IoT–enabled Home Automation System

Amanpreet Kaur
"AIT-CSE
Chandigarh University
Punjab, India"
amanpreet.e15096@cumail.com

Sehajpreet Kaur
"AIT-CSE
Chandigarh University
Punjab, India"
sakaur1509@gmail.com

Baby Monal
"AIT-CSE
Chandigarh University
Punjab, India"
babymonal2019@gmail.com

***Abstract*— Smart home automation system popularity has surged due to the widespread inculcation of technological advancement. With the integration of many technologies, including sensors and actuators, smart homes provide improved convenience, security, and energy efficiency. This research study compares and contrasts Proteus and Workwi, two well-known home automation technologies. Through an analysis of their component parts and integration procedures, we provide a thorough grasp of the benefits and drawbacks of each strategy. The IOT is used by both systems to enable easy and effective home control. The paper also looks at possible directions for future research to advance this quickly developing subject by improving the functionality and accessibility of smart home automation. [2]**

Keywords—Webhook, Proteus, Bot, MQ2, Blynk Cloud, Workwi, Sensors, integration, IOT.

I. INTRODUCTION

A. Background of Iot based Home Automation

Over the past few decades, the idea of "smart homes" has undergone tremendous change. At first, smart home automation was restricted to simple functions like lighting and appliance management. But as technology has advanced, especially with regard to the IOT, smart homes systems have grown to a larger extent with various complex and networked approaches.

Early Developments: In the 1950s, the United States saw the development of its first automated homes, which had simple controls for lights and appliances.[4] The idea of "intelligent homes" began to take shape, focusing on how different technologies could be combined to make a home that was more automated and responsive. More complex home automation systems were created as a result of developments in computer and microelectronics technology. [5]

Future prospects for smart home automation appear bright, as consumer adoption and technological improvements continue.

B. Objectives and Scope

The objectives of the research solely focus on the below endpoints:

1. To look at the condition of smart home automation technology at the moment.
2. To evaluate the advantages and challenges of putting smart home systems into place.
3. To compare and contrast the potential and operational efficiency of two distinct home automation systems.
4. To recognize new developments and potential paths in the automation of smart homes.

The study's scope includes the technological underpinnings of smart home systems, such as sensors, actuators, Internet of Things (IoT), and control systems.[4] The study also looks into the various use cases and applications of smart homes, including user experience, security, and energy management.

In addition, the study addresses the ethical ramifications of data privacy, security, and monitoring while assessing how smart home technology affects device accessibility.

Lastly, the study examines new trends and prospective advancements in the industry to provide light on how smart home automation may develop in the future.

II. LITERATURE REVIEW

A. Historical Development and Innovations in the field

R. Sarmah et. al presented SURE-H system which is safe and effective smart home solution that lets homeowners conserve energy and guard against burglary and strange activity. When the system is deployed, it looks for moving things in the surrounding area using a motion detector. Sensors configured are attached with ESP8266- 12E module to automate devices using BLYNK MOBILE APP. [1]

K. M. Kumar et. al. proposed two models in their work by utilizing the Raspberry Pi and NodeMCU respectively. The Blynk software program, available for Android devices, controls the household appliances. NodeMCU is used to implement the Manual and Auto modes of operation, while Raspberry Pi is used to control AC and DC appliances.[2]

R. Sivapriyan et. al. provides proficient knowledge regarding the data risks and difficulties along with IoT-based homes. The principles and challenges in IoT-based environment are highlighted by taking into account the appropriate measures to construct a secure management system, managing to distinct partitions along with discussing

countermeasures to dangers and threats in real-world scenarios.[3]

H. K. Singh et. al. showcased a web application which uses Node.js server to remotely operate electric switches using NodeMCU (ESP8266) microcontroller and relays. The system uses Node.js for runtime environment based on JavaScript, Express.js for web app framework and MONGO DB for storing the important data. The log file generated as a end result is used to track the user behavior.[4]

H. Durani et. al explored the connection of several household appliances, including lights, fans, water pumps, and gardening systems, with NodeMCU (ESP8266). Users can use an Android app to control these appliances by employing coding and hosting the application online. With the help of this app, wireless circuit device tracking and management are made possible when the NodeMCU is linked to the internet. The article shows how to create an Android app and manage an IoT application using Blynk as the platform.[5]

Tate K et. al. presented novel smartphone-based Home Automation System with low-cost wireless communication through internet. The main goal of the system used is to access home appliances and status of home by using android phone. The uniqueness of the paper is the use of SSR and ULN 2003 driver. Software design consist of embedded programming and Android Application Development MIT App Inventor2. Through this paper they have tried to reduce the challenges of real time operations and remote operation of devices.[6]

Bharat B et. al. proposed a system design to monitor devices via mobile phone using Wi-Fi as networking protocol and raspberry pi as server. The novelty of the paper is that the setup is invented in such manner that even if the user goes offline the system will transit to automatic position thus managing the devices according to the sensors values. For designing they have used microprocessor Raspberry pi, MCU(ESP-8266), Sensor units and GPS module. This prototype is useful for in-time home security and controlling of remote projects.[7]

D. Pavithra et. al. has made a home automation for security purpose using Raspberry pi and IR, PIR sensor which will detect the movement of people. Also, web interface is made to control these devices and sensor. Alert system is arranged in such a way that if any fire erupts in the house, then the image is directly gone in the phone of owner thus helping in making decision quickly. The proposed architecture is appropriate for home protection monitoring and for controlling the home appliances and protection from inflammable disasters with instant possible solutions.[8]

Khusvinder Gill et. al. through their paper showed the usage of ZigBee in solving the problem of slow adoption of home automation. They have demonstrated the system through 4 devices, radiator valve, a light switch, ZigBee remote control and safety sensor.

This paper discussed the complexity of the architectures accepted by preexisting systems, and requirements of the device installations, the deficiency of interoperability in between various home automation systems, developed by various manufacturers that use the said technology.[9]

Jinn-Kwei Guo et. al. in this paper they have described the usage of the embedded volume controller, “SUNPLUS SPCE061A, combined with Microchip 2 .4GHz Z i g B e e m o d u l e s”, i n H o m e Automation. The voice-controller includes a ZigBee module that plays the part of an interactive end user interface. It was both feasible and user interactive for home automation.[10]

III. SECURITY CHALLENGES AND CONCERNS

1. Denial of Service Attacks: This attack can disable IoT device by flooding the system with excessive traffic or exploiting vulnerabilities through malformed packets. This could result in the disruption of communication between the user and the device. For instance, an attacker might target the system's smart camera, causing it to go offline and allowing unauthorized physical access to the home without leaving digital evidence. Mitigation: To counter this, we have implemented rate-limiting mechanisms on the webhook service (via Make). This prevents the system from being overwhelmed by traffic, ensuring that even during a DoS attack, the system remains operational and responsive.[8]

2. Unauthorized Access: One of the most common security concerns in smart home systems is unauthorized access due to weak or easily guessable passwords, such as "1234" or using personal details like birthdays. Without multi-factor authentication (MFA), such systems are vulnerable to unauthorized entry and manipulation by cybercriminals. Our system addresses this by incorporating strong authentication measures and multi-factor authentication for critical components, particularly in the communication with the Telegram bot and make webhook service. This ensures that only authoritative individuals can control the device and receive notifications, significantly reducing the risk of unauthorized access.[6]

3. Secure Communication with Telegram: For real-time notifications, such as fire or gas alerts, our system relies on Telegram. Telegram is known for its high-level system safeguarding features, including integrated end level encryption for Secret Communications and two- factor authentication (2FA) for user accounts. Mitigation: By using Telegram's secure infrastructure, our system ensures that critical notifications are protected from interception and unauthorized access. This offers a reliable and secure communication platform, ensuring that users are promptly and securely informed in case of emergency situations.

4. Access Control: When it comes to potential vulnerabilities related to limited access control information, reliance on single-factor authentication, and device security, Workwi and Blynk Cloud's access control offer functionality for IoT development. It is advised to look into Workwi's access control capabilities, turn on 2FA on Blynk Cloud as our system using the blynk device user id and user name for authentication which in return establish granular access controls for the integration with the Workwi integration. Make sure that users are educated with secure passwords, keep an eye on user behavior, and implement

granular access controls. [3] [1]

5. Cyberattacks: Cyberattacks can target Internet of Things devices that are connected using protocols like MQTT. Strong security mechanisms including encryption, authentication, authorization, data validation, secure firmware updates, network segmentation, monitoring, logging, and adhering to security best practices must be put in place in order to reduce these threats. Organizations may safeguard their Internet of Things systems and considerably lower the probability of successful assaults by implementing these tactics. [3] [1]

IV. SYSTEM ARCHITECTURE AND DESIGN

Proteus Based Integration

A. Components used in the experimental setup

1. Raspberry pi: Acts as the central processing unit for your home automation system. It runs the control scripts and communicates with all connected sensors and devices (e.g., lights, fans, etc.) via GPIO pins and potentially over MQTT for remote control.[6]

2. LCD: Used for displaying information such as sensor readings, status messages, or alerts. It provides a user interface for monitoring and interacting with the home automation system in real-time.

3. MQ2 sensor: It is a gas sensor that detects various emissions such as LPG and smoke which helps in monitoring air quality and can trigger alerts or safety measures (e.g., turning on a buzzer or shutting off gas appliances) when harmful gas levels are detected.[6][8]

4. Bulb: Serves as a controllable light source within your home automation system. It can be turned on or off based on sensor inputs (e.g., motion detected by the PIR sensor) or remotely via the MQTT app.

5. PIR sensor: Detects motion by sensing changes in infrared radiation, typically emitted by human bodies. This sensor is crucial for automating actions, such as turning on lights (bulb) when someone enters a room or turning them off after a period of inactivity.[7]

6. Light Intensity Control: This feature involves controlling the brightness of lights based on ambient light levels (detected by an LDR, for instance). It helps save energy by adjusting lighting according to the available natural light.

7. Temperature Sensor: Monitors the ambient temperature in the environment. It can be used to automate a fan or other cooling systems based on temperature thresholds, ensuring a comfortable indoor climate.[9]

8. Fan circuit: Controls the operation of a fan based on temperature readings. It can be turned on or off automatically depending on the temperature sensor's input, helping to maintain a comfortable temperature in the space.

9. ADC Module: Converts analog signals from sensors (like the MQ2 and temperature sensors) into digital signals that the Raspberry Pi can process. This is crucial for reading data from analog sensors, as the Raspberry Pi operates with digital signals.

10. Buzzer: An output device that produces sound alerts. It can be triggered by various events, such as gas detection by the MQ2 sensor or motion detected by the PIR sensor, to notify users of potential hazards or actions that need attention.[10][6]

B. Software Used

1. Proteus: Proteus supports a wide range of components, including microcontrollers, sensors, and communication modules, making it an ideal tool for prototyping and testing embedded systems before physical implementation.

Its user-friendly interface and real-time simulation capabilities enable users to visualize and troubleshoot their designs effectively.

2. Telegram Bot: API to communicate with the Telegram server, allowing developers to create custom functionality tailored to specific needs.

Telegram Bots are popular in-home automation projects, as they can enable remote control of devices, send alerts, and provide real-time updates through messaging.

C. Integration Process:

The home automation system in Proteus operates through a series of integrated sensors and actuators to enhance safety and convenience within a living environment.

The process begins with the PIR sensor, which detects motion; when a person is detected, it outputs a value, and the LCD displays "Person Detected" to indicate presence.

If no motion is detected, the LCD shows "Person Not Detected." Upon detection of a person, the system automatically turns on the bulb, allowing users to adjust the light intensity to their preference.

Furthermore, the system incorporates a temperature sensor that activates the fan when the ambient temperature exceeds a predefined threshold, promoting comfort and safety.

The MQ2 gas sensor plays a critical role in monitoring for hazardous gases. If it registers a value of 1, indicating a potential fire, the system promptly sends an alert message to the Telegram bot, notifying users of the situation.

This integrated approach not only enhances the overall functionality of the home automation system but also ensures real-time responses to changing environmental conditions, thereby improving safety and user experience.

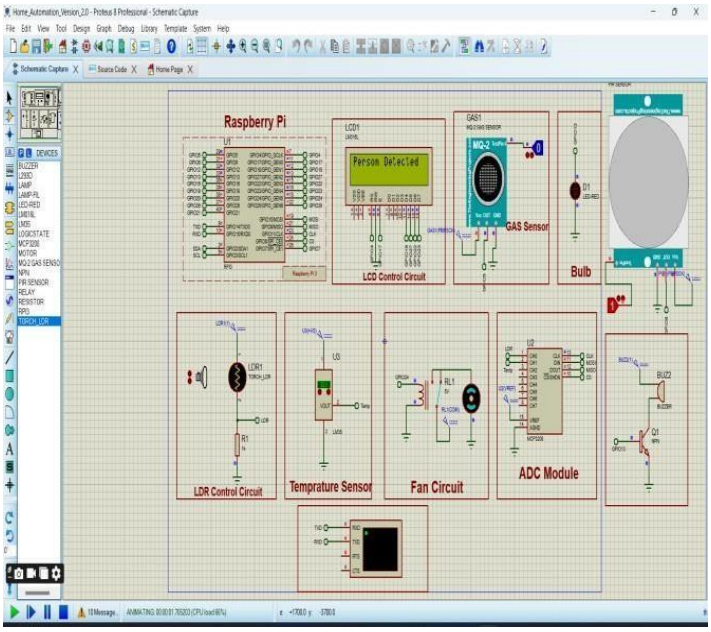
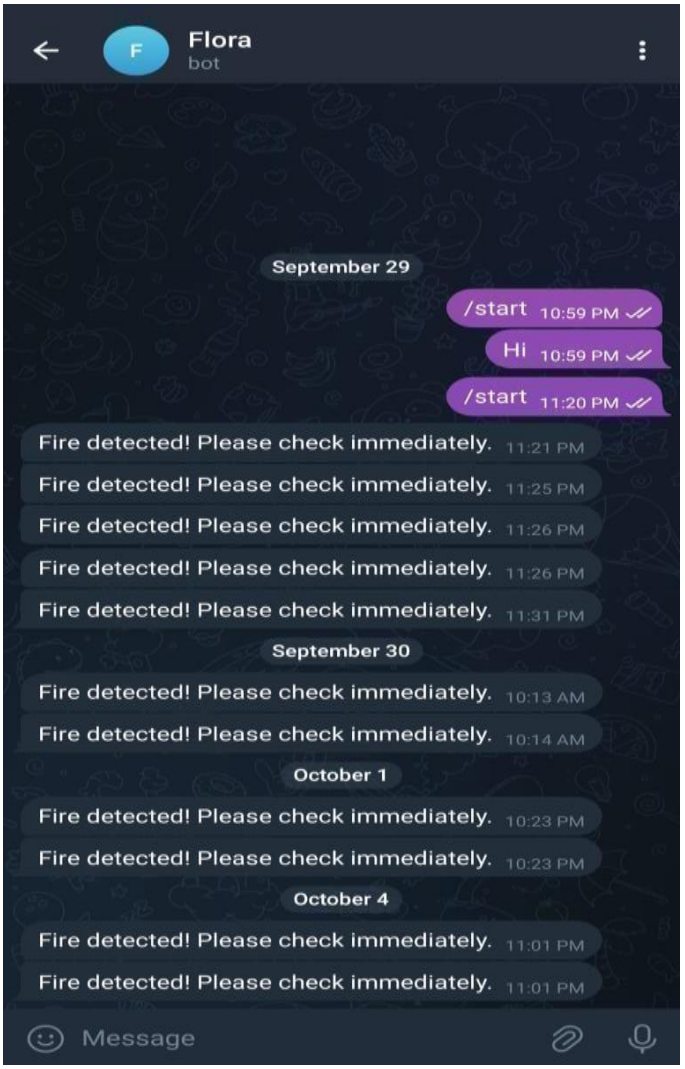


Fig1.1: Home automation connections on Proteus

Fig: Fire alert message on Telegram Bot



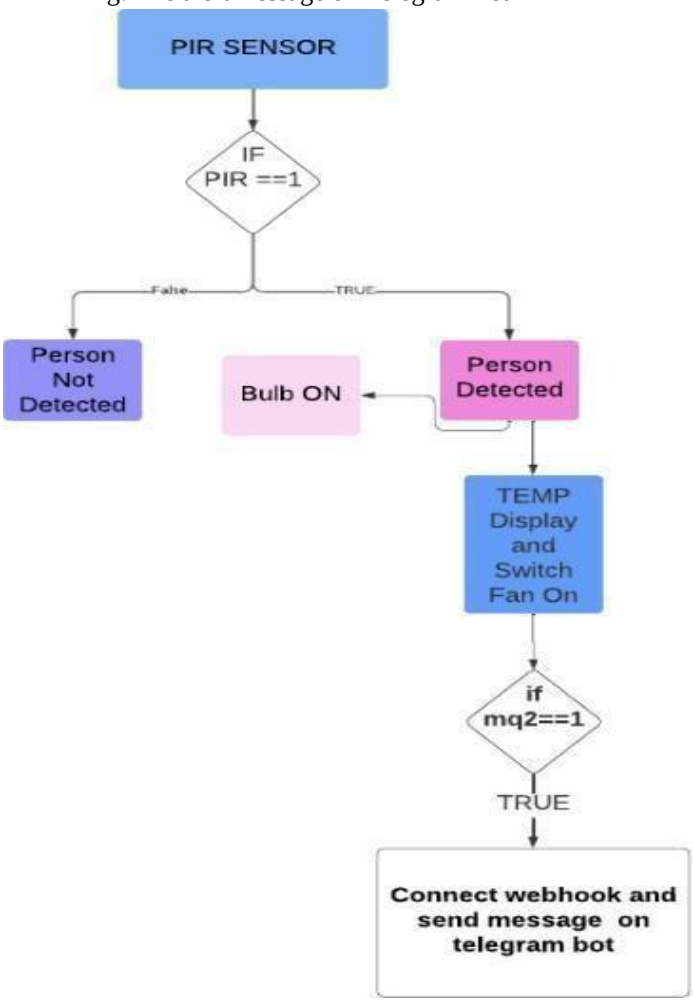


Fig 1.2: Home Automation Flowchart

Fig 1.3 Telegram Bot

ii) Blynk Cloud Based Integration

A. <u>Components used in experimental setup</u>

1. Blynk Device: A piece of hardware, like an Arduino or ESP32, that is linked to the Blynk platform and may be managed and observed via the Blynk app or cloud.[2]

2. Relay: It is an electric on/off device that uses minimal amount of voltage levels to automate high-voltage circuits; frequently used in Internet of Things applications to remotely turn appliances on and off.[4] [1]

3. LED: A light-emitting diode that is frequently used to indicate outputs or status in a variety of applications.

4. Pushbutton: It is a basic switch mechanism that, when pressed, makes or breaks a connection in electronic circuits to allow for user input.

5. PIR Motion Sensor: A sensor used in automation projects or security systems to detect the presence of items; it picks up infrared light emitted by moving objects.

6. ESP32: A microcontroller with Bluetooth and Wi-Fi capabilities that is frequently used in Internet of Things projects for sensor and device control and wireless communication. [1]

7. DHT22: A sensor for humidity and temperature measurements. Projects involving weather monitoring or home automation frequently use it.[2]

8. MQ2 Gas Sensor: Typically found in safety and environmental monitoring systems, this sensor senses the presence of gases such as smoke, propane, and methane.[4]

B. Software Used:

1. Blynk cloud: A cloud-based platform that makes it possible to connect, monitor, and control Internet of Things devices. It provides dashboards, widgets, and APIs for remote interaction with smart devices.[4] [5]

2. Wokwi Interface: A virtual platform for microcontrollers and Internet of Things applications. In a virtual environment, it enables users to create, develop, and test circuits utilizing parts like Arduino, ESP32, sensors, and actuators. It is frequently used to learn and prototype without requiring physical hardware.

C. Integration Process

1. Start a Wokwi project: Visit Wokwi.com to register or sign in. After selecting the microcontroller (such as the ESP32), click "New Project". Via the component's search box, add devices (such as sensors, relays, and LEDs) by utilizing the library. As shown in the circuit schematic, connect the parts (drag and drop to wire them). Make sure the connections for the ESP32 adhere to the proper pinouts.

2. Configure Cloud Blynk: Visit Blynk cloud, sign in, or register for the new account for creating the setup. In the Blynk cloud, create a new Template and set up the required DataStream (virtual buttons, LEDs, and sensor readings). Take a copy of Blynk's Device Name, Authentication Token, and Template ID. You'll need them to use your ESP32 code. [5]

3. Wokwi editor: To write or upload code, use the code editor tab in Wokwi web interface by accessing the Wokwi.com. In order to integrate an ESP32, use the Blynk library. Install the required libraries. To handle the input and output from your buttons, relays, and sensors, write more code.

4. Use Wokwi to Connect and Simulate Make that the code has the necessary Wi-Fi credentials set. If all of your parts are linked correctly and the code is accurate, the virtual microcontroller will be able to interface with the Blynk cloud when you simulate the project on Wokwi.

5. Use Blynk for Monitoring and Control Add buttons, screens, or graphs to the Blynk app that match the virtual pins you've set up. Now, you can use the Blynk app or dashboard to keep an eye on sensors (such the temperature from DHT22) and operate devices (like relays).

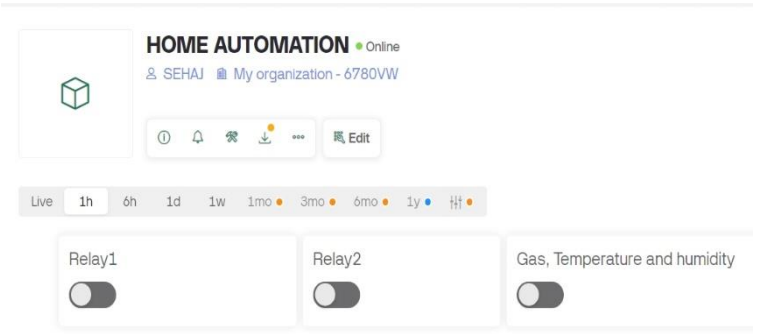


Fig 1.4 Home Interface on Blynk Cloud

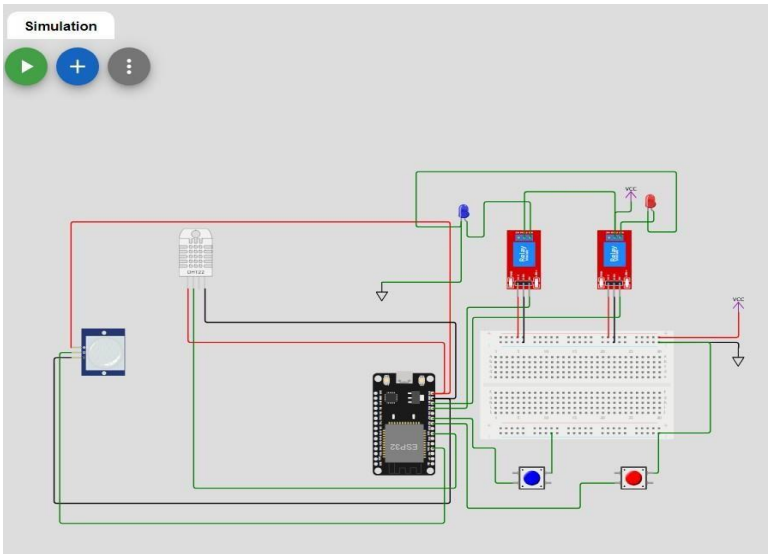


Fig 1.5 Blynk Cloud Interface

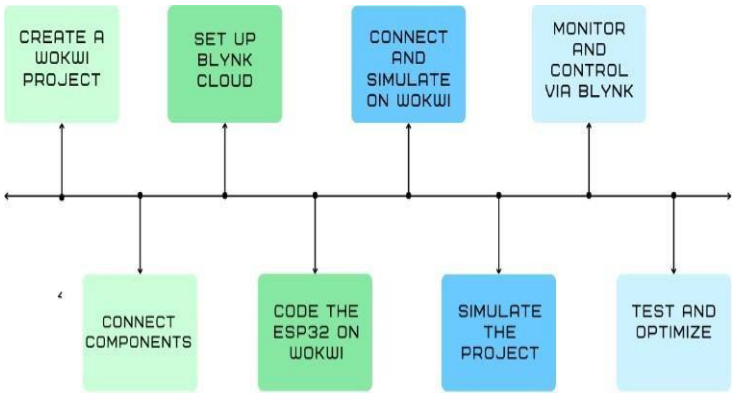


Fig 1.6: Flowchart of the Integration process

V. Results

A. Proteus based Integration

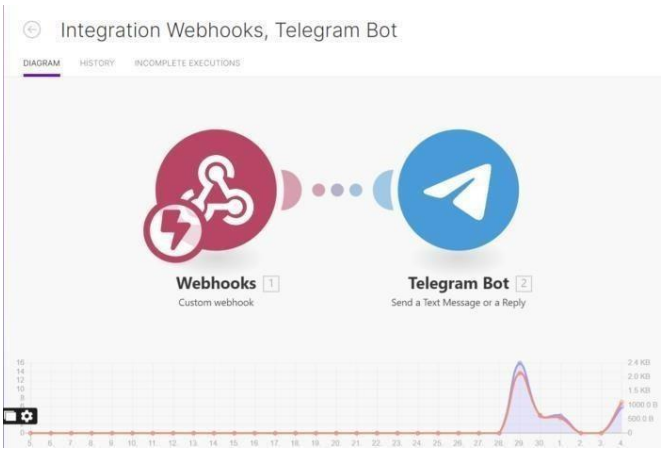


Fig 1.7 Integration Webhook and Telegram Bot

B. Blynk Cloud Integration

```
[1407] Connecting to Wokwi-GUEST
[8770] Connected to WiFi
[8770] IP: 10.10.0.2
[8771]
    ___  __             __
   / _ )/ /_ _____  __ / /__
  / _  / / // / _ \/  '_/
 /____/_/\_, /_//_/_/\_\
        /___/ v1.3.2 on ESP32

 #StandWithUkraine    https://bit.ly/swua

[8782] Connecting to blynk.cloud:80
[9684] Redirecting to blr1.blynk.cloud:80
[9688] Connecting to blr1.blynk.cloud:80
[11415] Ready (ping: 128ms).
Temp: 24.00 °C
Humi: 40.00 %
Gas Value: 0
```

Fig 1.8 Connecting to the Blynk Cloud on Wokwi

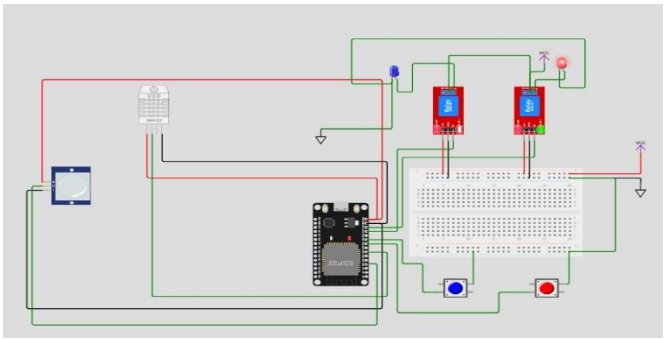


Fig 1.9 Wokwi Running Simulation

VI. Research Concentrations

1. Decentralized Energy Markets and Blockchain Integration: This field looks into how homeowners might sell extra energy from solar panels or battery storage by actively participating in decentralized energy markets through their smart homes. The development of safe blockchain energy trading platforms, AI-powered energy management systems, and the integration of renewable energy sources with home automation are the main areas of research.

2. Interfaces between Virtual Reality and Augmented Reality: AR is used to make visual dashboards that can be accessed via AR glasses or smartphones to monitor smart home equipment. With virtual reality (VR), homeowners may remotely control their smart home's lighting, security, and climate. Enhancing user interfaces, developing user-friendly control systems, and investigating novel AR/VR applications in smart home management are the goals of research.

3. AI-Driven Predictive Maintenance for Smart Home Appliances: This field investigates the use of machine learning to forecast potential failure times of smart home appliances (such as air conditioners and refrigerators). Through the examination of consumption trends and sensor data, researchers hope to identify any problems before homeowners do, cutting downtime and maintenance expenses while facilitating automated maintenance job scheduling.

4. IoT Smart Home Networks: The aim of this research is to promote user data integrity and privacy in networks of linked smart homes. It looks into machine learning for threat detection, decentralized authentication, and sophisticated encryption techniques. The objective is to develop frameworks that provide homeowners the ability to manage data sharing while guaranteeing strong defense against online attacks. [2]

VII. CONCLUSION AND FUTURE SCOPE

The integration of IoT technology, such as microcontrollers, sensors, and mobile applications, has the potential to improve home security and energy efficiency, as demonstrated by the IoT-enabled smart home system project. [5]

By employing simulation platforms such as Wokwi.com and seamless remote-control platforms like Blynk Cloud, the system facilitates real-time monitoring and automation of household appliances, thereby enhancing user convenience and encouraging energy conservation. [4]

Also, the system's dependability in automating home tasks and offering improved security measures is highlighted by the Proteus simulation's success and robust MQTT connection. [5]

Future advancements might include enhanced user interface designs, machine learning for energy management optimization, and sophisticated security features. [5] [1]

The system's capabilities will also be further improved by increasing its scalability, combining it with well-known smart assistants, ensuring it meets the evolving needs of users in the smart home landscape.[4]

References

[1] R. Sarmah, M. Bhuyan and M. H. Bhuyan, "SURE-H: A Secure IoT Enabled Smart Home System," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 59-63, doi: 10.1109/WF- IoT.2019.8767229.

[2] K. M. Kumar and S. Chaudhury, "Development of a Smart Home Automation System using IoT enabled Devices," 2022 IEEE 19th India Council International Conference (INDICON), Kochi, India, 2022, pp. 1-5, doi: 10.1109/INDICON56171.2022.10040165.

[3] R. Sivapriyan, S. V. Sushmitha, K. Pooja and N. Sakshi, "Analysis of Security Challenges and Issues in IoT Enabled Smart Homes," 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2021,

pp. 1-6, doi: 10.1109/CSITSS54238.2021.9683324.

[4] H. K. Singh, S. Verma, S. Pal and K. Pandey, "A step towards Home Automation using IOT," 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-5, doi: 10.1109/IC3.2019.8844945.

[5] H. Durani, M. Sheth, M. Vaghasia and S. Kotech, "Smart Automated Home Application using IoT with Blynk App," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 393-397, doi: 10.1109/ICICCT.2018.8473224.

[6] Tate K, Pawar M. HOME AUTOMATION WITH ANDROID UNDER IOT CONCEPT. IJIERT - International Journal of Innovations in Engineering Research and Technology. 2016 February 20.

[7] Bohara B, Maharjan S, Shrestha BR. IoT Based Smart Home using Blynk Framework.

[8] D. Pavithra and R. Balakrishnan, "IoT based monitoring and control system for home automation," 2015 Global Conference on Communication Technologies GCCT), Thuckalay, India, 2015, pp. 169-173, doi: 10.1109/GCCT.2015.7342646.

[9] K. Gill, S. -H. Yang, F. Yao and X. Lu, "A ZigBee-based home automation system," in IEEE Transactions on Consumer Electronics, vol. 55, no. 2, pp. 422-430, May 2009, doi: 10.1109/TCE.2009.5174403.

[10] J. -K. Guo et al., "Interactive Voice-Controller Applied to Home Automation," 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kyoto, Japan, 2009, pp. 828-831, doi: 10.1109/IIH-MSP.2009.320.