AMERICAN JOURNAL OF BOTANY AND BIOENGINEERING
https://biojournals.us/index.php/AJBB
ISSN: 2997-9331

Article

Smart home by using IOT

Mohammed Abdul Kareem Kaml [1]
Saif Ali Hadi [2]
Baqer Sattar Muneam [3]
Zaid Husam Mohammed Ali [4]
Mohammed Raad Hashem [5]

Citation: Kaml, M. A. K., Hadi, S. A., Muneam, B. S., Ali, Z. H. M., & Hashem, M. R. (2025). Smart home by using IoT. American Journal of Botany and Bioengineering, 2(1), 81–100.

Received: 4th Jan 2025
Revised: 10th Jan 2025
Accepted: 14th Jan 2025
Published: 17th Jan 2025

[1] Al-Hussian University College, Medical Devices Technology Engineering
[2] Al-Hussian University College, Medical Devices Technology Engineering
[3] Al-Hussian University College, Medical Devices Technology Engineering
[4] Al-Hussian University College, Medical Devices Technology Engineering
[5] Al-Hussian University College, Medical Devices Technology Engineering
*Correspondence: email@gmail.com

Abstract: The Smart Home Automation System Based on IoT (Internet of Things) Is Designed to Provide an Intelligent and Connected Environment Within a Residential Setting. The System Utilizes Sensors, Actuators, And Internet Connectivity to Enable Automation, Control, And Monitoring of Various Home Devices and Systems. Through The Integration of IoT Technologies, The Smart Home Automation System Enhances Convenience, Energy Efficiency, Security, And Overall Comfort for The Residents. The Internet of Things (IoT) describes a network infrastructure of identifiable things that share data through the Internet. A smart home is one of the applications for the Internet of Things. In a smart home, household appliances could be monitored and controlled remotely. This raises a demand for reliable security solutions for IoT systems. Authorization and authentication are challenging IoT security operations that need to be considered. For instance, unauthorized access, such as cyber-attacks, to a smart home system could cause danger by controlling sensors and actuators, opening the doors for a thief. This paper applies an extra layer of security of multi-factor authentication to act as a prevention method for mitigating unauthorized access. One of those factors is face recognition, as it has recently become popular due to its non-invasive biometric techniques, which is easy to use with cameras attached to most trending computers and smartphones. In this paper, the gaps in existing IoT smart home systems have been analyzed, and we have suggested improvements for overcoming them by including necessary system modules and enhancing user registration and log-in authentication. We propose software architecture for implementing such a system. To the best of our knowledge, the existing IoT smart home management research does not support face recognition and liveness detection within the authentication operation of their suggested software architectures

Keywords: Smart home automation, IoT, multi-factor authentication, face recognition, energy efficiency, security solutions, biometric authentication, smart home systems

Introduction

A Smart home automation system based on the internet of things (IoT) can be an efficient way to manage your home. The system can include smart devices, such as a thermostat, that are connected to the internet. These devices can be controlled through an automation system, which can make it easier to manage your home's temperature and energy use. Additionally, a smart home automation system can enhance your home's security and energy efficiency. The home automation system is a mobile web-based application. This paper can be customized a lot as it has multiple GPIO port that can be programmed and they can give the user control over various things from his smart phone like security, surveillance, lighting, energy management, access control, entertainment. Home automation system should also provide a user-friendly interface on the host side, so that devices can be easily setup, monitored and controlled. The main reason to develop this system is to save time and manpower along with maintaining security and convenience. This is how an automated system proves useful to people in providing them security, comfort and easily accessible. The Internet of Things (IoT) is a system of sensors and actuators embedded in physical objects equipped with unique identifiers and the ability to transfer data over both wired and wireless networks. The substantial development activity in IoT includes many categories, such as smart grid, smart logistics, environment and safety testing, intelligent transportation, industrial control and automation, finance and service, military defense, health care, fine agriculture, and smart homes. Smart homes are homes that incorporate a communication network that connects the key sensors and actuators, and allows them to be accessed, monitored or controlled remotely. In a smart home, there are certain characteristics; the network size is small, the number of users is very few (as it is restricted to the family members), and different network connectivity can be used, such as 3G, 4G, and Wi-Fi. The data management occurs through a local server; IoT Devices are using RFID or WSN wireless technologies, and the bandwidth requirement is small. The smart home is also known as house automation, in which domestic activities are made more comfortable, convenient, secure and economical. As a result, home automation became popular due to its numerous benefits. A home automation system consists of four main components. The first is the user interface, such as a computer or phone used to give orders to the control system. The second component is the transmission mode, which is the Ethernet (wired), or Bluetooth (wireless). The third is the central controller, which is the hardware interface that communicates with the user interface by controlling electronic devices. The final component is various electronic devices, such as an air conditioner, a lamp, or a heater that are compatible with the mode of transmission, and connected to the central controlling system. There are many challenges present in IoT systems, such as management, performance, privacy, and security. The security challenges include authorization, authentication, and access control. Therefore, registration and log-in are important security operations in a smart home system, as unauthorized access to the system (such as a cyber-attack) could cause danger by opening the door for a thief, threatening the safety of residents and their belongings. In this paper, we suggest a user-friendly multi-factor authentication for the proposed smart home system. One of those factors is the password, and the other factor is facing recognition. The integration scenario for face recognition and liveness detection with the log-in operation to smart home is a novelty for this paper. Multifactor authentication is a secure authentication process combined of more than one authentication technique chosen from various independent categories of credentials to provide better way of validating legitimate users. Multi-factor authentication creates a layered hindrance, thus making it more difficult for an unauthorized individual to reach the system. In this case, even if attackers break one factor, they still have one more impediment to break before they can access the system. The two-factor authentication solution is cost effective to customers, and has the means of providing flexible and strong authentication. It reduces the fraud rate when compared to one factor authentication. The use of multi-factor authentication is growing in order to help verify the identities of users requesting to access the system for information that could be sensitive or could control the system. The four most common types of authentication factors are the cognitive information (such as passwords), items that a user

possesses (such as smart cards), a biometric trait of the user (such as face recognition and fingerprints), and a user's location information (such as IP address and GPS). This research presents a novel contribution in comparison to the previous research by suggesting a log-in module for managing the operations of user registration and log-in more securely. This module is integrated within the suggested software architecture of the IoT smart home, and then it is explained in detail. In this research, the added features to the smart home system are compared to the smart home systems of related work in the discussion section of this paper. The integration of face recognition and liveness modules within the log-in module is first presented by this research[1].

The internet of things, or IoT, is a network of interrelated devices that connect and exchange data with other IoT devices and the cloud. IoT devices are typically embedded with technology such as sensors and software and can include mechanical and digital machines and consumer objects.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, deliver enhanced customer service, improve decision-making and increase the value of the business.

With IoT, data is transferable over a network without requiring human-to-human or human-to-computer interactions.

A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low, or any other natural or man-made object that can be assigned an Internet Protocol address and is able to transfer data over a network.

An IoT ecosystem consists of web-enabled smart devices that use embedded systems -- such as processors, sensors and communication hardware -- to collect, send and act on data they acquire from their environments.

IoT devices share the sensor data they collect by connecting to an IoT gateway, which acts as a central hub where IoT devices can send data. Before the data is shared, it can also be sent to an edge device where that data is analyzed locally. Analyzing data locally reduces the volume of data sent to the cloud, which minimizes bandwidth consumption.

Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices -- for example, to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these webenabled devices largely depend on the specific IoT applications deployed.

IoT can also use artificial intelligence and machine learning to aid in making data collection processes easier and more dynamic.[2]

Some of the advantages of IoT include the following:

- Enables access to information from anywhere at any time on any device.
- Improves communication between connected electronic devices.
- Enables the transfer of data packets over a connected network, which can save time and money.
- Collects large amounts of data from multiple devices, aiding both users and manufacturers.
- Analyzes data at the edge, reducing the amount of data that needs to be sent to the cloud.
- Automates tasks to improve the quality of a business's services and reduces the need for human intervention.
- Enables healthcare patients to be cared for continually and more effectively.

Some disadvantages of IoT include the following:

- Increases the attack surface as the number of connected devices grows. As more information is shared between devices, the potential for a hacker to steal confidential information increases.

- Makes device management challenging as the number of IoT devices increases. Organizations might eventually have to deal with a massive number of IoT devices, and collecting and managing the data from all those devices could be challenging.
- Has the potential to corrupt other connected devices if there's a bug in the system.
- Increases compatibility issues between devices, as there's no international standard of compatibility for IoT. This makes it difficult for devices from different manufacturers to communicate with each other.

IoT helps people live and work smarter. Consumers, for example, can use IoTembedded devices -- such as cars, smartwatches or thermostats -- to improve their lives. For example, when a person arrives home, their car could communicate with the garage to open the door; their thermostat could adjust to a preset temperature; and their lighting could be set to a lower intensity and color.

In addition to offering smart devices to automate homes, IoT is essential to business. It provides organizations with a real-time look into how their systems really work, delivering insights into everything from the performance of machines to supply chain and logistics operations.

IoT enables machines to complete tedious tasks without human intervention. Companies can automate processes, reduce labor costs, cut down on waste and improve service delivery. IoT helps make it less expensive to manufacture and deliver goods, and offers transparency into customer transactions.

IoT is one of the most important technologies and it continues to advance as more businesses realize the potential of connected devices to keep them competitive.

IoT offers several benefits to organizations. Some benefits are industry-specific and some are applicable across multiple industries. Common benefits for businesses include the following:

- Monitors overall business processes.
- Improves the customer experience.
- Saves time and money.
- Enhances employee productivity.
- Provides integration and adaptable business models.
- Enables better business decisions.
- Generates more revenue.

IoT encourages companies to rethink how they approach their businesses and gives them the tools to improve their business strategies.

Generally, IoT is most abundant in manufacturing, transportation and utility organizations that use sensors and other IoT devices; however, it also has use cases for organizations within the agriculture, infrastructure and home automation industries, leading some organizations toward digital transformation.

IoT can benefit farmers in agriculture by making their job easier. Sensors can collect data on rainfall, humidity, temperature and soil content and IoT can help automate farming techniques.

IoT can also help monitor operations surrounding infrastructure. Sensors, for example, can monitor events or changes within structural buildings, bridges and other infrastructure that could potentially compromise safety. This provides benefits such as improved incident management and response, reduced costs of operations and improved quality of service.

A home automation business can use IoT to monitor and manipulate mechanical and electrical systems in a building. On a broader scale, smart cities can help citizens reduce waste and energy consumption.[3]

IoT touches every industry, including healthcare, finance, retail and manufacturing.

Project outline

Chapter one

Introduction of the project.

Chapter two

We will present the theoretical basis of project
And define all the components that are used in project and description on microcontroller.

Chapter three

In this chapter, we explain the mechanism of the proposed system and the details of its implementation and design.

Literature Review

In this literature review, we will explore some of the key research papers on this topic.

1-"Smart Energy Monitoring and Control System Based on IoT" by Chunxiao Li et al. (2018) his paper proposed a smart energy monitoring and control system based on IoT, which uses wireless sensors to collect data from energy meters and sends it to the cloud for analysis. The system allows users to monitor their energy consumption in real-time and control their energy usage remotely using a mobile app. The proposed system was evaluated in a real-world setting, and the results showed that it could effectively reduce energy consumption.

2-"IoT-Based Smart Energy Monitoring and Control System for Sustainable Energy Management" by N. Nandhini et al. (2020) This paper proposed an IoT-based smart energy monitoring and control system for sustainable energy management. The system uses a combination of wireless sensors, smart meters, and cloud computing to monitor energy consumption and control energy usage. The system also includes a mobile app that allows users to monitor their energy usage and receive alerts when their energy consumption exceeds a certain threshold. The proposed system was evaluated in a real-world setting, and the results showed that it could effectively reduce energy consumption.[4]

3-"Smart Energy Management System Based on IoT" by M. Firdhous et al. (2019(This paper proposed a smart energy management system based on IoT, which uses a combination of wireless sensors, smart meters, and cloud computing to monitor energy consumption and control energy usage. The system includes a mobile app that allows users to monitor their energy usage and receive alerts when their energy consumption exceeds a certain threshold. The proposed system was evaluated in a real-world setting, and the results showed that it could effectively reduce energy consumption .

4-"A Review on Internet of Things (IoT)-Based Energy Management Systems for Smart Homes" by T. Thamizh Selvan et al. (2020) This paper provides a comprehensive review of IoT-based energy management systems for smart homes. The paper discusses various IoT-based energy management systems, including smart meters, wireless sensors, and cloud computing, and provides a detailed analysis of their features, advantages, and limitations. The paper also discusses the challenges and future research directions in the field of IoT-based energy management systems for smart homes.

The research papers discussed above provide valuable insights into the design and implementation of IoT-based energy meter monitoring systems. These systems have the potential to reduce energy consumption and promote sustainable energy management, which is critical for a greener future.[5]

Materials and Methods

The project consists of the following main parts:

1-Arduino UNO

2- Esp8266 WIFI

3-Current Sensor ACS712

4- Four Channal Relay

2.2.1 Arduino UNO

Arduino Uno is a microcontroller board based on the ATmega328P (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator (CSTCE16M0V53-R0), a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. You can tinker with your Uno without worrying too much about doing something wrong, worst-case scenario you can replace the chip for a few dollars and start over again.[6]
"Uno" means one in Italian and was chosen to mark the release of Arduino Software (IDE) 1.0. The Uno board and version 1.0 of Arduino Software (IDE) were the reference versions of Arduino, now evolved to newer releases. The Uno board is the first in a series of USB Arduino boards, and the reference model for the Arduino platform; for an extensive list of current, past or outdated boards see the Arduino index of boards.
The Arduino UNO is a standard board of Arduino. Here UNO means 'one' in

Italian. It was named as UNO to label the first release of Arduino Software. It was also the first USB board released by Arduino. It is considered as the powerful board used in various projects. Arduino.cc developed the Arduino UNO board.
Arduino UNO is based on an ATmega328P microcontroller. It is easy to use compared to other boards, such as the Arduino Mega board, etc. The board consists of digital and analog Input/Output pins (I/O), shields, and other circuits.

The Arduino UNO includes 6 analog pin inputs, 14 digital pins, a USB connector, a power jack, and an ICSP (In-Circuit Serial Programming) header. It is programmed based on IDE, which stands for Integrated Development
Environment. It can run on both online and offline platforms.[7]

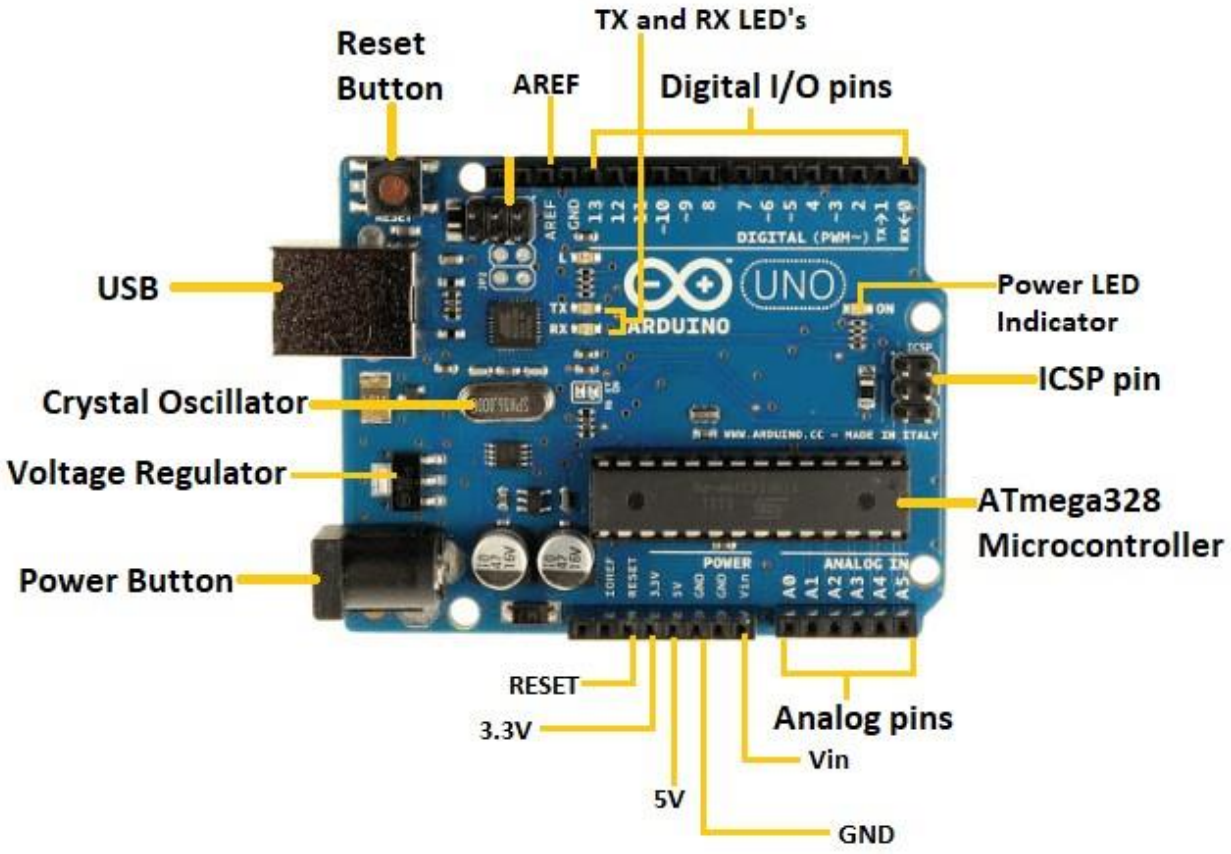


Figure (2.1) Arduino Uno Pinout

o **ATmega328 Microcontroller**- It is a single chip Microcontroller of the Atmel family. The processor code inside it is of 8-bit. It combines **Memory (SRAM, EEPROM, and Flash), Analog to Digital Converter, SPI serial ports, I/O lines, registers, timer, external and internal interrupts, and oscillator.**

o **ICSP pin** - The In-Circuit Serial Programming pin allows the user to program using the firmware of the Arduino board.

o **Power LED Indicator**- The ON status of LED shows the power is activated. When the power is OFF, the LED will not light up.

o **Digital I/O pins**- The digital pins have the value HIGH or LOW. The pins numbered from D0 to D13 are digital pins.

o **TX and RX LED's**- The successful flow of data is represented by the lighting of these LED's.

o **AREF-** The Analog Reference (AREF) pin is used to feed a reference voltage to the Arduino UNO board from the external power supply.

o **Reset button**- It is used to add a Reset button to the connection.

o **USB**- It allows the board to connect to the computer. It is essential for the programming of the Arduino UNO board.

o **Crystal Oscillator**- The Crystal oscillator has a frequency of 16MHz, which makes the Arduino UNO a powerful board.

o **Voltage Regulator**- The voltage regulator converts the input voltage to 5V. o **GND**- Ground pins. The ground pin acts as a pin with zero voltage. o **Vin**- It is the input voltage.

- **Analog Pins**- The pins numbered from A0 to A5 are analog pins. The function of Analog pins is to read the analog sensor used in the connection. It can also act as GPIO (General Purpose Input Output) pins.[8]

2.2.2 Esp8266 Wi-Fi

ESP8266 is a low-cost Wi-Fi module that can be used in a wide variety of Internet of Things (IoT) projects. It was first introduced by the Chinese company Espressif Systems in 2014 and quickly gained popularity due to its low cost and ease of use. The ESP8266 module contains a microcontroller and a Wi-Fi module, which makes it possible to connect to a Wi-Fi network and communicate with other devices over the network. The module can be programmed using the Arduino IDE, which makes it easy to get started with programming and developing IoT projects. The ESP8266 module has a range of features that make it suitable for a wide variety of IoT projects [17][18]. Some of its features include: Support for 802.11 b/g/n Wi-Fi standards Support for WPA/WPA2 encryption Built-in TCP/IP protocol stack Built-in microcontroller 10-bit ADC for analog inputs SPI, I2C, and UART communication interfaces Low power consumption The ESP8266 module can be used in a wide variety of IoT projects, such as home automation, smart agriculture, industrial automation, and more. Its low cost and ease of use make it an ideal choice for hobbyists and makers who want to develop their own IoT projects.

Pin out

The ESP8266 module has different pinouts depending on the specific module being used. However, the most common pinout for the ESP8266 is as follows:

VCC: This is the power supply pin, which should be connected to a 3.3V power source.
GND: This is the ground pin.

TXD: This is the UART transmit pin.
RXD: This is the UART receive pin.

CH_PD: This is the chip enable pin, which should be connected to a 3.3V power source to enable the chip.

GPIO0: This is a general-purpose input/output pin. It is also used to put the ESP8266 module into programming mode.
GPIO2: This is another general-purpose input/output pin.

Reset: This is the reset pin, which can be used to reset the ESP8266 module. It is important to note that the ESP8266 module is a 3.3V device, and should not be powered with 5V, as this can damage the module [19][20]. Additionally, some modules may have additional pins for

Table 2.1: The ESP8266 pinout

Pin number	Pin Name	Pin function
1	Ground	Ground
2	GPIO1	General purpose IO, serial TX1
3	GPIO2	General purpose IO
4	CH_PD	Active high chip enables
5	GPIO0	General purpose IO, launch serial programming mode if low while reset or power ON

6	RESET	Active low external reset signal
7	GPIO3	General purpose IO, serial RX
8	VCC	Power supply

specific features or functions, so it is always recommended to refer to the datasheet or documentation for the specific module being used. [9]

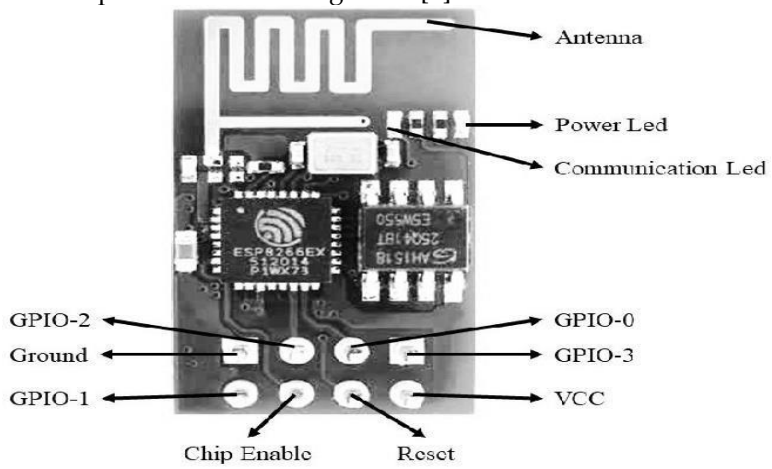


Figure (2.2) : The ESP8266 pinout

2.2.3 Current Sensor ACS712

The ACS712 is a series of integrated circuit (IC) current sensors developed by Allegro Microsystems. The ACS712 is designed to measure both AC and DC currents accurately and provide an output voltage proportional to the measured current. The output voltage of the ACS712 is linearly proportional to the measured current and can be directly read by a microcontroller or an analog-to-digital converter (ADC(.The ACS712 is available in different variants that can measure different current ranges, from a few milliamperes to several amperes. The most commonly used variants are the ACS712ELCTR-05B-T, ACS712ELCTR-20A-T, and ACS712ELCTR-30A-T, which can measure up to 5A, 20A, and 30A, respectively. The ACS712 has several advantages over traditional current sensing techniques, including low insertion loss, high accuracy, low power consumption, and small form factor. The ACS712 also eliminates the need for external calibration, as it is factory calibrated for accuracy . The ACS712 is widely used in a variety of applications, including motor control, power management, battery chargers, and energy metering. The ACS712 is also used in renewable energy systems, such as solar and wind power, to monitor the current flowing from the panels or the turbines. the ACS712 is a versatile and reliable current sensor that can be used in a wide range of applications. Its high accuracy, low power consumption, and small form factor make it an excellent choice for many embedded system projects .

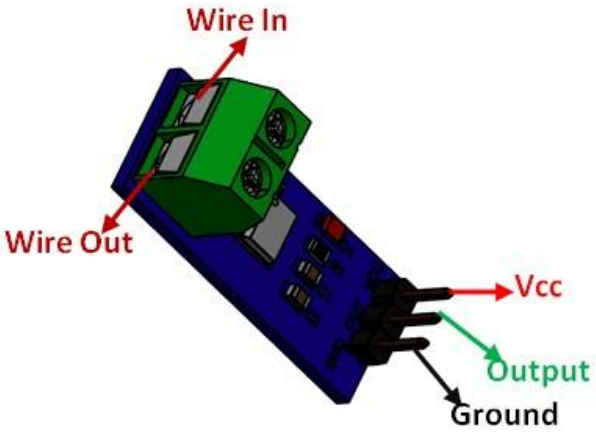


Figure (2.3) ACS712 current sensor pinout

Pinout

The ACS712 current sensor has a three-pin package, with the following pinout:

VCC: This pin is used to supply power to the sensor. The voltage applied to this pin should be between 4.5V and 5.5V.

OUT: This pin is used to output the voltage proportional to the measured current. The output voltage varies linearly with the measured current and has a sensitivity of 185 mV/A .

GND: This pin is connected to the ground.

The pinout of the ACS712 may vary slightly depending on the package used. For example, the ACS712ELC-05B variant uses a 5-pin package with additional pins for filtering and noise reduction. However, the basic pinout remains the same for all variants of the ACS712 current sensor .

2.2.4 Four-Channal Relay

The four-channel relay module contains four 5V relays and the associated switching and isolating components, which makes interfacing with a microcontroller or sensor easy with minimum components and connections. The contacts on each relay are specified for 250VAC and 30VDC and 10A in each case, as marked on the body of the relays.

The four-channel relay module contains four 5V relays and the associated switching and isolating components, which makes interfacing with a microcontroller or sensor easy with minimum components and connections. There are two terminal blocks with six terminals each, and each block is shared by two relays. The terminals are screw type, which makes connections to mains wiring easy and changeable.

The four relays on the module are rated for 5V, which means the relay is activated when there is approximately 5V across the coil. The contacts on each relay are specified for 250VAC and 30VDC and 10A in each case, as marked on the body of the relays.

The switching transistors act as a buffer between the relay coils that require high currents, and the inputs which don't draw much current. They amplify the input signal so that they can drive the coils to activate the relays. The freewheeling diodes prevent voltage spikes across the transistors when the

relay is turned off since the coils are an inductive load. The indicator LEDs glow when the coil of the respective relay is energized, indicating that the relay is active. The optocouplers form an additional layer of isolation between the load being switched and the inputs.
The isolation is optional and can be selected using the VCC selector jumper. The input jumper contains the main VCC, GND, and input pins for easy connection using female jumper wires.[10]

2.2.4.1 Four-Channel Relay Module Specifications

- Supply voltage – 3.75V to 6V
- Trigger current – 5mA
- Current when the relay is active - ~70mA (single), ~300mA (all four)
- Relay maximum contact voltage – 250VAC, 30VDC
- Relay maximum current – 10A

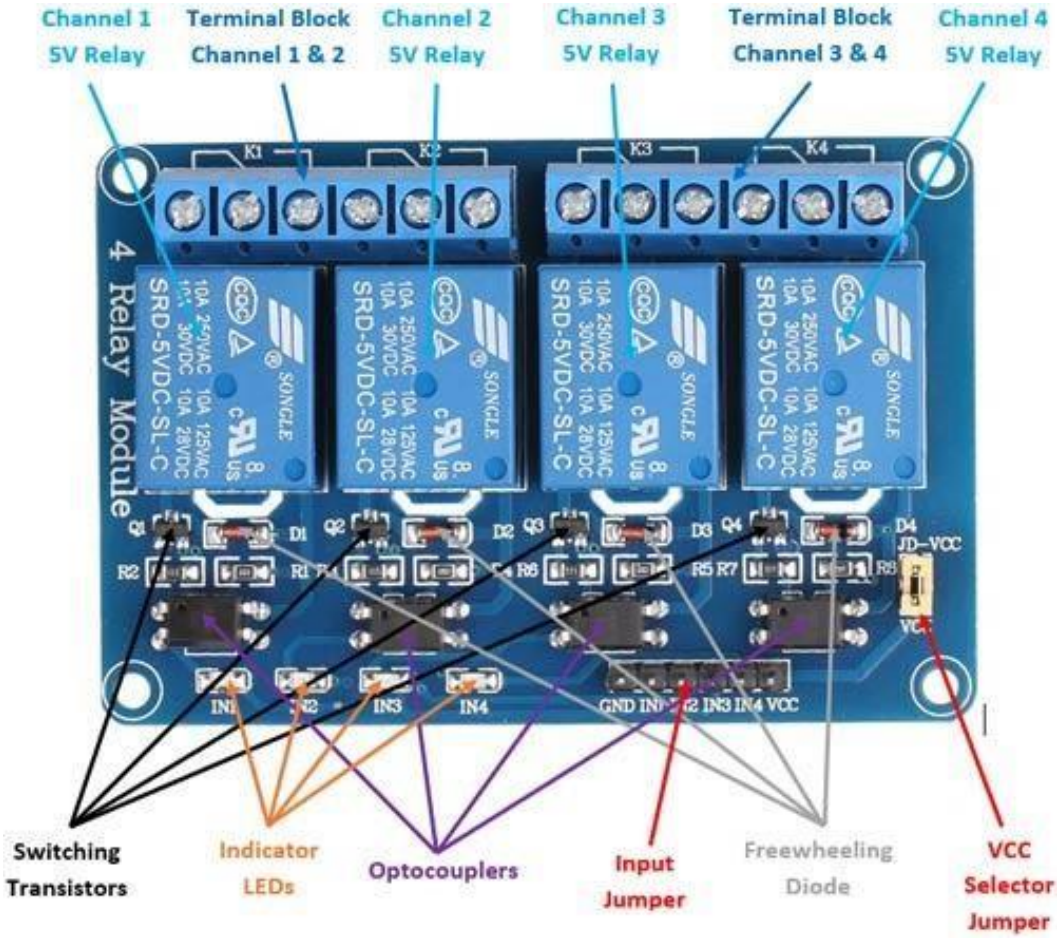


Figure (2.4) Four-Channel Relay Module

2.2.4.2 Internal Circuit Diagram for Four-Channel Relay Module The circuit on the board is as follows:

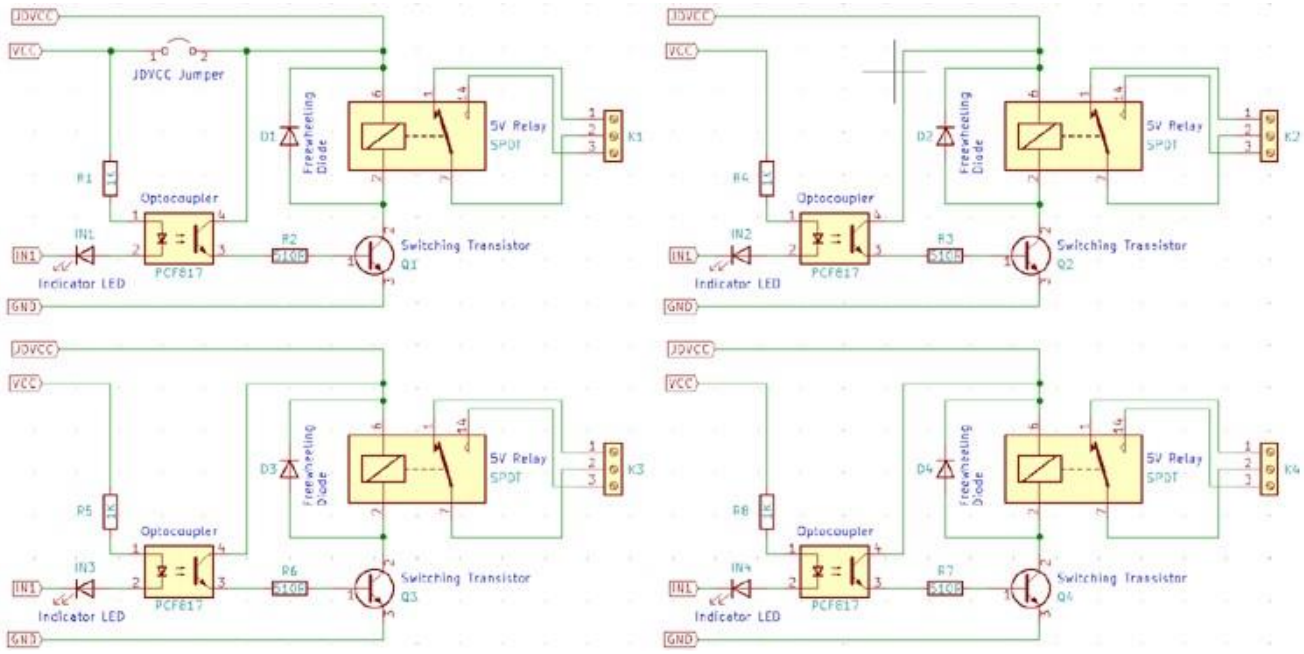


Figure (2.5) Internal Circuit Diagram for Four-Channel Relay Module

2.2.4.3 How to Use the Four-Channel Relay Module

The four-channel can be used to switch multiple loads at the same time since there are four relays on the same module. This is useful in creating a central hub from where multiple remote loads can be powered. It is useful for tasks like home automation where the module can be placed in the main switchboard and can be connected to loads in other parts of the house and can be controlled from a central location using a microcontroller.

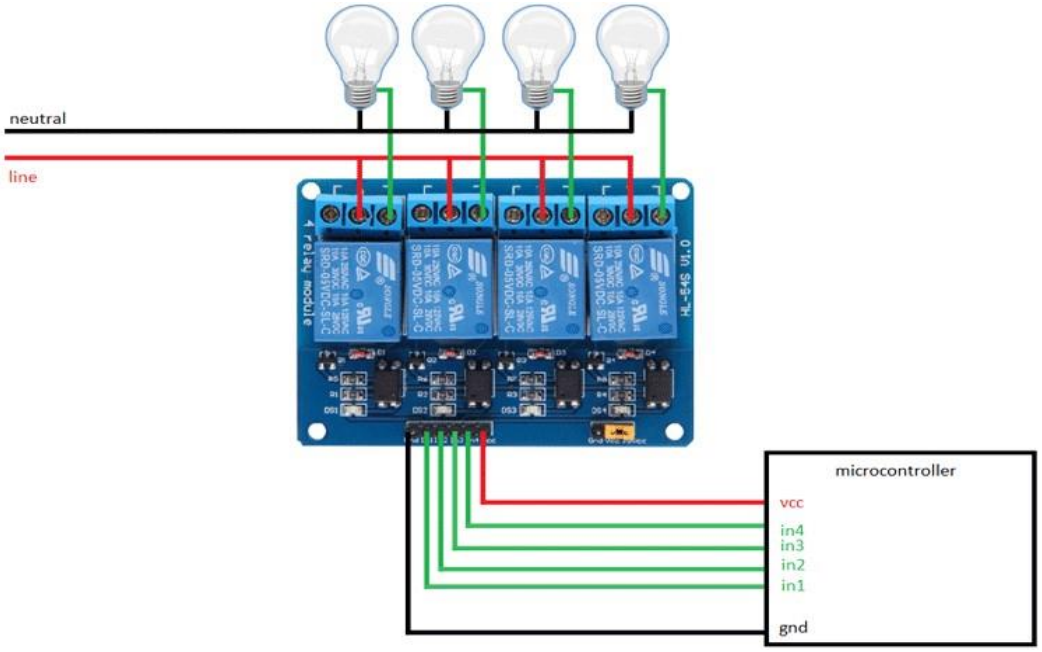


Figure (2.6) How to connect Four-Channel Relay Module

In this diagram, four separate loads (represented by lightbulbs) have been connected to the NO terminals of the relay. The live wire has been connected to the common terminal of each relay. When the relays are activated, the load is connected to the live wire and is powered. This setup can be reversed by connecting the load to the NC terminal that keeps it powered on till the relay is activated.

Pinout

The Four-channel relay module has a three-pin package, with the following pinout:

GND: Ground reference for the module
Input1: Input to activate relay 1

Input2: Input to activate relay 2

Input3: Input to activate relay 3

Input4: Input to activate relay 4

VCC: Power supply for the relay module

VCC: Power supply selection jumper

JD-VCC: Alternate power pin for the relay module

Design and implementation

3.1 introduction

In this chapter we will talk about how to link the electronic materials to our proposed project that we talked about in the previous chapter

3.2 Electronic proposed circuit design

3.2.1 Flow Charts:

The Flow Charts in **Figure (3.1)** below show that the connection between electronics components

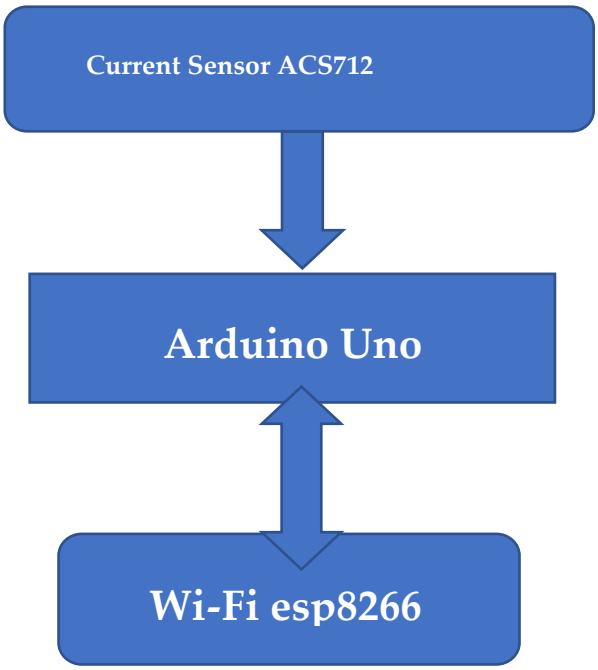


Figure (3.1) Flow Chart

3.2.2 Connection the circuit diagram Procedure

1- Connected the ACS712 current sensor to Arduino as shown in figure (3.2) below:

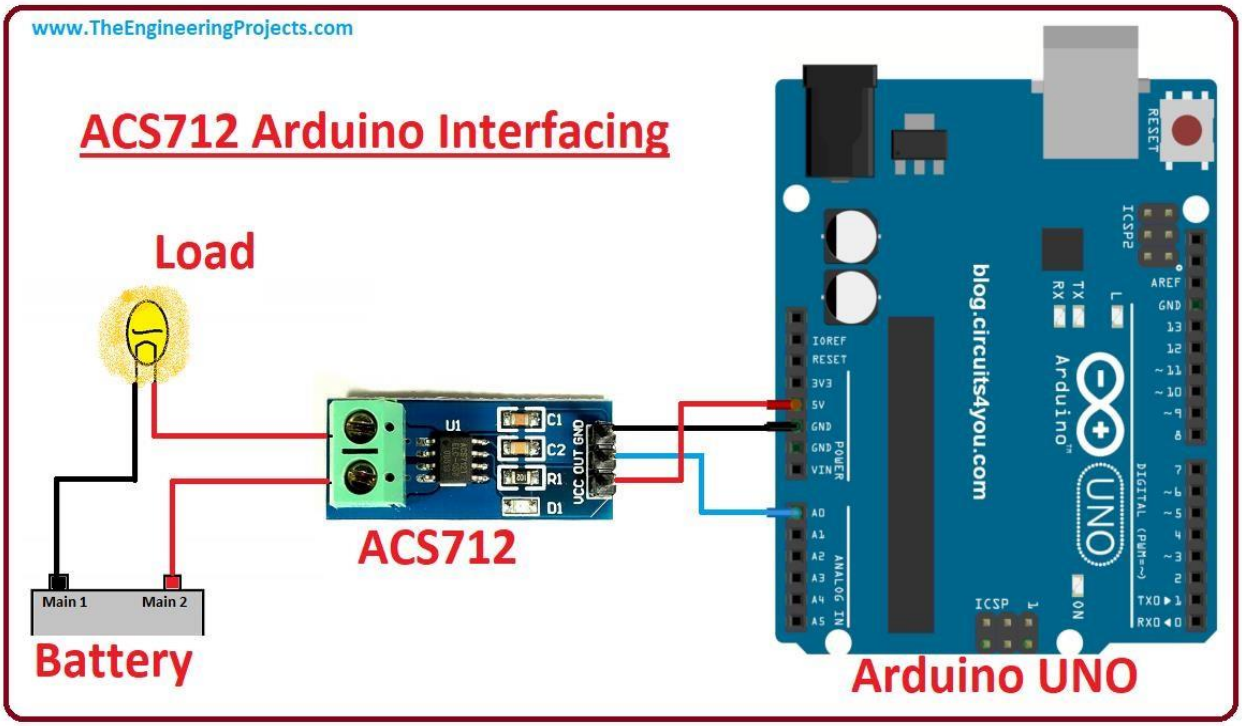


figure (3.2) ACS712 current sensor to Arduino connection

2-Connected the ESP8266 chip to Arduino as shown in figure (3.3):

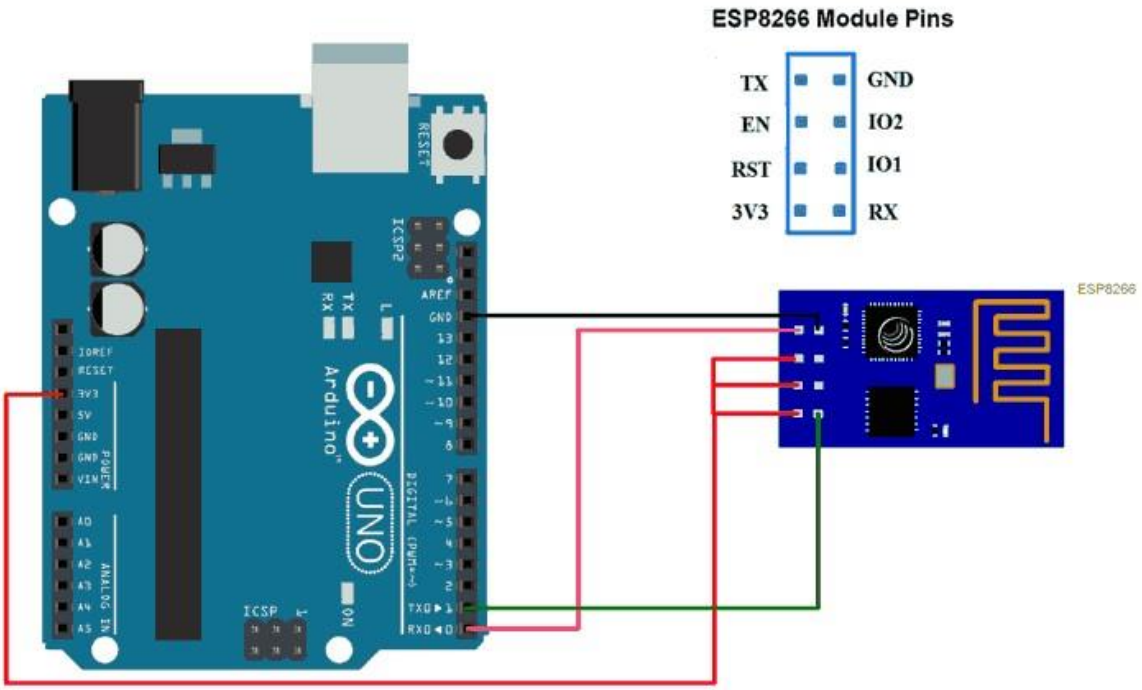


figure (3.3) Arduino UNO with ESP8266 Wi-Fi connection

3-Connected the 4-Ch Relay module to Arduino as shown in figure (3.4):

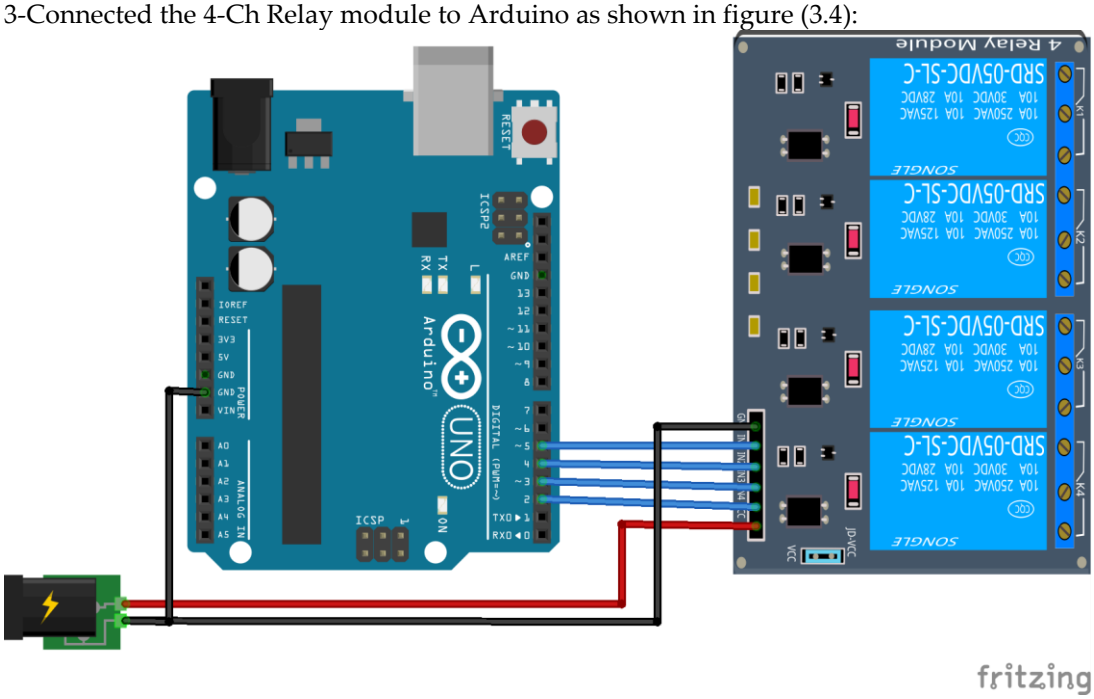


figure (3.4) Arduino UNO with 4-Ch relay

4- we insert our circuit in the plastic box as shown figure (3.5) below:

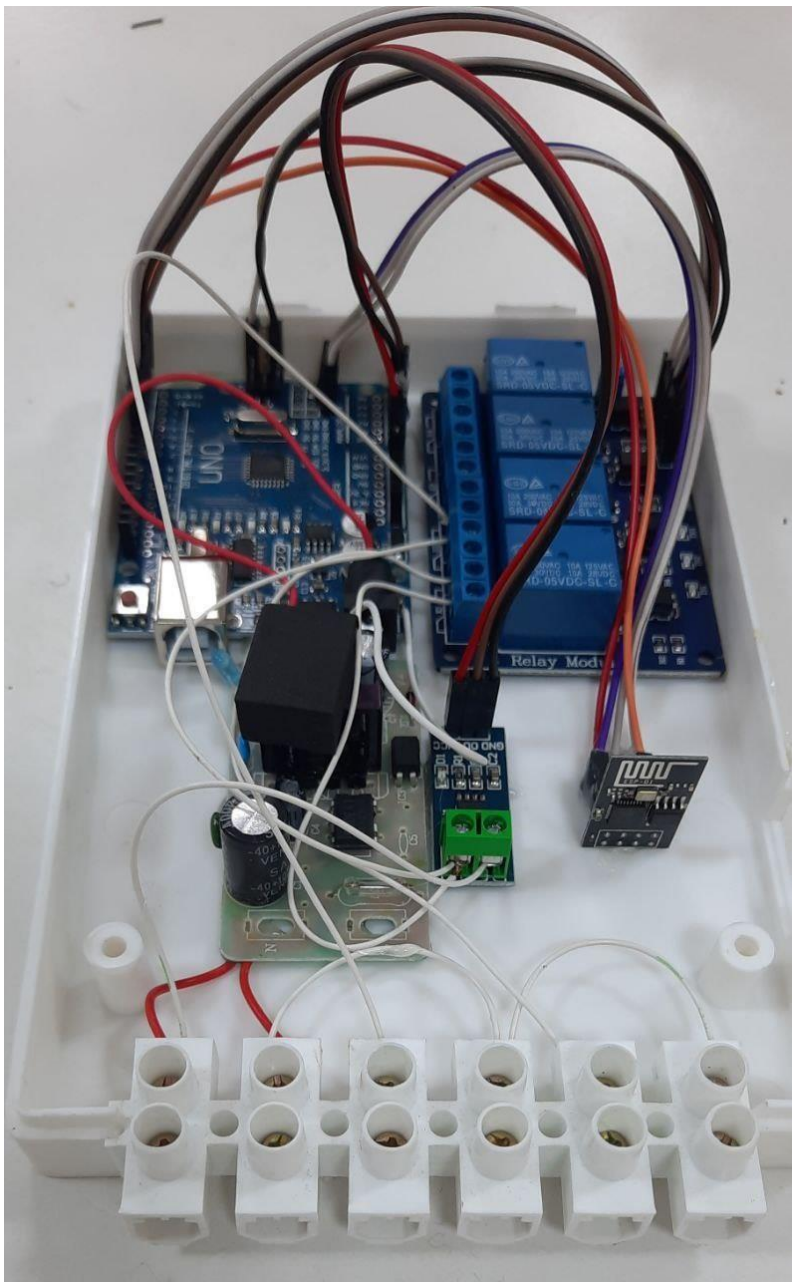


figure (3.5) proposed circuit in side box

5- After connection components install electric point on the pox as shown in figure (3.6) below:

figure (3.6) project shape from outside

Results and Discussion

Current Measurement: The ACS712 current sensor will provide analog voltage readings proportional to the current consumption of the device being monitored. By converting the analog readings to current values using appropriate calibration, you will be able to measure the current flowing through the device.

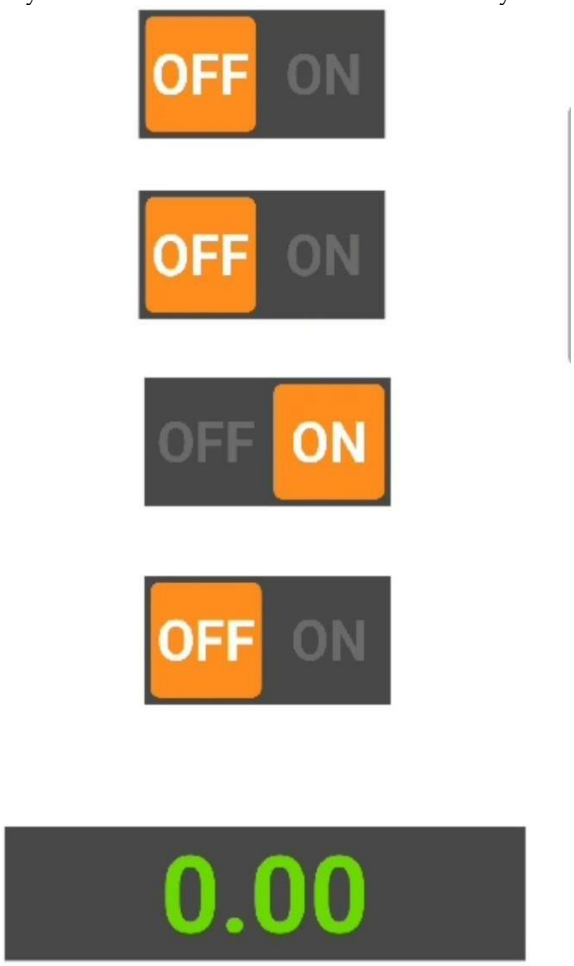
Remote Control: The ESP8266 module, when connected to the WIFI network and the server or platform, will allow you to remotely control the relay module. Sending commands to the module will switch the corresponding relay on or off, thereby controlling the power supply to the connected device.

Power State Change: When you send a command to turn the relay on or off, the power supply to the connected device will be toggled accordingly. You should observe the device turning on or off in response to the command.

Current Monitoring and Analysis: By monitoring the current readings received from the ACS712 sensor, you can observe the device's power consumption in real-time. You can analyze the data to understand patterns of energy usage and make informed decisions for energy optimization or load management.

It's important to note that the specific implementation and visualization of the results may vary based on the server or platform you use for data collection and analysis. You may need to develop or configure the server or platform to receive and process the data from the ESP8266 module and present it in a user-friendly manner.

Additionally, you can extend the experiment by integrating additional features, such as data logging, historical analysis, or integration with other smart home devices or systems. The possibilities are vast, and you can further enhance the functionality based on your requirements and creativity.[11]



Figure(4.1) Explains the mechanism for monitoring current consumption and controlling devices.

Conclusion

In conclusion, the experiment using Arduino Uno, ESP8266 Wi-Fi module, ACS712 current sensor, and a four-channel relay demonstrated a basic implementation of a smart home energy monitoring and control system using IoT. The experiment allowed for the measurement of current consumption, remote control of a connected device, and monitoring of power state changes.

By integrating the ACS712 current sensor, the system provided real-time current readings, enabling users to monitor and analyze the energy usage of the connected device. This data can be used to make informed decisions regarding energy optimization and load management.

The remote-control capability offered by the ESP8266 module and relay module allowed users to turn the connected device on or off remotely, providing convenience and flexibility in managing power consumption.

The experiment serves as a starting point for developing more advanced smart home solutions, such as integrating additional sensors, implementing advanced automation, or integrating with other smart home devices and platforms.

Overall, the experiment showcased the potential of IoT technology in creating smart home systems that enhance energy efficiency, convenience, and control.[12]

Future work

The experiment described above provides a foundation for further exploration and future work in the field of smart homes using IoT. Here are some potential areas for future development and improvement:

Enhanced Energy Monitoring: Expand the energy monitoring capabilities by integrating additional sensors, such as voltage sensors, power factor measurement, or energy meters. This would provide more comprehensive data for energy analysis and optimization.

Advanced Automation: Implement advanced automation features based on the energy consumption data. For example, create rules and algorithms to automatically adjust device settings or schedule power usage based on energy efficiency goals or time-of-use pricing.

Integration with Smart Grid: Explore integration with the smart grid infrastructure to take advantage of demand response programs and grid management initiatives. This would allow for bidirectional communication and coordination with the utility grid, enabling load shifting and optimizing energy usage based on grid conditions.

Integration with Voice Assistants: Incorporate voice assistant technologies, such as Amazon Alexa or Google Assistant, to enable voice control and interaction with the smart home system. This would enhance user convenience and hands-free operation.

Data Analytics and Visualization: Develop advanced data analytics and visualization tools to provide more detailed insights into energy consumption patterns, trends, and recommendations for energy efficiency improvements. This could involve techniques like machine learning algorithms or predictive analytics.

Security and Privacy Enhancements: Strengthen the security and privacy measures of the smart home system by implementing encryption, secure authentication, and access controls. Regularly updating firmware and ensuring secure communication protocols will help protect user data and prevent unauthorized access.

Integration with Renewable Energy Sources: Explore integration with renewable energy sources, such as solar panels or wind turbines. This would involve monitoring the energy generation from these sources and optimizing the usage of renewable energy within the smart home system.

User-Friendly Interfaces: Focus on developing user-friendly interfaces, such as mobile apps or web dashboards, to allow users to easily monitor and control their smart home systems. Intuitive interfaces and personalized settings can enhance the user experience.

Interoperability with Other Devices and Platforms: Ensure interoperability with other IoT devices and platforms by adopting industry standards and protocols. This would enable seamless integration of various smart home devices and systems.

Environmental Monitoring and Sustainability: Extend the smart home system to incorporate environmental monitoring sensors, such as air quality sensors or humidity sensors. This would enable users to maintain a healthy and sustainable living environment.

These are just a few examples of potential areas for future work in smart homes using IoT. As technology advances and new innovations emerge, there will be even more possibilities to explore in creating intelligent and efficient homes.

REFERENCES

[1] https://www.researchgate.net/publication/371607691_SMART_HOME_AUTOMATION_SYSTEM_BASED_ON_IoT

[2] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.
Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

[3] Li, S., Da Xu, L., & Zhao, S. (2015). The Internet of Things: A survey of enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[4] https://www.researchgate.net/publication/344234112_A_Smart_Home_System_based_on_Internet_of_Things/link/5f5efab7a6fdcc116410a061/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

[5] Lee, S., & Lee, J. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.

[6] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[7] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. IEEE Internet of Things Journal, 1(1), 22-32.

[8] Chui, M., Löffler, M., & Roberts, R. (2010). The Internet of Things. McKinsey Quarterly, 9(7), 1-9.

[9] Antonopoulos, A., & Gillam, L. (2017). Building the Internet of Things: Implement new business models, disrupt competitors, and transform your industry. Wiley.

[10] Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(5), 164-173.

[11] Noura, M., Atiquzzaman, M., & Gaedke, M. (Eds.). (2018). Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Springer.