An Innovative Approach for Secured Smart Office and Home System using IoT

An Innovative Approach for Secured Smart Office and Home System using IoT

Apurva Shashank [1], Rajiv Vincent [2*]

[1]School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India.

[2]School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India.

E-Mail:* rajiv.vincent@vit.ac.in

Abstract. As technology grows every day, everybody wants to use smart devices (phones, lights, appliances, etc.). Nowadays we find that many houses and offices are neither safe nor smart. To overcome this problem, we have proposed a smart and secure office and home system using IoT. The proposed system contains several components, where a single microcontroller will connect and control several components. Our system will sense the environment and will detect movement and also will distinguish whether a human has moved in or out of the sensors. Secondly, when light falls on its resistance decreases and as it senses darkness its resistance becomes high. Next, our system will sense the blockage level in the housing pipelines and give information about the exact blockage point. Finally, it will control the gardening system. This system will monitor and use all the data from the sensors and principally facilitate physically challenged persons to manage all of their home and office devices from one place, and simultaneously saves power as well.

Keywords: IoT, smart home, smartphone, actuators, Node MCU.

1. Introduction

Through proliferation and employment of the Internet, the interest in IoT empowered gadgets has expanded violently. Simultaneously, there are issues concerning theft or burglary anything from little houses to enormous businesses. Continuous checking of individuals' conduct and exercises are required for assuring safety. The alleged shrewd home utilizing the house as a stage interfaces with different gadgets identified with home life by adopting creativity in the powered system of communications, electrical computerization innovation, personal computer innovation, and remote innovation.

The smart home can further boost home security through aesthetics and eco-accommodating living conditions. Contrasting with existing frameworks, the Node MCU framework is better in achieving the goals with less power energy utilization. Here, Passive Infrared Sensor (PIR) sensors are used as basic but powerful proximity triggers for individuals. The system is appropriate for observing in a small home or office, bank storage space, stopping passage, what's more, home. A little movement

is recognized via the PIR sensor which is suited for Node MCU and data is also saved in the module. Specific software based on IoT can monitor remotely the motion and provide alerts while detecting movement.

The motivation behind this task is to bring out an IoT based sagacious smart device checker and checking is done by the respective mobile. In the smart home checker, the microprocessor and IoT connect to the files to the web. The mobile application in the cell phone associates to the web using Wi-Fi or by utilizing wired web connections from expert centers; likewise, the microcontroller is linked to the web through LAN or home Wi-Fi. Here the master sends the order to the slaves, in addition to which the microprocessor sets the particular device on open or close [1].

Figure 1 represents various kinds of smart appliances in a home. It shows that when the PIR sensor is working and find some interference in the environment, then it can alert the homeowner in different ways, like, ring the buzzer, switch on the light and send the notification to the owner. Figure 2 depicts the smart home controller of our proposed system.

Fig 1. Smart Home Autonomous System

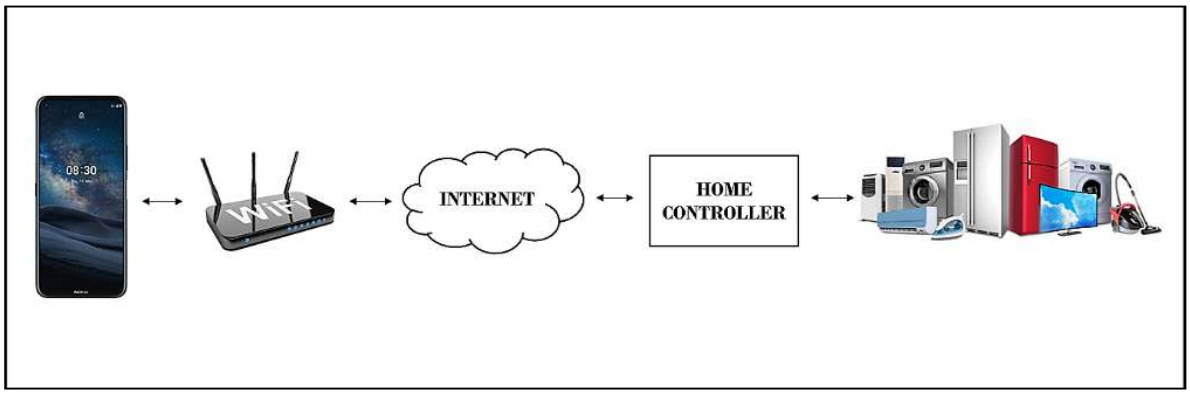

Fig 2. Smart Home Controller

2. Related work

The work by Madhu G M and C.Vyjayanthi [5] every device is connected to the internet through the IoT protocol and controlling is done through HTTP requests sent from the Android mobile application. The API (Application Programming Interface) connects the server and android application and allows it to interact and exchange data with the server. Whenever the user sends requests from the android application, the API connects to the server and it sends requests to the controller, further to which the controller performs ON/OFF function of the device based on the request received.

Another study based on research by Roshmi Sarmah, Manasjyoti Bhuyan, and Monowar H. Bhuyany [4] SURE-H framework is exhibited to guarantee the security of savvy home mechanization framework with numerous segments, for example, slaves, movement sensors, cloud master, mobile kind of stuff discovery module, and caution module. It is monitored from a distance-dependent on slave verification. The "SURE-H" framework was structured so that it can satisfy the requirements of the slave which lessens manpower exertion, adds energy, and is built progressively secure. Any smart android gadget can be utilized to screen the profound office condition to distinguish any theft. It has a few highlights incorporated like ease, least time, overwhelmingly adaptable.

One work proposed by Yavuz et al. [6] uses a phone and PIC (programmable interface) a mobile controlling gadget, for inspecting the office electric power using gadgets. The framework doesn't encourage remote correspondence rather it utilizes a pin check algorithm to work with link systems. The framework guaranteed wellbeing as it can't be utilized by unapproved slaves as the framework utilizes the pin check algorithm.

In 2013, T. Oluwafemi et al. [8] demonstrated how a basic gadget in an office, for example, a fluorescent light (CFL), when associated with a home mechanization system through the internet, can be controlled by the unknown person then he/she can cause physical injury (break glass, fire incident, etc.) to the office members.

3. System Architecture

The framework relies on the Master-Slave model. Here, the gadgets including sensors, actuators, and microprocessors are treated as slaves which are related to the master. The plan can be broken down into 4 groups they are Home device, second is Control Unit, third is Master, and fourth is Slave [1]. The connection between the slave machine and the central unit line is via wired media, and between the control unit and the slave, the unit is either by LAN or Wi-Fi. The master is based on HTTP and the slave communications are done via API requests.

To structure a strong framework, at first, the sensors are designed furthermore and joined to the Node MCU module. This module is set for recognizing supervision through the wired or remote framework. The Node MCU component of the transfer board is customized with Arduino and after that, it is designed to get and operate a particular order conveyed through the internet after getting the feedback from the slave.

The cloud master is arranged to be dependent on a cloud administration platform known as "Blynk". Blynk gives a start to finish system progression arrangement based on IoT. At last, we plan an app associated with the Node MCU unit connected by a cloud specialist organization over the Internet [9].

The slave utilizes the net to access the cloud master and controls the home mechanization framework. Low power exchanging transfers can be utilized to incorporate gadgets with the Node MCU component for showing the exchanging usefulness. If the master is linked with the Internet then mobile slaves can get to the master utilizing electronic applications over the Internet. Figure 3 depicts the system architecture and figure 4 depicts the flow diagram of our system.

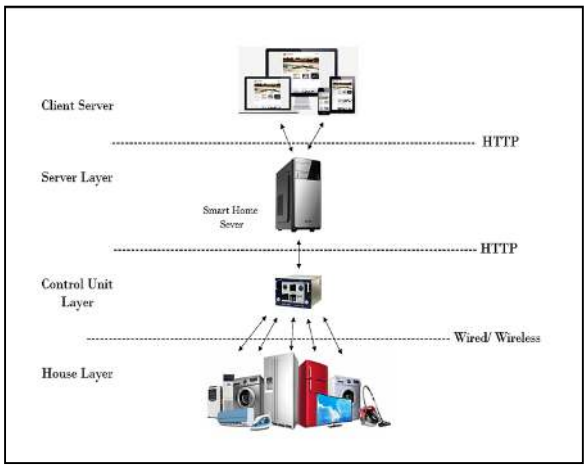

Fig 3. System Architecture

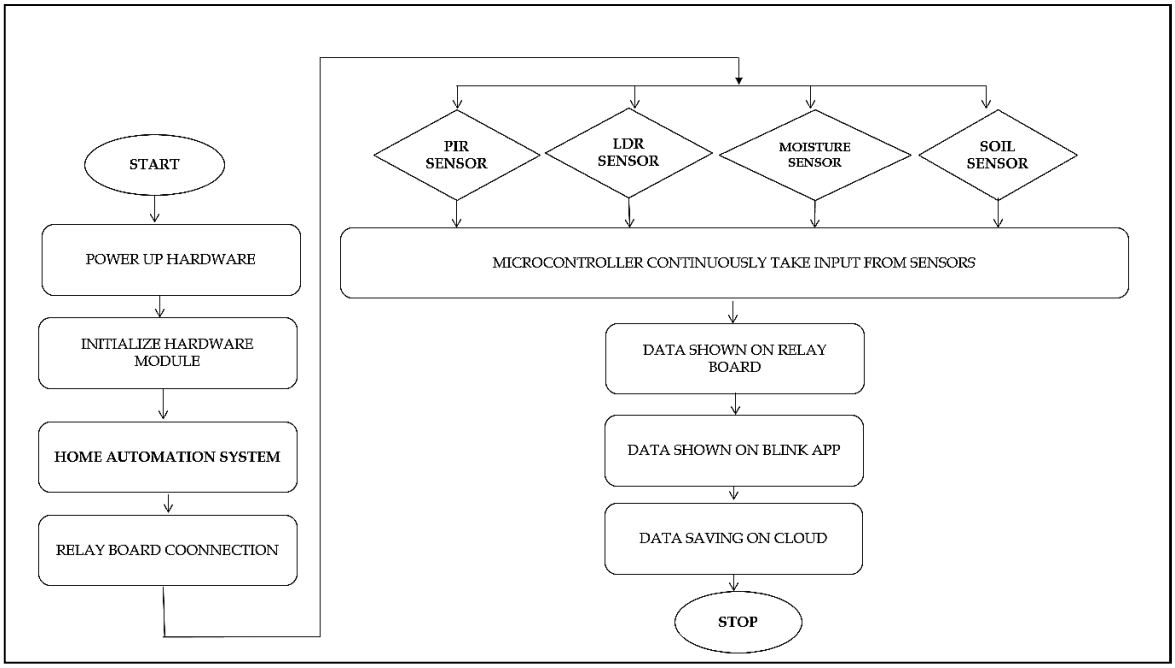

Fig 4. Flow Diagram

4. Hardware Specifications

The components used in our system are:

- Node MCU (ESP8266)
- Relay Board
- PIR Sensor (Passive Infrared Sensor)
- LDR Sensor (Light Dependent Resistor)
- DHT11 Sensor (Digital Humidity & Temperature Sensor)
- Soil Sensor

Fig 5. Node MCU

Fig .6 Relay Board

Node MCU shown in figure 5 is a microcontroller as the controller for this project which has many advantages.

Figure 6 depicts a relay board. In this system, we are using the 4 Channel Relay Board because we can connect 4 different components at one time and can trigger it at the same time. 4 types of sensors that will sense the environment and send the data are being used.

5. Implementation

The task's execution is partitioned into two sections. In the first part, the Node MCU will gather the programs and commands for controlling the sensors as we want. In the programming portion, the mobile application executes the programs and commands.

5.1 Software

In this system, we use a software named Arduino API as the bridge between the software and hardware and application software Blynk is used for connecting the microcontroller, sensors, and actuators as we want.

5.2 Hardware

We utilize a Node MCU microprocessor in this system. This board is a unique board for IoT applications that will use less power with integrated Wi-Fi and inbuilt Node MCU [2].
Here the Node MCU will be connected to the local Wi-Fi of our home and by then to the circuit of the board. The board will work from the commonplace in open mode. GPIO (General Purpose Input Output) pin picks the hand-off action, for instance in case the GPIO pin yield is low, then the exchange will be in open-loop condition. After that move when the circuit reaches the end, it closes the GPIO and when it reaches the high state then also it just closes the circuit [5].

Encrypting will be completed by Arduino programming. From the outset, in the wake of controlling up, the board will close the circuit for the Wi-Fi and partners with the enrolled framework using SSID and Passcode, because of this no one other than the owner can regulate the appliances. By then, it will carry out the code to interface the program with the respective GPIO and this will bring the database headings from the master using a GET request. The sensors will be differentiated within a short time and relating GPIO pin to either high or low is done. This strategy will remain in the microcontroller till the end with the objective of constant control on the sensors and the functions they are performing.

First of all, we'll power up the system by starting the hardware via a low voltage output like from Micro USB through the laptop, and then we'll transfer the setup code to the microcontroller through the same Micro USB. To initialize it will first verify the SSID and Passcode from the code to connect to the local Wi-Fi. Then the Node MCU gives a blink to show that it has been started, and then it will instruct relay board to respective sensors linked to it.

After connecting all the sensors, they all start collecting the inputs from the environment as they are programmed. The microcontroller is set to take all the inputs from the sensors one by one and save it, and then they will transfer the stored data from all the sensors to their respective output area, as PIR gives the output as the notification on the Smart Phone and DHT11 gives the output on the cloud server as shown in figure 7. Figure 8a and 8b illustrate the PIR sensor outputs.

Fig: 7a. Screenshot of the application showing that all 4 relay points are working

Fig: 7b. Screenshot of the application showing that PIR sensor giving the notification of intrusion in the environment

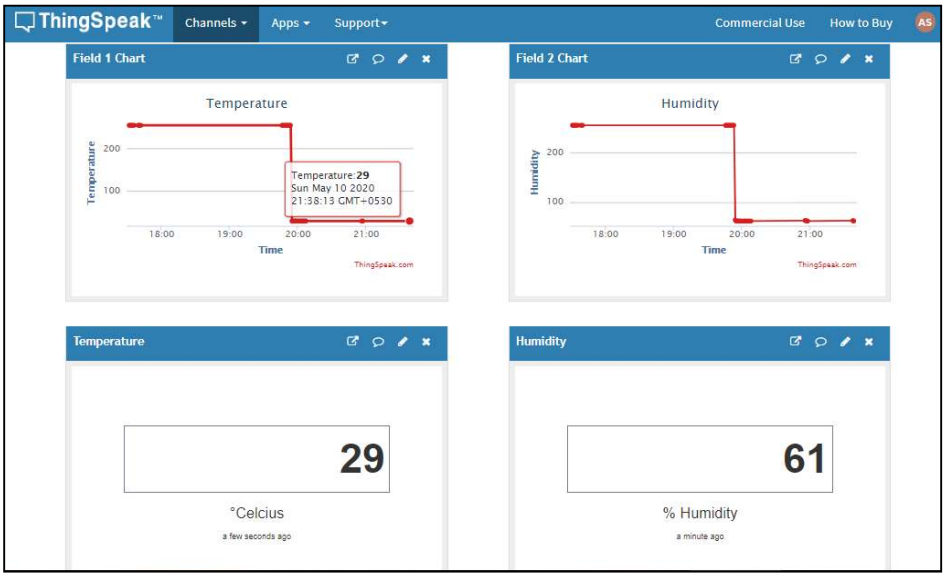

Fig 8 Output of DHT11 Sensor in the cloud server (ThingSpeak)

6. Discussion

The system will show the home automation control apparatus through a smart mobile app utilizing IoT. This will be a financially feasible and secure technique for controlling the gadgets remotely. IoT gives the fundamental communication foundation, taking the execution of this control apparatus to an enormous scale. The test that we confronted is regarding the rate of checking. Each test will take up to 7 seconds to switch between open or close [1]. This is a direct result of using network controllers that are open source. The speed of the test could be quicker and additional highlights of security could be investigated.

7. Result

In this paper, we found that how Node MCU was a better option compared to Arduino and Raspberry Pi for Home Automation System. Node MCU's GPIO's (General Purpose Input Output) helps to connect different types of sensors whether it's Digital sensors or Analog sensors. This system allows the user to give their commands, with which appliances can be started or stopped with the help of the application on our smartphone.

We have worked on different sensors and got various results in platforms like Android or iOS using the cloud platform. Using the PIR (change to full form) sensor the Arduino script tracked the motion sensor's difference using IR (infrared) signal. If there was any interference in the signal then the motion flag was set and it activates the output lines, where we can get the output as we want like if we want to switch the lights on or if we want to set the buzzer to ring an alarm as the signal.

The Temperature and Humidity Sensor will sense, measure, and report both the humidity and air temperature. The LDR (Light Dependent Resistor) allows higher voltage to pass through it, whenever it finds a high intensity of light and low voltage whenever there is a high intensity of light. The sensor is activated when the motion is detected and after detecting it will record any intrusion within the surveillance area and every 15 seconds it will alert the user by sending a notification to the application on the user's smartphone.

In the future, we have planned to incorporate several other sensors to enhance our proposed system with increased processing power.

8. Conclusion

This paper aims to show a financially effective Home Automation system model that uses the smart app to control home devices. As an enhancement, we can view the result in our app or the cloud server, but if we upgrade a little bit then we can see the cloud server data on our app or website. This paper has attempted to make a smart home system in a very convenient and faster manner. In the future extension to the project, the smart home system can be expanded to make a smart city with 5G with almost every appliance that will be connected with a smart micro-controller and the

microcontroller with our smart cell-phones. With the output from the sensors stored and it can be used to do future planning, temperature and humidity will help weather forecasting and the soil sensor will be useful for identifying the quality of the soil.

References

[1] Mandula K Parupalli R, Murty .C.A.S and Magesh E 2015 Mobile Based Home Automation Using Internet Of Things (IoT) *International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, pp. 340-343

[2] Piyare R. and Tazil.M. 2011 Bluetooth Based Home Automation System Using Cell Phones *IEEE 15th International Symposium on Consumer Electronics*, pp. 192-195.

[3] Yan M, H. Shi 2013 Smart Living Using Bluetooth Based Android Smartphone International *journal of wireless & mobile networks* **5**(1), pp .65-72.

[4] Sarmah R , Bhuyan M and Bhuyan M.H. 2019 SURE-H: A Secure IoT Enabled Smart Home System *2019 IEEE 5th World Forum on Internet of Things (WF-IoT),* IEEE, pp. 59-63.

[5] Madhu G M and C. Vyjayanthi 2018 Implementation of Cost-Effective Smart Home Controller with Android Application using Node MCU and Internet of Things (IoT) *2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE)* pp.1-5

[6] E. Yavuz, B. Hasan, I. Serkan, and K. Duygu, 2007 Safe and Secure Pic Based Remote Control Application for Intelligent Home, *International Journal of Computer Science and Network Security*, **7**(5), pp. 179-182.

[7] Tseng S, Li B, Pan J, and Lin.C. 2014 An Application of Internet Of Things With Motion Sensing On Smart House *IEEE International Conference on Orange Technologies*, pp. 61–64,

[8] T. Oluwafemi, S. Gupta, S. Patel, T. Kohno 2013 Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of home automation security *Learning from Authoritative Security Experiment Result*, pp.13-24.

[9] Theodore Ramli, Natashia Nabiha Dabimel, Mazlina Mamat, Norfarariyanti Parimon, Rosalyn R. Porl, 2016 Simple Speech Controlled Home Automation System Using Android Devices , *Journal of Scientific Research and Development* 3(1): pp. 33-38, 2016

[10] Subhajit Dey, Tamaghna Kundu, Sourav Mukherjee, and Mili Sarkar, 2015 Web-Based Real-Time Home Automation And Security System *International Journal of Electrical and Electronic Engineering & Telecommunications*,**4**(3), pp. 1-8.