people in their daily routines by making the appliances communicate to each other in an effective manner thereby saving and conserving energy and cost.

Allowing the data to be communicated and shared between devices and then translating it into our required way, it makes our systems efficient.

3.1.2.7 Automation of daily tasks leads to better monitoring of devices

The IOT allows you to automate and control the tasks that are done on a daily basis, avoiding human intervention. Machine-to-machine communication helps to maintain transparency in the processes. It also leads to uniformity in the tasks. It can also maintain the quality of service. We can also take necessary action in case of emergencies.

3.1.2.8 Efficient and Saves Time

The machine-to-machine interaction provides better efficiency, hence; accurate results can be obtained fast. This results in saving valuable time. Instead of repeating the same tasks every day, it enables people to do other creative jobs.

3.1.2.9 Saves Money

Optimum utilization of energy and resources can be achieved by adopting this technology and keeping the devices under surveillance. We can be alerted in case of possible bottlenecks, breakdowns, and damages to the system. Hence, we can save money by using this technology.

3.1.2.10 Better Quality of Life

All the applications of this technology culminate in increased comfort, convenience, and better management, thereby improving the quality of life.

3.1.3 Disadvantages of IOT

3.1.3.1 Compatibility

Currently, there is no international standard of compatibility for the tagging and monitoring equipment. I believe this disadvantage is the most easy to overcome. The manufacturing companies of these equipment just need to agree to a standard, such as Bluetooth, USB, etc. This is nothing new or innovative needed.

3.1.3.2 Complexity

As with all complex systems, there are more opportunities of failure. With the Internet of Things, failures could sky rocket. For instance, let’s say that both you and your spouse each get a message saying that your milk has expired, and both of you stop at a store on your way home, and you both purchase milk. As a result, you and your spouse have purchased twice the amount that you both need. Or maybe a bug in the software ends up automatically ordering a new ink cartridge for your printer each and every hour for a few days, or at least after each power failure, when you only need a single replacement.

3.1.3.3 Privacy/Security

With all of this IOT data being transmitted, the risk of losing privacy increases. For instance, how well encrypted will the data be kept and transmitted with? Do you want your neighbours or employers to know what medications that you are taking or your financial situation?

3.1.3.4 Safety

Imagine if a notorious hacker changes your prescription. Or if a store automatically ships you an equivalent product that you are allergic to, or a flavour that you do not like, or a product that is already expired. As a result, safety is ultimately in the hands of the consumer to verify any and all automation.

As all the household appliances, industrial machinery, public sector services like water supply and transport, and many other devices all are connected to the Internet, a lot of information is available on it. This information is prone to attack by hackers. It would be very disastrous if private and confidential information is accessed by unauthorized intruders.

3.1.3.5 Lesser Employment of Menial Staff

The unskilled workers and helpers may end up losing their jobs in the effect of automation of daily activities. This can lead to unemployment issues in the society. This is a problem with the advent of any technology and can be overcome with education. With daily activities getting automated, naturally, there will be fewer requirements of human resources, primarily, workers and less educated staff. This may create Unemployment issue in the society.

3.1.3.6 Technology Takes Control of Life

Our lives will be increasingly controlled by technology, and will be dependent on it. The younger generation is already addicted to technology for every little thing. We have to decide how much of our daily lives are we willing to mechanize and be controlled by technology.

3.1.4 Application Grounds of IOT

3.1.4.1 Wearables

Wearable technologies is a hallmark of IOT applications and is one of the earliest industries to have deployed IOT at its services. Fit Bits, heart rate monitors, smartwatches, glucose monitoring devices reflect the successful applications of IOT.

3.1.4.2 Smart homes

This area of application concerned to this particular project, so a detailed application is discussed further. Jarvis, an AI home automation employed by Mark Zuckerberg, is a remarkable example in this field of application.

3.1.4.3 Health care

IOT applications have turned reactive medical based system into proactive wellness-based system. IOT focuses on creating systems rather than equipment. IOT creates a future of medicine and healthcare which exploits a highly integrated network of sophisticated medical devices. The integration of all elements provides more accuracy, more attention to detail, faster reactions to events, and constant improvement while reducing the typical overhead of medical research and organizations

Figure 2. Working of IOT enables care devices.

3.1.4.4 Agriculture

A greenhouse farming technique enhances the yield of crops by controlling environmental parameters. However, manual handling results in production loss, energy loss, and labour cost, making the process less effective. A greenhouse with embedded devices not only makes it easier to be monitored but also, enables us to control the climate inside it. Sensors measure different parameters according to the plant requirement and send it to the cloud. It, then, processes the data and applies a control action

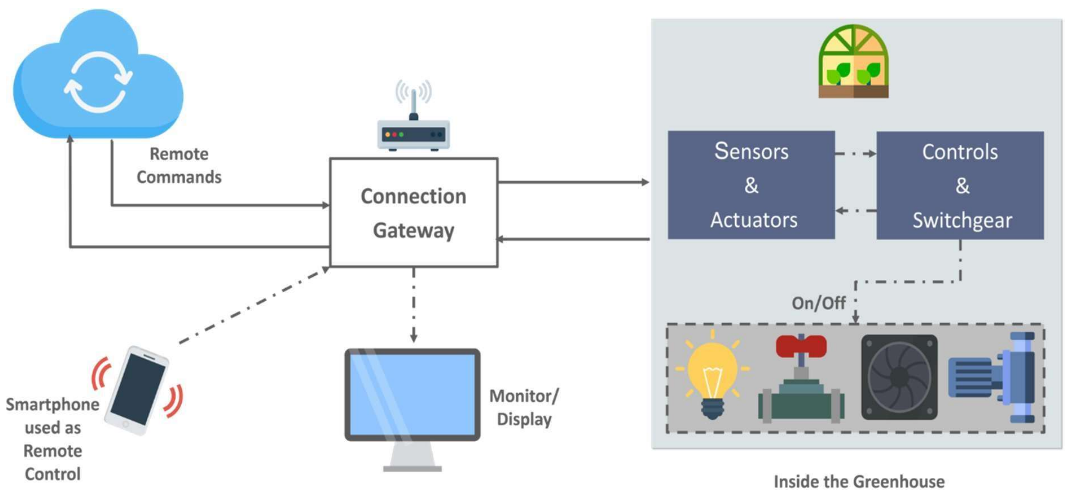


Figure 3. IOT controlled greenhouse environment.

3.1.4.5 Industrial Automation

For a higher return of investment this field requires both fast developments and quality of products. This vitality thus coined the term IIOT. This whole schematic is re-engineered by IOT applications. Following are the domains of IOT applications in industrial automation Factory Digitalization Product flow Monitoring Inventory Management Safety and Security Quality Control Packaging optimization Logistics and Supply Chain Optimization

3.1.4.6 Government and Safety

IOT applied to government and safety allows improved law enforcement, defense, city planning, and economic management. The technology fills in the current gaps, corrects many current flaws, and expands the reach of these efforts. For example, IOT can help city planners have a clearer view of the impact of their design, and governments have a better idea of the local economy.

3.1.5 IOT Technologies and Protocols

Several communication protocols and technologies cater to and meet the specific functional requirements of IOT system.

3.1.5.1 Bluetooth

Bluetooth is a short range IOT communication protocol/technology that is profound in many consumer product markets and computing. It is expected to be key for wearable products in particular, again connecting to the IOT albeit probably via a smartphone in many cases. The new Bluetooth Low-Energy (BLE) – or Bluetooth Smart, as it is now branded – is a significant protocol for IOT applications.

Importantly, while it offers a similar range to Bluetooth it has been designed to offer significantly reduced power consumption.

3.1.5.2 Zigbee

ZigBee is similar to Bluetooth and is majorly used in industrial settings. It has some significant advantages in complex systems offering low-power operation, high security, robustness and high and is well positioned to take advantage of wireless control and sensor networks in IOT applications. The latest version of ZigBee is the recently launched 3.0, which is essentially the unification of the various ZigBee wireless standards into a single standard.

3.1.5.3 Z-Wave

Z-Wave is a low-power RF communications IOT technology that primarily design for home automation for products such as lamp controllers and sensors among many other devices. A Zwane uses a simpler protocol than some others, which can enable faster and simpler development, but the only maker of chips is Sigma Designs compared to multiple sources for other wireless technologies such as ZigBee and others.

3.1.5.4 Wi-Fi

Wi-Fi connectivity is one of the most popular IOT communication protocol, often an obvious choice for many developers, especially given the availability of Wi-Fi within the home environment within LANs. There is a wide existing infrastructure as well as offering fast data transfer and the ability to handle high quantities of data. Currently, the most common Wi-Fi standard used in homes and many businesses is 802.11n, which offers range of hundreds of megabit per second, which is fine for file transfers but may be too power-consuming for many IOT applications.

3.1.5.5 Cellular

Any IOT application that requires operation over longer distances can take advantage of GSM/3G/4G cellular communication capabilities. While cellular is clearly capable of sending high quantities of data, especially for 4G, the cost and also power consumption will be too high for many applications. But it can be ideal for sensor-based low-bandwidth-data projects that will send very low amounts of data over the Internet.

3.1.5.6 NFC

NFC (Near Field Communication) is an IOT technology. It enables simple and safe communications between electronic devices, and specifically for smartphones, allowing consumers to perform transactions in which one does not have to be physically present. It helps the user to access digital content and connect electronic devices. Essentially it extends the capability of contactless card technology and enables devices to share information at a distance that is less than 4cm.

3.1.5.7 Lora-WAN

Lora WAN is one of popular IOT Technology, targets wide-area network (WAN) applications. The Lora WAN design to provide low-power WANs with features specifically needed to support low-cost mobile secure communication in IOT, smart city, and industrial applications. Specifically meets requirements for low-power consumption and supports large networks with millions and millions of devices, data rates range from 0.3 kbps to 50 kbps.

3.1.6 IOT software

IOT software addresses its key areas of networking and action through platforms, embedded systems, partner systems, and middleware. These individual and master applications are responsible for data collection, device integration, real-time analytics, and application and process extension within the IOT network. They exploit integration with critical business systems (e.g., ordering systems, robotics, scheduling, and more) in the execution of related tasks.

3.1.6.1 Data Collection

This software manages sensing, measurements, light data filtering, light data security, and aggregation of data. It uses certain protocols to aid sensors in connecting with real-time, machine-to-machine networks. Then it collects data from multiple devices and distributes it in accordance with settings. It also works in reverse by distributing data over devices. The system eventually transmits all collected data to a central server.

3.1.6.2 Device

Integration Software supporting integration binds (dependent relationships) all system devices to create the body of the IOT system. It ensures the necessary cooperation and stable networking between devices. These applications are the defining software technology of the IOT network because without them, it is not an IOT system. They manage the various applications, protocols, and limitations of each device to allow communication.

3.1.6.3 Real-Time Analytics

These applications take data or input from various devices and convert it into feasible actions or clear patterns for human analysis. They analyse information based on various settings and designs in order to perform automation-related tasks or provide the data required by industry.

3.1.6.4 Application and Process Extension

These applications extend the reach of existing systems and software to allow a wider, more effective system. They integrate predefined devices for specific purposes such as allowing certain mobile devices or engineering instruments access. It supports improved productivity and more accurate data collection.

3.2 NODE MCU

Node-MCU (Node Microcontroller Unit) is a low-cost open source IOT platform. It initially included firmware which runs on the ESP8266 Wi-Fi SoC from Expressive Systems, and hardware which was based on the ESP-12 module. Later, support for the ESP32 32-bit MCU was added.

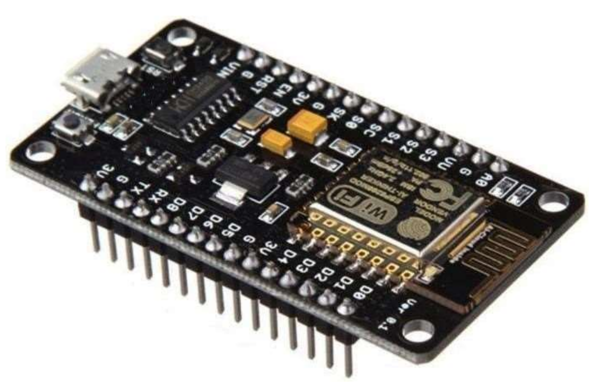


Figure 4. Node MCU Development Board.

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.

The firmware uses the Lua scripting language. The firmware is based on the eLua project, and built on the Expressive Non-OS SDK for ESP8266. It uses many open-source projects, such as lua- cjson 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.

3.2.1 Pin Configuration of Node MCU Development Board

This module provides an access to the GPIO subsystem. All the access is based on I/O index number of Node MCU kits, not the internal GPIO pins. For example, the D0 pin on the development kit is mapped to GPIO pin 16. Node MCU provides access to the GPIO pins and the following pin mapping table is a part of the API documentation.

PIN NAME ON NODE MCU DEVELOPMENT KIT	ESP8266 INTERNAL GPIO PIN NUMBER	PIN NAME ON NODE MCU DEVELOPMENT KIT	ESP8266 INTERNAL GPIO PIN NUMBER
0 [*]	GPIO1 6	**7**	GPIO13
1	GPIO5	**8**	GPIO15
2	GPIO4	**9**	GPIO3
3	GPIO0	**10**	GPIO1
4	GPIO2	**11**	GPIO9
5	GPIO1 4	**12**	GPIO10
6	GPIO1 2		

Table 1. Node MCU index ↔ GPIO mapping

[*] D0 (GPIO16) can only be used for GPIO read/write. It does not support open drain/interrupt/PWM/I²C or 1-Wire.

The ESP8266 Node MCU has total 30 pins that interface it to the outside world. The pins are grouped by their functionality as:

Power pins:

There are four power pins viz. one VIN pin & three 3.3V pins. The VIN pin can be used to directly supply the ESP8266 and its peripherals, if you have a regulated 5V voltage source. The 3.3V pins are the output of an on-board voltage regulator. These pins can be used to supply power to external components.

GND:

is a ground pin of ESP8266 Node MCU development board. 12 IC Pins: are used to hook up all sorts of I2C sensors and peripherals in your project. Both I2C Master and I2C Slave are supported. I2C interface functionality can be realized programmatically, and the clock frequency is 100 kHz at a maximum. It should be noted that I2C clock frequency should be higher than the slowest clock frequency of the slave device.

GPIO Pins:

ESP8266 Node MCU has 17 GPIO pins which can be assigned to various functions such as I2C, I2S, UART, PWM, IR Remote Control, LED Light and Button programmatically. Each digital enabled GPIO can be configured to internal pull-up or pull-down, or set to high impedance. When configured as an input, it can also be set to edge-trigger or level-trigger to generate CPU interrupts.

ADC Channel:

The Node MCU is embedded with a 10-bit precision SAR ADC. The two functions can be implemented using ADC viz. Testing power supply voltage of VDD3P3 pin and testing input voltage of TOUT pin. However, they cannot be implemented at the same time.

UART Pins:

ESP8266 Node MCU has 2 UART interfaces, i.e. UART0 and UART1, which provide asynchronous communication (RS232 and RS485), and can communicate at up to 4.5 Mbps. UART0 (TXD0, RXD0, RST0 & CTS0 pins) can be used for communication. It supports fluid control. However, UART1 (TXD1 pin) features only data transmit signal so, it is usually used for printing log.

SPI Pins:

ESP8266 features two SPIs (SPI and HSPI) in slave and master modes. These SPIs also support the following general-purpose SPI features:

- 4 timing modes of the SPI format transfer
- Up to 80 MHz and the divided clocks of 80 MHz
- Up to 64-Byte FIFO

SDIO Pins:

ESP8266 features Secure Digital Input/output Interface (SDIO) which is used to directly interface SD cards. 4-bit 25 MHz SDIO v1.1 and 4-bit 50 MHz SDIO v2.0 are supported.

PWM Pins:

The board has 4 channels of Pulse Width Modulation (PWM). The PWM output can be implemented programmatically and used for driving digital motors and LEDs. PWM frequency range is adjustable from 1000 μs to 10000 μs, i.e., between 100 Hz and 1 kHz.

Control Pins:

are used to control ESP8266. These pins include Chip Enable pin (EN), Reset pin (RST) and WAKE pin.

- EN pin – The ESP8266 chip is enabled when EN pin is pulled HIGH. When pulled LOW the chip works at minimum power.
- RST pin – RST pin is used to reset the ESP8266 chip.
- WAKE pin – Wake pin is used to wake the chip from deep-sleep.

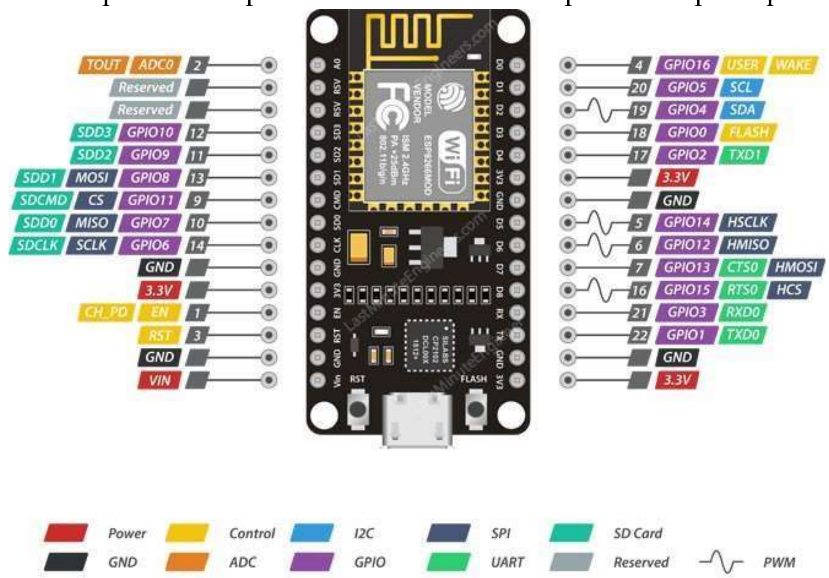


Figure 5. ESP8266 Node MCU pinout.

3.2.2 Parts of Node MCU Development Board

3.2.2.1 ESP 12-E Module

The development board equips the ESP-12E module containing ESP8266 chip having Tensilica Xtensa® 32-bit LX106 RISC microprocessor which operates at 80 to 160 MHz adjustable clock frequency and supports RTOS.

There's also 128 KB RAM and 4MB of Flash memory (for program and data storage) just enough to cope with the large strings that make up web pages, JSON/XML data, and everything we throw at IOT devices nowadays.

The ESP8266 Integrates 802.11b/g/n HT40 Wi-Fi transceiver, so it can not only connect to a Wi-Fi network and interact with the Internet, but it can also set up a network of its own, allowing other devices to connect directly to it. This makes the ESP8266 Node MCU even more versatile.

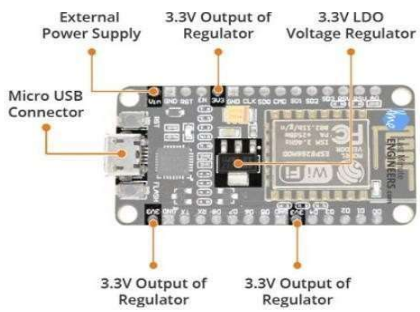
- Tensilica Xtensa® 32-bit LX106
- 80 to 160 MHz clock frequency
- 128 kb internal RAM
- 4 MB external flash
- 802.11b/g/n HT40 Wi-Fi transceiver

Figure 6. ESP 12E module in Node MCU Development board

3.2.2.2

Power Requirements As the operating voltage range of ESP8266 is 3V to 3.6V, the board comes with a LDO voltage regulator to keep the voltage steady at 3.3V. It can reliably supply up to 600mA, which should be more than enough when ESP8266 pulls as much as 80mA during RF transmissions. The output of the regulator is also broken out to one of the sides of the board and labelled as 3V3. This pin can be used to supply power to external components.

Power to the ESP8266 Node MCU is supplied via the on-board Micro B USB connector. Alternatively, if you have a regulated 5V voltage source, the VIN pin can be used to directly supply the ESP8266 and its peripherals



- Operating voltage 2.5V to 3.6V
- On-board 3.6V 600mA regulator
- 80 mA operating current
- 20 µA during sleep mode.

Figure 7. Power module on a Node MCU development board.

3.2.2.3 Peripheral I/O

The ESP8266 Node MCU has total 17 GPIO pins broken out to the pin headers on both sides of the development board. These pins can be assigned to all sorts of peripheral duties, including:

- ADC channel – A 10-bit ADC channel.
- UART interface – UART interface is used to load code serially.
- PWM outputs – PWM pins for dimming LEDs or controlling motors.
- SPI, I2C & I2S interface – SPI and I2C interface to hook up all sorts of sensors and peripherals.
- I2S interface – I2S interface if you want to add sound to your project.

As a result of the pin multiplexing feature (Multiple peripherals multiplexed on a single GPIO pin), a single GPIO pin can act as PWM/UART/SPI.

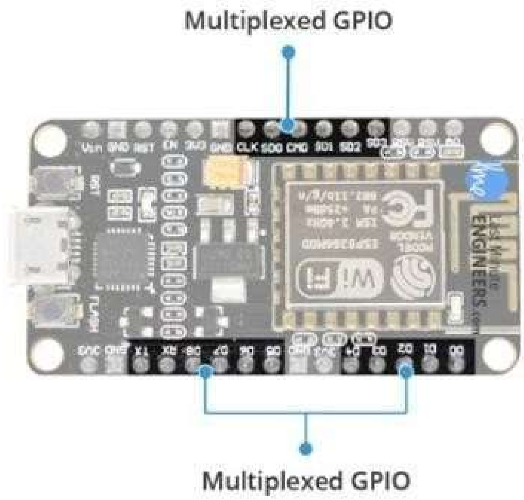
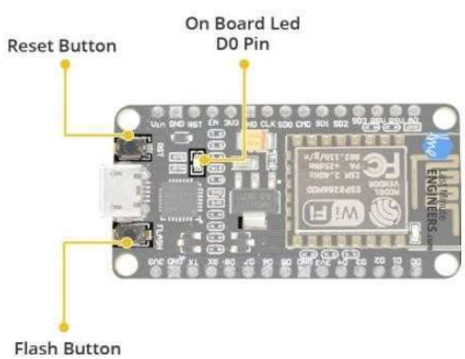


Figure 8. GPIO pins on Node MCU development board.

3.2.2.4 On Board Switches and LED Indicators

The ESP8266 Node MCU features two buttons. One marked as RST located on the top left corner is the Reset button, used of course to reset the ESP8266 chip. The other FLASH button on the bottom left corner is the download button used while upgrading firmware. The board also has a LED indicator which is user programmable and is connected to the D0 pin of the board.



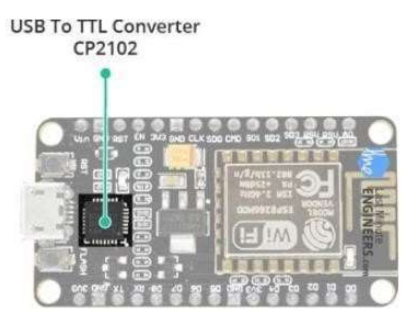
Switches and indicators

- RST: Reset the ESP8266 chip
- FLASH: Download new programs
- Blue LED: User programmable

Figure 9. ON board switches and LED indicators on Node MCU development board.

3.2.2.5 Serial Communication

The board includes CP2102 USB-to-UART Bridge Controller from Silicon Labs, which converts USB signal to serial and allows your computer to program and communicate with the ESP8266 chip.



- CP2120 USB-to-UART converter
- 4.5 Mbps communication speed
- Flow control support

Figure 10. CP2120 on Node MCU development board.

3.2.3 Installation of Node MCU

Mostly these days devices download and install drivers on their own, automatically. Windows doesn’t know how to talk to the USB driver on the Node MCU so it can’t figure out that the board is a Node MCU and proceed normally. Node MCU Amica is an ESP8266 Wi-Fi module-based development board. It has got Micro USB slot that can directly be connected to the computer or other USB host devices. Ti has got 15X2 header pins and a Micro USB slot, the headers can be mounted on a breadboard and Micro USB slot is to establish connection to USB host device. It has CP2120 USB to serial converter. In order to install CP2120 (USB to serial converter), user is needed to download the driver for the same. Once user downloads drivers as per its respective operating system, the system establishes connection to Node MCU. The user needs to node down the COM post allotted to newly connected USB device (Node MCU) from device manager of the system. This com port number will be required while using Node MCU Amica. As the CP2120 driver is been installed, the Node MCU can be programmed using Arduino IDE software by coding in embedded C. this requires ESP8266 board installation in Arduino IDE from board manager, and assigning communication port.

CHAPTER 4
PRPOSED SYSYTEM

PROPOSED SYSTEM

4.1 BLOCK DIAGRAM

4.1.1 Block diagram of the proposed system

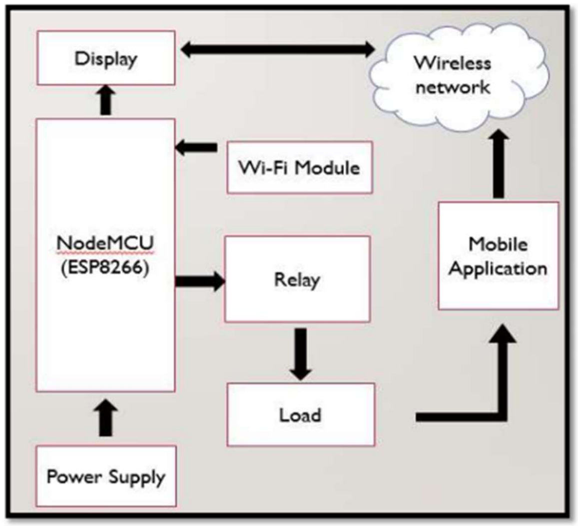


Figure 11. Block diagram of proposed system.

The block diagram gives the functionality of the overall project. The Node MCU unit is the microcontroller or the main controlling unit of the system. The user uses the mobile application in setting commands for functioning of the appliances. The mobile application interprets the command form in user in voice or switch mode and sends signal to the Node MCU unit, over a wireless network established by Wi-Fi communication. Hence the Wi-Fi module (actually inbuilt into Node MCU), helps the microcontroller establish Wi-Fi communication with a device and take commands from an application over wireless network. The Node MCU on further receiving the signal then turns on/off the appliance with the help of relay. The Node MCU, relay and the final appliances are physically connected. There is a power supply unit that powers the microcontroller, the relay as well as the final appliances. There is also a display unit that displays the status of the application.

4.1.2 Proposed system

The android OS provides the flexibility of using the open source. The inbuilt sensors can be accessed easily. The application used to control the system has the following features. Android Phone acts as a client and data are sent via sockets programming. The application takes command from user in two different modes.

- **Switch mode:**

  Switch mode uses the radio buttons that are used to control the home appliances. The radio button sends the status of the switch.

- **Voice mode:**

  Voice Mode is used to control the home appliances using voice command. Using the inbuilt microphone of Smartphone, the application creates an intent that fetches the speech data to the Google server which responds with a string data. The string data are further analyzed and then processed.

More detailed discussion about the modes of control and how they actually control the system is discussed if coming chapters.

4.2 OVERVIEW OF PROJECT

The following describes the process of creating an account in Webzee application and generating unique ID against a particular device. This ID acts as an identifier for the particular device on the Firebase server.

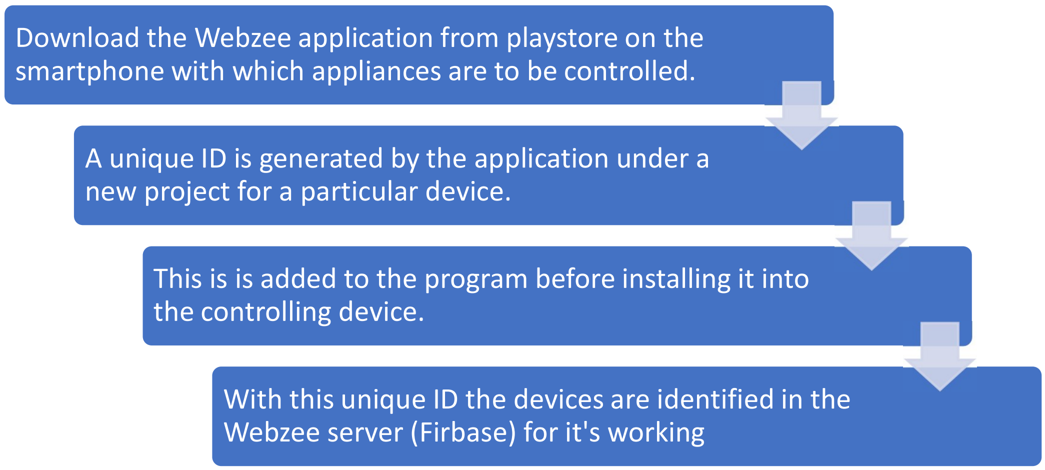


Figure 12. Creating an account and generating unique ID in Webweez Server

Once the unique Id is generated the next step would be to include this key into the coding written in embedded C to establish communication between Node MCU and Blynk Server. The following describes this process.

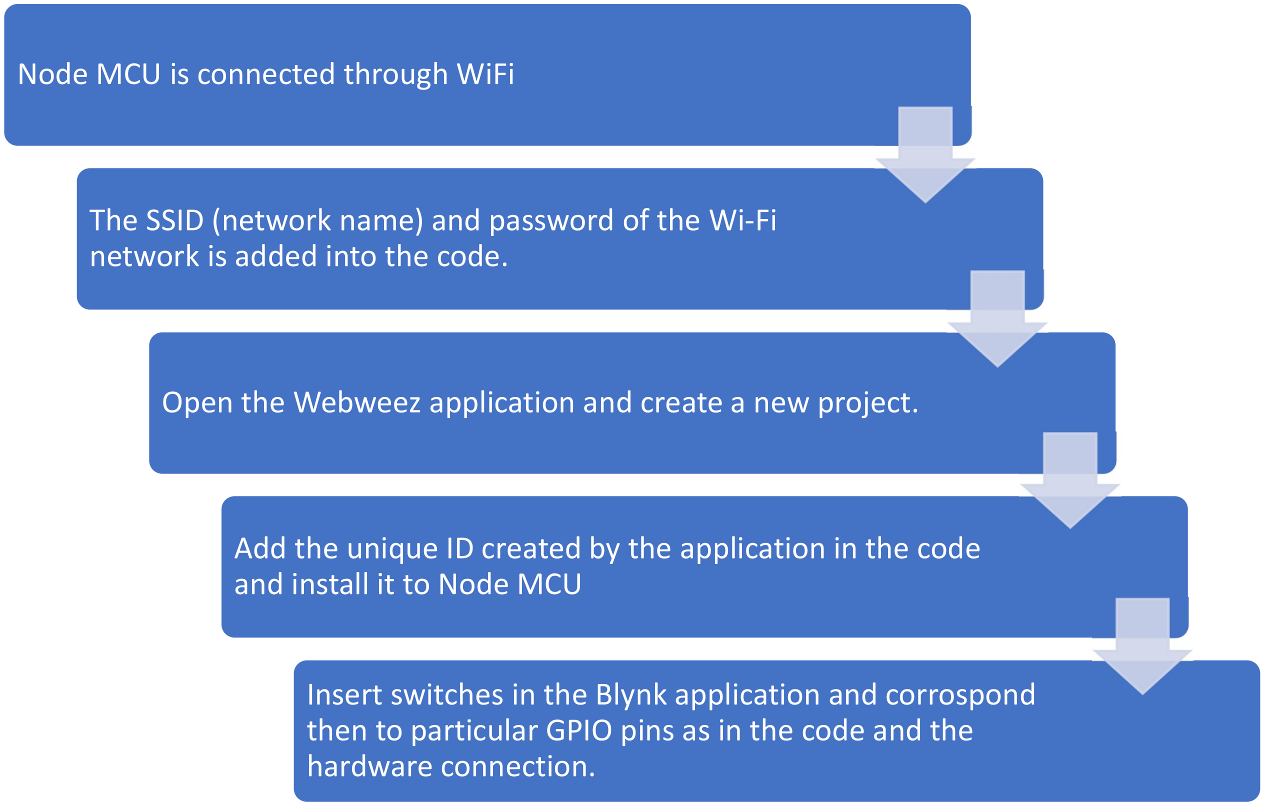


Figure 13. Setup to control Node MCU from Blynk application

4.3CIRCUIT DIAGRAM

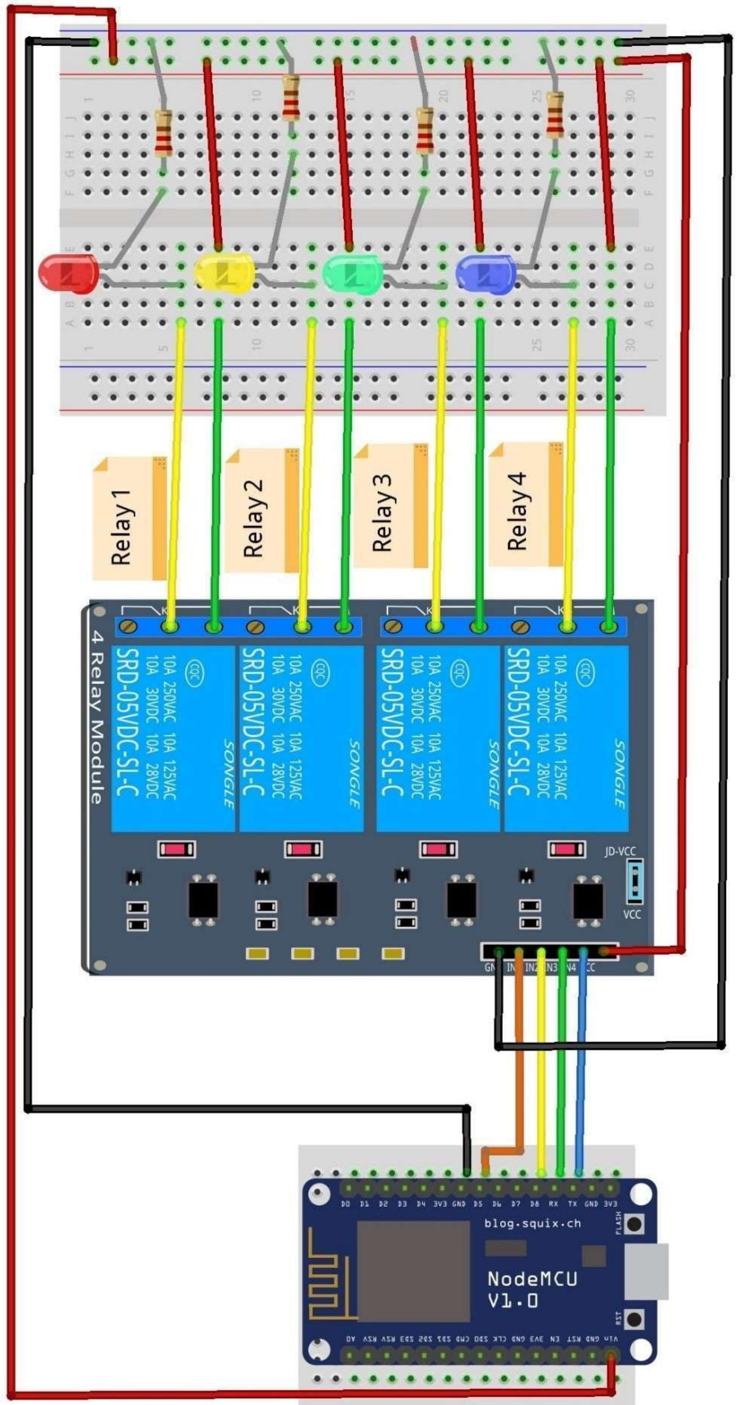


Figure 14. Connection diagram of Node MCU controlling 4 channel relay modules.

4.4 SYSTEM COMPONENTS

4.4.1 Android Apk for Home Control

- User Experience (UX) Design: Understand the importance of UX in ensuring user adoption and satisfaction. Consider principles like affordance, feedback, and consistency.
- Backend Integration: Explore how the app communicates with various devices, possibly using technology like html , firebase server and home grown web-app for real-time interactions.

4.4.2 AI-BASED FIRE MANGEMENT SYSTEM

AI-based fire management systems leverage artificial intelligence (AI) technologies to detect, monitor, and manage fire-related incidents more effectively. These systems combine various sensors, data analytics, and AI algorithms to provide real-time insights and automated responses to mitigate fire risks. Below is an overview of AI-based fire management systems:

1. Introduction

    Define the need for advanced fire management systems.

Discuss the limitations of traditional fire detection and management methods.

2. Components of AI-Based Fire Management Systems
    - Sensors: Deploy advanced sensors, such as infrared cameras, smoke detectors, and temperature sensors, to detect fire-related anomalies.
    - Data Analytics: Utilize data analytics techniques to process sensor data and identify potential fire risks or anomalies.
    - AI Algorithms: Implement machine learning and deep learning algorithms to analyze data patterns, predict fire incidents, and optimize response strategies.
3. Key Features and Capabilities Early Detection:
    - Enable early detection of fire incidents through real-time monitoring and analysis of sensor data.
    - Predictive Analytics: Utilize AI algorithms to predict potential fire risks based on historical data, environmental factors, and other relevant parameters.
    - Automated Response: Integrate with automated systems, such as sprinkler systems, alarms, and notification systems, to initiate timely responses and minimize damage.
    - Optimization: Continuously optimize system performance and response strategies based on real-time data and feedback.
4. Applications and Use Cases
    - Residential Buildings: Implement AI-based fire management systems in residential buildings to enhance safety and minimize property damage.
    - Commercial Buildings: Deploy advanced fire management solutions in commercial buildings, offices, and industrial facilities to ensure compliance with safety regulations and protect valuable assets.
    - Wildfire Management: Utilize AI technologies to monitor and manage wildfires more effectively, providing early warnings and enabling proactive measures to contain and control the spread of fires.
5. Challenges and Considerations
    - Data Privacy and Security: Address concerns related to data privacy and security, ensuring that sensitive information is protected and securely managed. Integration with
    - Existing Systems: Consider the integration of AI-based fire management systems with existing infrastructure, systems, and protocols.
    - Scalability and Adaptability: Ensure that the system is scalable and adaptable to different environments, requirements, and emerging technologies.
6. Future Trends and Opportunities
    - Discuss emerging trends, such as the integration of IoT devices, edge computing, and cloud-based solutions in AI-based fire management systems.
    - Highlight opportunities for research, innovation, and collaboration in advancing the field of AI-based fire management.

By leveraging AI technologies, fire management systems can enhance safety, improve response times, and minimize the impact of fire-related incidents, contributing to a safer and more secure environment.

4.5 MAIN FEATURES OF THE PROTOTYPE

The features of the developed prototype are:

- SThe prototype establishes a wireless remote switching system of home appliances.
- The prototype uses Wi-Fi to establish wireless control, which gives an indoor range to about150 feet.
- The command to switch on and off an appliance can be given from radio buttons on the application from one's smartphone.
- There is also a provision developed to use voice commands on smartphone to remotely switch home appliances
- Any device capable of Wi-Fi connectivity can be used to control the prototype.
- The control over home appliances is obtained over secure connections, by SSL over TCP, SSH.
- Simple design easy to integrate into a verity of appliances and extend on further range.
- Displays the status of each appliances on the application in smartphone
- Cost effective.

4.6 PROJECT LAYOUT

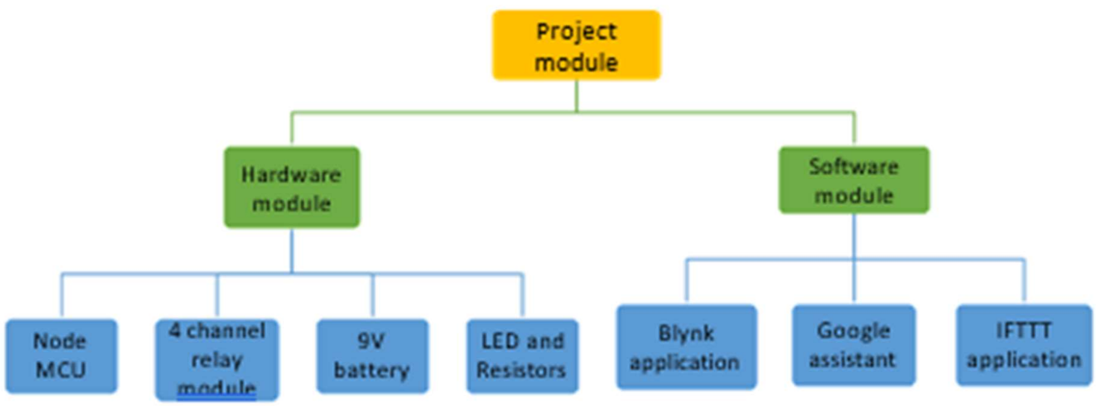


Figure 15. Layout of project module

CHAPTER 5
METHODOLOGY

METHODOLOGY

5.1 METHODOLOGY

AI-powered home automation refers to the use of artificial intelligence (AI) and machine learning to enhance and automate various aspects of your home, from controlling devices to improving energy efficiency and security. Here's a methodology for implementing AI in home automation:

1. Define Objectives: Start by defining your objectives and what you want to achieve with AI home automation. For example, you may want to improve energy efficiency, enhance security, or make your daily routines more convenient.
2. Assess Your Needs: Identify the specific areas or devices in your home that could benefit from automation and AI. This could include lighting, heating and cooling systems, security cameras, smart appliances, and more.
3. Select the Right AI Platform: Choose an AI platform or framework that suits your needs. Popular options include Amazon Alexa, Google Assistant, Apple Home Kit, or open-source platforms like Home Assistant. Ensure compatibility with your existing smart devices.
4. Smart Device Integration: Connect and integrate your existing smart devices with the AI platform. Ensure that your devices are compatible and can communicate with the platform effectively.
5. Data Collection and Analysis: Implement sensors and data collection devices to gather information about your home environment. This data will be used to make informed decisions. AI can analyze this data to provide insights and automation triggers.
6. Machine Learning Models: Develop or use pre-built machine learning models to analyze the data. These models can help predict user preferences, detect anomalies (e.g., security breaches or water leaks), and optimize energy usage.
7. Automation Rules: Set up automation rules based on the insights and predictions from your machine learning models. For example, you can create rules to adjust thermostat settings based on your daily routines, or to turn off lights when a room is unoccupied.
8. Voice and App Control: Configure voice commands and mobile apps to control your AI-driven home automation system. This allows you to interact with and manage your smart devices easily.

CHAPTER 6
SCHEMATIC
&
FLOWCHART

SCHEMATIC & FLOWCHART

6.1 Full System Schematic

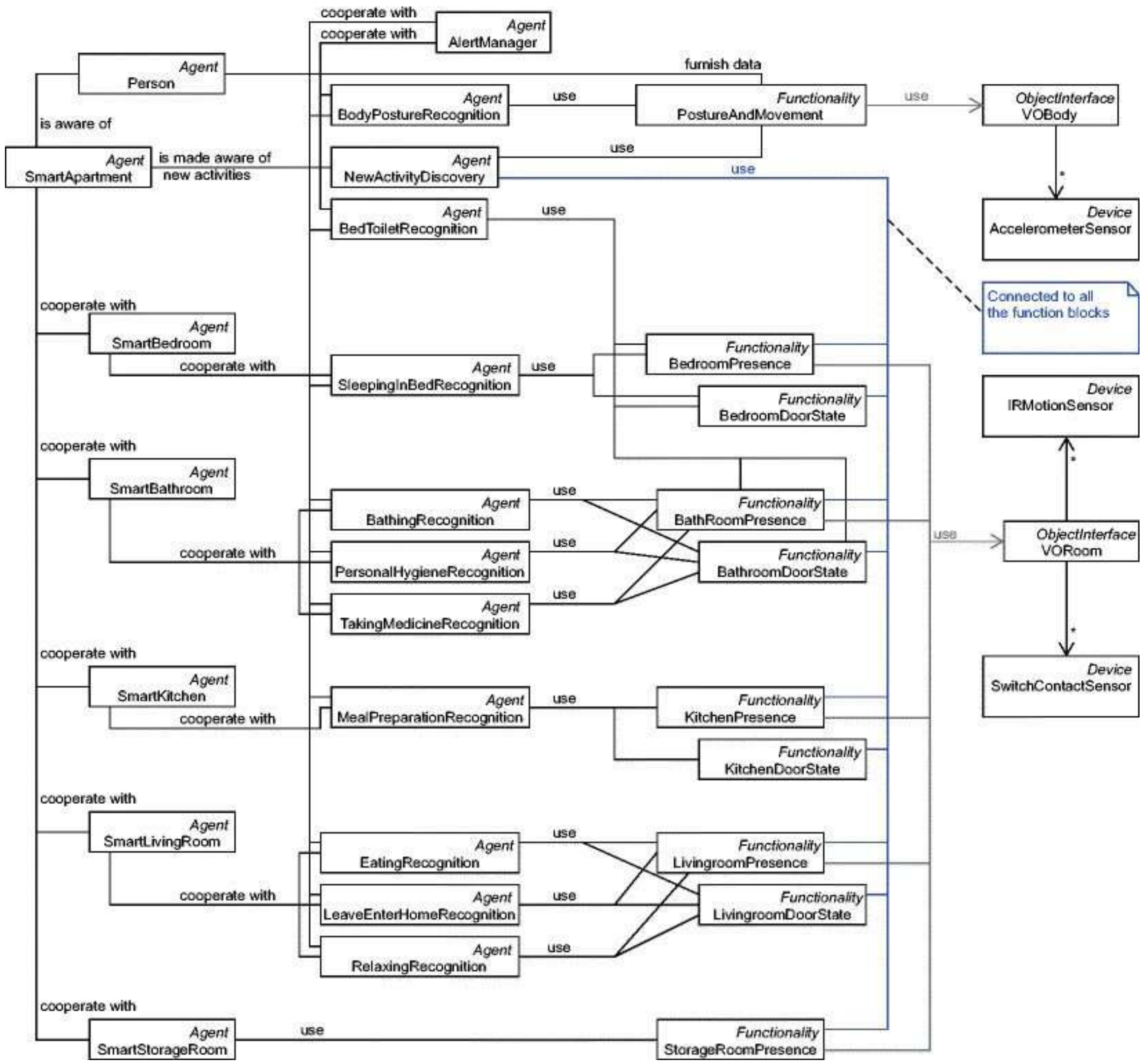


Fig: Full System Schematic Diagram

6.2 CIRCUIT DIGRAM

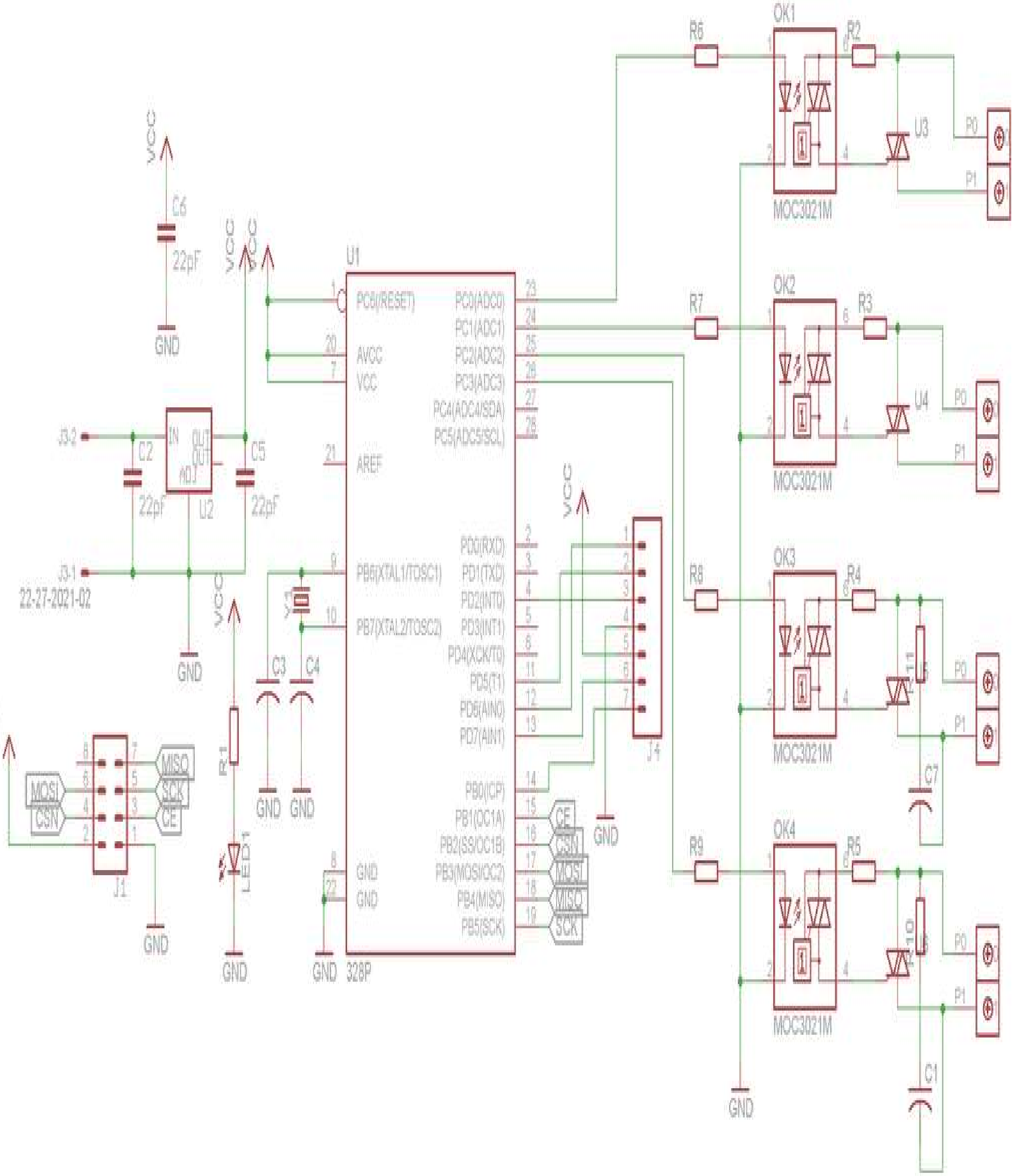


Fig 17 : Circuit Diagram

6.3 FLOWCHART

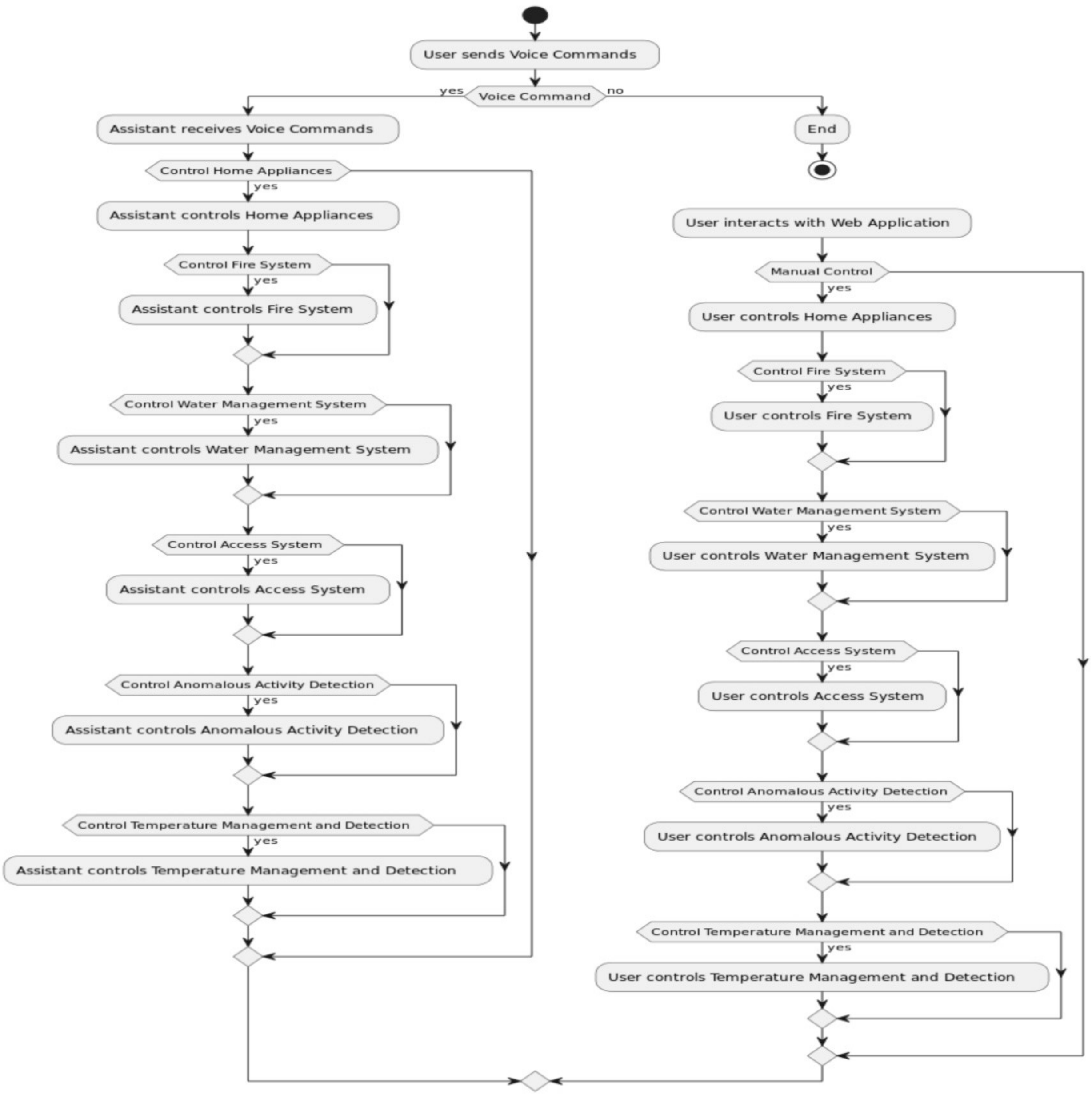


Fig 18 : Flowchart of System

CHAPTER 7
APPLICATIONS

APPLICATION's

AI smart automation has a wide range of applications across various sectors. Here are some notable applications of AI in smart automation:

1. **Home Automation:**
   - Smart Assistants: Devices like Amazon Echo or Google Home utilize AI to understand and respond to user commands, controlling various smart home devices.
   - Energy Management: AI algorithms can optimize energy usage by adjusting lighting, heating, and cooling systems based on occupancy and preferences.
2. **Industrial Automation**:
   - Predictive Maintenance: AI can analyze equipment data to predict when machinery is likely to fail, enabling timely maintenance and minimizing downtime.
   - Robotic Process Automation (RPA): Robots powered by AI algorithms can perform repetitive tasks with high precision and efficiency.
3. **Healthcare**:
   - Medical Diagnostics: AI algorithms can analyze medical images, such as X-rays and MRIs, to detect abnormalities and assist in diagnosis.
   - Patient Monitoring: AI-powered devices can monitor patient vitals and alert healthcare providers of any anomalies.
4. **Transportation**:
   - Autonomous Vehicles: AI plays a crucial role in enabling self-driving cars, optimizing routes, and ensuring safe navigation.
   - Traffic Management: AI algorithms can analyze traffic patterns and adjust signals in real-time to optimize traffic flow.
5. **Retail**:
   - Personalized Marketing: AI can analyze customer data to provide personalized product recommendations and targeted marketing campaigns.
   - Inventory Management: AI-powered systems can forecast demand, optimize inventory levels, and automate replenishment processes.
6. **Finance**:
   - Fraud Detection: AI algorithms can analyze transaction data to detect fraudulent activities and alert financial institutions.
   - Algorithmic Trading: AI-driven trading systems can analyze market trends and execute trades at optimal times.
7. **Agriculture**:
   - Precision Farming: AI-powered drones and sensors can monitor crop health, optimize irrigation, and detect pest infestations. –
   - Robotic Harvesting: Robots equipped with AI algorithms can harvest crops with precision and efficiency.
8. **Smart Cities**:
   - Infrastructure Management: AI can monitor and optimize city infrastructure, such as traffic lights, waste management, and energy distribution.

- Public Safety: AI-powered surveillance systems can analyze video feeds to detect suspicious activities and enhance public safety.

These are just a few examples highlighting the diverse applications of AI smart automation across different industries, demonstrating its transformative potential in enhancing efficiency, productivity, and innovation.

CHAPTER 8
CONCLUSION

CONCLUSION

The integration of AI into smart automation heralds a new era of efficiency, innovation, and personalized experiences across various sectors. From the comfort of our homes to the vast expanses of industrial landscapes, AI-powered solutions are revolutionizing the way we interact with technology and manage complex systems.

By leveraging advanced algorithms and data analytics, AI smart automation offers unparalleled advantages, including enhanced productivity, optimized resource utilization, and predictive insights. As we continue to advance in this digital age, embracing the transformative potential of AI smart automation will be crucial in shaping a more connected, intelligent, and sustainable future.

In summary, the applications of AI in smart automation are vast and transformative, paving the way for a smarter, more efficient world where technology works seamlessly to enhance our lives.

BIBLIOGRAPHY

1. *"Smart Energy Efficient Home Automation System using IOT", by Satyendra K. Vishwakarma, Prashant Upadhyaya, Babita Kumari, Arun Kumar Mishra.*

2. *"IOT Based Smart Security and Home Automation", by Shardha Somani, Parikshit Solunke, Shaunak Oke, Parth Medhi, Prof. P. P. Laturkar.*

3. *"A Dynamic Distributed Energy Management Algorithm of Home Sensor Network for Home Automation System", by Tui-Yi Yang, Chu-Sing Yang, Tien-Wen Sung; in 2016 Third International Conference on Computing Measurement Control and Sensor Network.*

4. *"Enhance Smart Home Automation System based on Internet of Things", by Tushar Churasia and Prashant Kumar Jain; in Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019) IEEE Xplore Part Number:CFP19OSV- ART; ISBN:978-1-7281-4365-1*

5. *"Visual Machine Intelligence for Home Automation", by Suraj, Ish Kool, Dharmendra Kumar, Shovan Barman.*

6. *"A Low Cost Home Automation System Using Wi-Fi based Wireless Sensor NetworkIncorporating internet of Things", by Vikram.N, Harish.K.S, Nihaal.M.S, Raksha Umesh, Shetty Aashik Ashok Kumar; in 2017 IEEE 7th International Advance Computing Conference.*

7. *"Voice Controlled Home Automation System using Natural Language Processing and Internet of Things", by Mrs. Paul Jasmin Rani, Jason Bakthakumar, Praveen Kumaar.B, Praveen Kumaar.U, Santhosh Kumar; in 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)*

8. *Wikipedia(2009). HomeAutomation. From https://en.wikipedia.org/wiki/Home_automation*

9. *Theory of IOT from :https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT*

10. *About Node MCU from: https://lastminuteengineers.com/esp8266-nodemcu-arduino-tutorial/*

APPENDIX

Fig 19: NODE MCU

FIG 20: REGISTOR

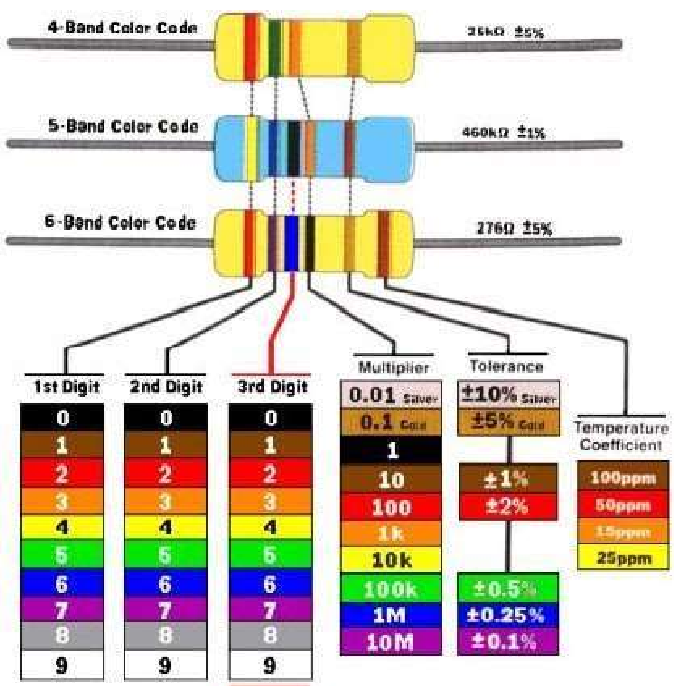


FIG 21: COLOUR CODE OF RESISTOR

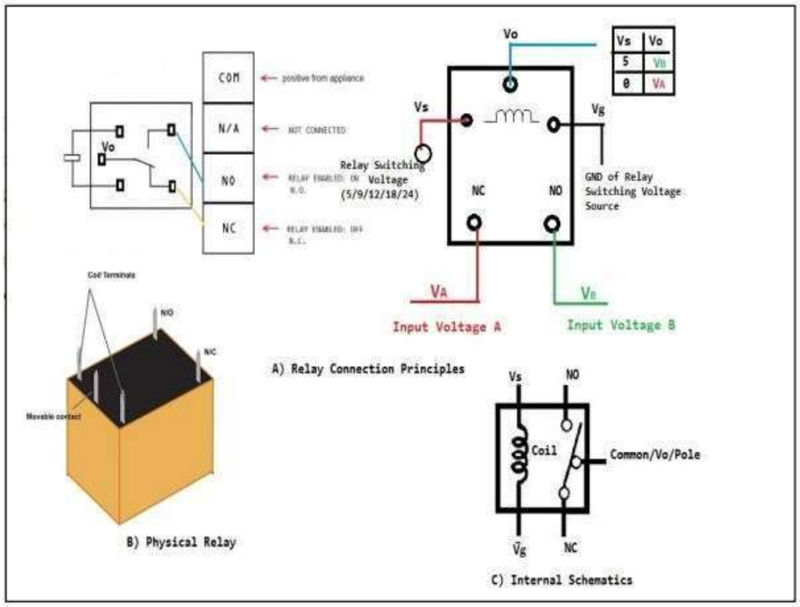


FIG 22: 6V CUBE RELAY

FIG 23: 4 CHANNEL RELAY

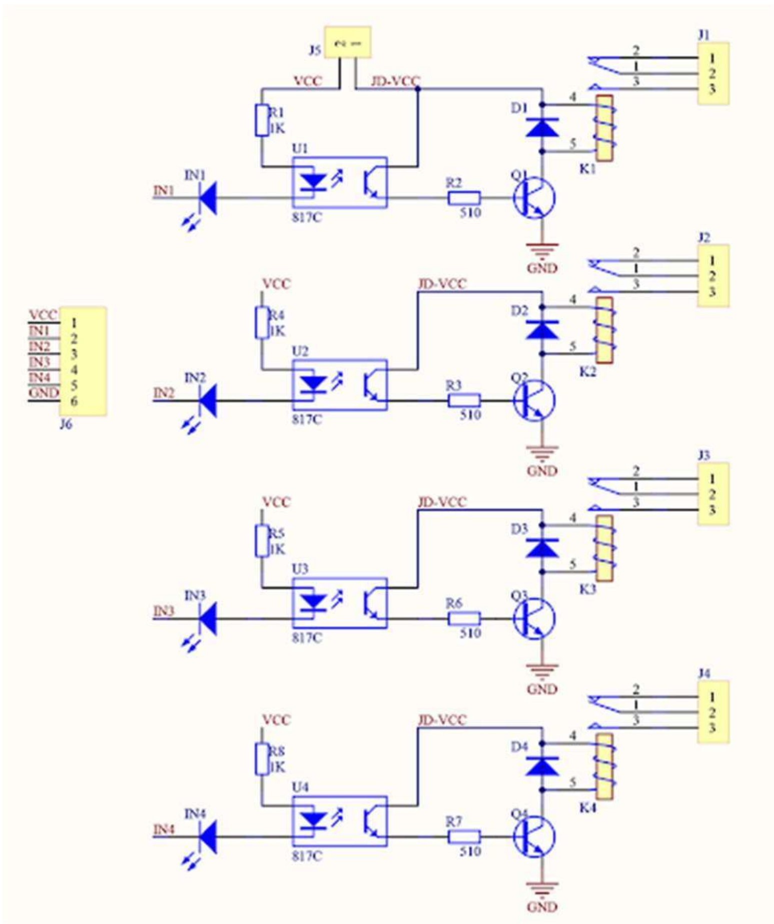


FIG 24: SCHEMATIC OF RELAY MODULE