Multi-Sensory Monitoring & Control using ESP8266 and Blynk

Parmod Kumar

Parmodsaini027@gmail.com

M. Tech Scholar, Department of Electrical & Electronics Engineering, BRCM CET, Bahal, (Haryana), India

Mr. Sandeep Kumar

sjakhar1989@gmail.com

Assistant Professor, Department of Electrical & Electronics Engineering, BRCM CET, Bahal, (Haryana), India

Dr. Vivek Kumar

hodeee@brcm.edu.in

Professor & Head, Department of Electrical & Electronics Engineering, BRCM CET, Bahal, (Haryana), India

ABSTRACT

In this work a multi-sensor based IoT enabled system has been implemented in order to enable the user for monitoring and control of proposed system based on certain inputs. The system has been implemented around the NodeMCU IoT enabled development board with on chip Wi-Fi chipset by Espressif. The hardware set-up along with the web-server dashboard will collectively fulfil the purpose. This is an experimental work and the developed prototype has validated the research work reported here in this dissertation work. Solution has been provided for each problem statement that has been discussed and the research has been carried out in a phased manner.

Keywords: IoT, Web server, NodeMCU, Home Automation

INTRODUCTION

NodeMCU is a reduced open-source IoT platform. It is open-source firmware with accessible prototyping board designs. The phrase "NodeMCU" is an abbreviation again for the terms "node" and "microcontroller" (micro-controller unit). It is built by the ESP8266 Wi-Fi SoC from Express if Systems (System on Chip). The firmware as well as the experimental board designs are free to the source. The ESP-12F Wi-Fi device has an ESP8266 core processor in smaller module sizes. Tensilica L106 has an industry-leading 32-bit MCU micro with a 16-bit short form, clock frequencies of 80 MHz and 160 MHz, RTOS compatibility, as well as and an embedded Wi-Fi on-board antenna. The module complies the with IEEE802.11 b/g/n standard and the whole TCP/IP protocol stack. It provides unequalled versatility in incorporating Wi-Fi abilities into other systems or serving as a stand-alone application at the lowest possible cost and with the least amount of room necessary. The ESP8266EX provides a complete and ego Wi-Fi network of social; it may host the program or offload Wi-Fi networking activities from some other application processor. A brief description of the complete development cycle of this IoT-based system was provided here. First of all, a briefing was done about the designing of schematic using a CAD tool by giving due consideration to the objectives of our work; then the PCB layout designing for hardware prototyping was demonstrated and discussed; then the bill-of-material required to assemble the hardware was given. Also, the algorithm design and firmware components used to drive this system were discussed here. In this work, the methodology was adopted to design and validate the schematic first and then the layout was designed as per the schematic. Finally, we used the PCB layout design to fabricate the PCB. Afterward, the hole drilling process was carried out followed by the component placement and soldering process. Finally, we obtained the hardware prototype for the proposed system in the form of a self-designed PCB card.

EXPERIMENTAL SET-UP

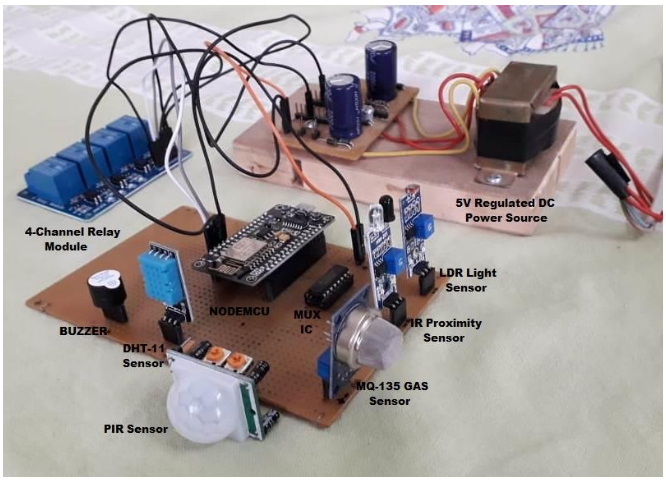

Figure-1: Experimental Set-up

The firmware was edited and compiled in the Arduino IDE (Integrated Development Environment). The very first step before starting writing the code is to write an algorithm. So, we referred the algorithm at each and every step of firmware writing to minimize the possibility of error and minimize the time by writing an efficient source code for the system. There are certain key features of the firmware I found worth describing those below here.As an initial and necessary step the appropriate libraries were included at the beginning of firmware. The libraries used here were as shown here.

```
#define BLYNK_PRINT Serial
#include <ESP8266WiFi.h>
#include <BlynkSimpleEsp8266.h>
#include <DHT.h>
```

Then suitable names were assigned to the NodeMCU analog as well as digital pins with the help of #define function. The names were assigned to the pins just for the ease of user's understanding about each pin's functionality; otherwise, it could be difficult to remember each pin function by its pin number. The pin definitions as shown below were made as per the designed schematic diagram and printed circuit board (PCB).

```
/******** Pin Definition ************/

//Relays for switching appliances
#define Relay1            D6
#define Relay2            D2
#define Relay3            D1
#define Relay4            D5

//DHT11 for reading temperature and
//humidity value
#define DHTPIN            D7

//buzzer to use it for alert
#define buzzer            D0

//Selection pins for multiplexer module
//to switch between different sensors
//and give data on a single analog pin
#define S0                D3
#define S1                D4

//Analog pin to read the incoming analog
//value from different sensors
#define analogpin         A0
```

Then the source code was to demand from the user to enter an Authorized Unique Token ID provided by the Blynk App server. This token ID can be accessed by an authorized user only through a registered e-mail address. So, this step was considered very important here, as, to establish the communication between the NodeMCU and the Blynk this token id must be entered in the firmware as shown below.

```
// You should get Auth Token in the Blynk App.
// Go to the Project Settings (nut icon).
char auth[] = "XvnyBAxdH-Dp22GpHH53SOQv88DdjaV2";
```

Next important step was to enter the user's Wi-Fi Credentials like mobile's hotspot ssid and password to which the system needs to establish connection with.

```
// Your WiFi credentials.
// Set password to "" for open networks.
char ssid[] = "Redmi";
char pass[] = "abcd#1234";
```

For the Blynk here in this code some virtual variables (V0, V3, etc.) were assigned enabling it to communicate with different sensors and devices as shown below.

```
Blynk.virtualWrite(V0, t);
Blynk.virtualWrite(V1, h);
Blynk.virtualWrite(V2, proximity);
Blynk.virtualWrite(V3, gas);
Blynk.virtualWrite(V4, motion);
Blynk.virtualWrite(V5, light);
```

As per the 16:1 multiplexer's select line status of S0 and S1, each of the connected analog output sensor got NodeMCU's service. The other two status lines of the multiplexer i.e. S2 and S3 were grounded as we were demonstrating the system application with just four analog output sensors. The source code was as shown below.

```
// Address 00
digitalWrite(S0, LOW);
digitalWrite(S1, LOW);
gas = analogRead(analogpin);
Serial.print("Gas - "); Serial.println(gas);


// Address 11
 digitalWrite(S0, HIGH);
 digitalWrite(S1, HIGH);
 int raw_light = analogRead(analogpin);
 light = map(raw_light, 1024, 0, 0, 100);
 Serial.print("Light - "); Serial.println(light);

 Blynk.run();
 timer.run();

// Address 10
 digitalWrite(S0, HIGH);
 digitalWrite(S1, LOW);
 motion = analogRead(analogpin);
 if (motion > 512)
 {
   motion = 1;

 }
 else
 {
   motion = 0;

 }

// Address 01
 digitalWrite(S0, LOW);
 digitalWrite(S1, HIGH);
 proximity = analogRead(analogpin);
 Serial.print("Proximity - "); Serial.println(proximity);
 if (proximity < 512)
 {
   proximity = 1;
   digitalWrite(buzzer, HIGH);
 }
 else
 {
   proximity = 0;
   digitalWrite(buzzer, LOW);
 }
```

RESULTS & DISCUSSION

The firmware was edited, compiled and tested on Arduino IDE and multiple libraries were included to make the system run. The output response of the system was checked on serial monitor at each stage. To establish communication between the user and the developed IoT system various credentials were required from the user to be included at the firmware level only. The system access was limited to the Wi-Fi hotspot based local area network only. Multiple iterations were carried out to debug the firmware to get the desired results. The results obtained from the final prototype board were observed on a mobile application known as Blynk. Blynk was downloaded and installed into the user's handset and an account was created there by entering the required user credentials. The user was assigned an authorization token ID over the e-mail which was entered in the firmware itself before uploading it to the NodeMCU. A new project was created in the graphical-user-interface window of the Blynk App by selecting some widgets from its wide library and configured those widgets as per the system hardware and firmware. All the sensors and the relay board along with the NodeMCU were connected and powered p. The NodeMCU based hardware and the Blynk over the mobile handset got connected with the help of Wi-Fi. The individual system outputs from each sensor were successfully monitored on the Blynk project screen and that too in real-time. Also, the relays were triggered remotely by using this platform. Hence the work was tested and validated. The hardware set-up was initially assembled over a breadboard only and with the help of jumper wires all the sensors and the four-channel relay module were interfaced to the NodeMCU board and the power source. Initially the NodeMCU interfacing with each sensor was carried out individually and then at a later stage all the sensors were integrated in a single system along with the controlling relays. The firmware was uploaded to the NodeMCU and the system response was checked for the desired results. There was a power drop issue in the circuit and the reason was because of the significant amount of power drain by the system as all the sensors, relay and NodeMCU were connected at singe time and power demand increased. Hence, the power source rating was increased to meet the system demand. Multiple iterations were carried out to calibrate the system. By the end of successful completion of this work it was concluded that the IoT is a new scenario of wireless communication devices. IoT is the development of existing internet facility to manage everything which exists in the world or exists in the future. Things having individualities and the simulated dispositions functioning in smart space using a smart interface to link and connect within the social environment and user context. The IoT also can be considered as global networks which give the communication between things to things, human to things and human to human. As per this work, surveillance is the procedure of close deliberate perception or supervision kept up over an individual, gathering, and so forth particularly one in care or under doubt. For the above-mentioned purposes now a day's devices are equipped with various sensors as per application requirements. Sensors are communicating with each other using various topologies in IoT. Data travels locally or remotely from or in by each sensor node. As per application and requirements, sensor nodes may be of same type or different type. For a smart home, it is essential to combine sensor network with internet and intelligent real life objects. Integration of these sensors, smart objects, devices and network is IoT. The final prototype board's results were viewed on a smartphone application called Blynk. Blynk was downloaded directly on the user's device, and an account was established by inputting the necessary user credentials. The user was granted an authentication token ID by e-mail, which was then inserted into the firmware before it was uploaded to the NodeMCU. In the Blynk App's graphical user interface window, a new project was formed by picking certain widgets from its extensive library and configuring those widgets by the system hardware and firmware. All of the sensors and relay board, as well as the NodeMCU, were carefully linked and powered by a DC power supply. The Wi-Fi hotspot network was used to connect the NodeMCU-based hardware and the Blynk over the mobile device. Individual sensor outputs may be easily checked on the Blynk project screen in real-time. This platform was also used to remotely activate the relays. A four-channel relay module was connected to the NodeMCU, which ran on 5V dc only. All four relay outputs were linked to the alternating current load, and LED lamps were utilized as a demonstration. Otherwise, any single-phase alternating current demand might be connected to the separate relay outputs. The user should keep in mind that the wireless communication network established here for the system was a local network only, and therefore system functionality was restricted to the bounds of the local Wi-Fi hotspot utilized by the user to establish system connectivity. Other protocols at the firmware level would be necessary to access this system from anywhere in the world. As a result, the work was tested and confirmed using the produced hardware as well as the Blynk App on a mobile phone. The hardware set-up was initially assembled over a breadboard only and with the help of jumper wires all the sensors and the four-channel relay module were interfaced to the NodeMCU board and the power source. Initially, the NodeMCU interfacing with each sensor was carried out individually, and then at a later stage, all the sensors were integrated into a single system along with the controlling relays. The firmware was uploaded to the NodeMCU and the system response was checked for the desired results. There was a power drop issue in the circuit and the reason was because of the significant amount of power drain by the system as all the sensors, relay, and NodeMCU were connected at a single time and power demand increased. Hence, the power source rating was increased to meet the system demand. Multiple iterations were carried out to calibrate the system. The firmware was edited, compiled, and tested on Arduino IDE and multiple libraries were included to make the system run. The output response of the system was checked on the serial monitor at each stage. To establish communication between the user and the developed IoT system various credentials were required from the user to be included at the firmware level only. The system access was limited to the Wi-Fi hotspot-based local area network only. Multiple iterations were carried out to debug the firmware to get the desired results. After we carried out testing on the system for all the desired parameters, a final prototype was designed and developed by assembling a printed circuit board (PCB).

CONCLUSION

As IoT is a vast field and researchers are still struggling hard to explore its potentials in multiple applications. Thus, IoT is still an emerging field and as new sensors and networks are evolving day by day so do the scope of its applications are widening with time. This work may be expanded to demonstrate more complex LAN and WAN communication protocols like LoRA, BLE, Zigbee, Z-waves, AWS cloud platforms, and so on. As IoT is the fastest emerging technology today and is widely accepted and is growing at a much faster pace worldwide. So, prospects for this kind of work are always open. Following effectively completing this project, it was found that the Internet of Things (IoT) constituted a new framework for wireless communication devices. The Internet of Things (IoT) is the development of current networks to handle anything that is or will be present in the future. Items with personas and simulated dispositions that operate in the smart home environment and use a connected device to connect and engage within a social environment and user context. By the end of successful completion of this work it was concluded that the IoT is a new scenario of wireless communication devices. IoT is the development of existing internet facility to manage everything which exists in the world or exists in the future. Things having individualities and the simulated dispositions functioning in smart space using a smart interface to link and connect within the social environment and user context. The IoT also can be considered as global networks which give the communication between things to things, human to things and human to human. As per this work, surveillance is the procedure of close deliberate perception or supervision kept up over an individual, gathering, and so forth particularly one in care or under doubt. For the above mentioned purposes now a day's devices are equipped with various sensors as per application requirements. Sensors are communicating with each other using various topologies in IoT. Data travels locally or remotely from or in by each sensor node. As per application and requirements, sensor nodes may be of same type or different type. For a smart home, it is essential to combine sensor network with internet and intelligent real life objects. Integration of these sensors, smart objects, devices and network is IoT.

REFERENCES

[1] Dilip Kumar Sharma; Neeraj Baghel; Siddhant Agarwal, “Multiple Degree Authentication in Sensible Homes based on IoT Device Vulnerability”, 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), IEEE.

[2] Satyendra K. Vishwakarma; Prashant Upadhyaya; Babita Kumari; Arun Kumar Mishra, “Smart Energy Efficient Home Automation System Using IoT”, 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE.

[3] Kabita Agarwal; Arun Agarwal; Gourav Misra, “Review and Performance Analysis on Wireless Smart Home and Home Automation using IoT”, 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC), IEEE.

[4] Tushar Chaurasia; Prashant Kumar Jain, “Enhanced Smart Home Automation System based on Internet of Things”, 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC), IEEE.

[5] Tui-Yi Yang; Chu-Sing Yang; Tien-Wen Sung, “A Dynamic Distributed Energy Management Algorithm of Home Sensor Network for Home Automation System”, 2016 Third International Conference on Computing Measurement Control and Sensor Network (CMCSN), IEEE.

[6] Whether heated A. Jabbar; Mohammed Hayyan Alsibai; Nur Syaira S. Amran; Samiah K. Mahanadi, “Design and Implementation of IoT-Based Automation System for Smart Home”, 2018 International Symposium on Networks, Computers, and Communications (ISNCC), IEEE.

[7] Shradha Somani; Parikshit Solunke; Shaunak Oke; Parth Medhi; P.P. Laturkar, “IoT Based Smart Security and Home Automation”, 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), IEEE.

[8] Puneet Kumar Aggarwal; P. S. Grover; Laxmi Ahuja, “A Performance Evaluation Model for Mobile Applications”, 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE.

[9] John Fox; Andrew Donnellan; Liam Doumen, “The deployment of an IoT network infrastructure, as a localized regional service”, 2019 IEEE 5th World Forum on Internet

of Things (WF-IoT), IEEE.

[10] Alok Kumar Gupta; Rahul Johari, "IOT based Electrical Device Surveillance and Control System", 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE.

[11] Fan Wu; Taiyang Wu; Mehmet Rasit Yuce, "Design and Implementation of a Wearable Sensor Network System for IoT-Connected Safety and Health Applications", 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), IEEE.

[12] Arvind Arya; Akash Taliyan; Pradeep Chauhan; Anju Gautam, "Smart Kitchen with New Measurement, Web and Application Based with Affordable Design", 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE.

[13] Sachin A. Goswami; Bhargav P. Padhya; Ketan D. Patel, "Internet of Things: Applications, Challenges, and Research Issues", 2019 (IoT in Social, Mobile, Analytics, and Cloud) (I-SMAC), IEEE.