AUTOMATE HOME THROUGH VOICE

Himanshu Chaurasia*[1],Anurag Shukla*[2], Gaurav Singh*[3], Prashant Maurya*[4], Ahmed Maaz Inam*[5]

*[1]Department of Computer Science and Engineering, Babu Banarasi Das Institute of Technology and Management, Lucknow, U.P, India
[2]Department of Computer Science and Engineering, Babu Banarasi Das Institute of Technology and Management, Lucknow, U.P, India
[3]Department of Computer Science and Engineering, Babu Banarasi Das Institute of Technology and Management, Lucknow, U.P, India
[4]Department of Computer Science and Engineering, Babu Banarasi Das Institute of Technology and Management, Lucknow, U.P, India

ABSTRACT

The main motive of this project is to automate home with the help of Node MCU and remotely control by any Android OS smart phone. As technology is improving day by day so our houses are also getting smarter. Smarter houses are rapidly shifting from conventional switches to centralized automated system, involving remote controlled digital switches. Conventional switches creates a fear of getting shocks and also difficult for physically challenged people to use.

Keywords: IoT, Smart Home, Node MCU, Wireless, Internet, Switches, Automation.

I. INTRODUCTION

Today we have various remote control devices like TV and other electronic systems, which makes our life very convenient. Now, with the help of this project, we can control tube lights, fans and other household appliances with a remote control. But when we hit the market, such devices aren't cost-effective, so we found a solution. We have developed a new system that is more affordable and allow users to control electronic devices without spending money on remote controls. This project will help users to control all their electronic devices with their smartphones. The technology used is the IoT, which allows you to access your electronic devices from anywhere via the Internet. As always, we are aware of our time, so it also helps us to save our time.

The Internet of Things (IoT) incorporates networks that allow sensors, software, electronic devices, and devices to share or collect data and perform specific actions. A vast network of physical devices.

Simply put, the IoT is made up of two words: the Internet and things.

- Objects – Physical devices, appliances, gadgets, etc.
- Internet – The Internet for these devices to connect .

The IoT aims to extend Internet connections not only to computers and smartphones, but to other devices that people use at home and at work. This technology enables remote control of devices over the network infrastructure. The result is less human effort and easier access to connect devices. Autonomous control allows the device to be operated without human intervention.

II. RELATED WORK

In recent years, wireless communication technology has advanced. In the late 2000s, we implemented a remote irrigation system that established wireless communication between three different farms (vineyards, apple orchards, and flood irrigated meadows) in widely dispersed areas of Australia's Galborn Valley. During this time, 3G wireless technology was developed and our remote controlled irrigation system was introduced into the new 3G network infrastructure. Real-time communication and remote access in such a large deployment was achieved using Remote Desktop Session over port 3399. As technology become advances, security breaches and vulnerabilities develop and this type of remote access and control is no longer considered secure. Recent work has been a large-scale deployment via a virtual private network (VPN), a remote water tank that allows access to IoT devices via smartphones with secure communication with sensors in multiple water tanks. The successful development and user acceptance of these smart technologies depends not only on cost-effectiveness and robustness, but also on ease of use, operational integration and trust building. Therefore, this paper considers the next step in research in the development of integrated voice control systems that provide consumers with secure and personalized services. In this article, we have taken the first step in this direction with the development of smart home automation systems.

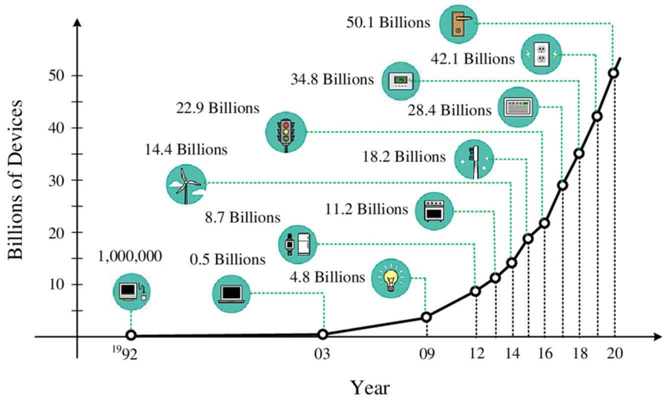

Fig. (a)

III. LITERATURE SURVEY

A. Home Automation System

The basic definition of a home automation system is to create a network between household appliances and internet so that all appliances in the home can be controlled by one machine. There's another term for this, it's a smart home. Imagine ,we come home and turning on the lights without touching the light switch. Imagine the moment when we're away from home and we don't worried about our home security. All of these integrated systems create a home known as a smart home.

B. Device-to-device communication

In device-to-device communication, there are two or more devices that are directly connected to each other, as shown in Figure (b). These devices are interconnected via many types of sources such as WiFi and ZigBee that helps in establishing a direct communication between two or more devices.

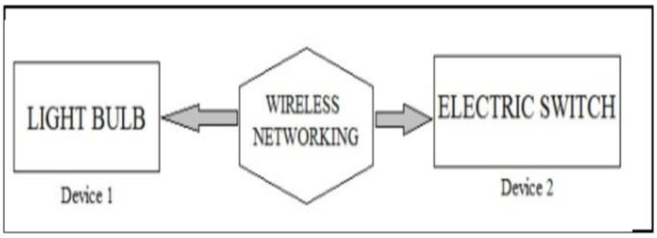

Fig. (b)

C. Device-to-cloud communication

In this communication network, IoT devices are connected to the cloud network, which is an application for exchanging data, as shown in Figure (c). Use existing sources such as wired Ethernet and the Internet for communication between the device and the cloud. Some popular consumers of IoT devices like Home Nest are using this communication model. For example, in the case of Nest Learning Thermostat, a device used to maintain temperature at specific points in time, the device sends its data to the cloud over the Internet, which is used to calculate household energy usage. In addition, this application also allows users to access and evaluate this thermostat data. However, there is a limitation in this area that only devices and clouds from the same manufacturer can be used.

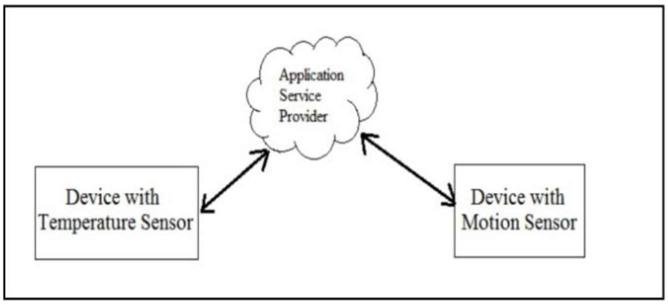
Application Service Provider
Device with Temperature Sensor
Device with Motion Sensor

Fig (c)

IV.Hardware Architecture and Implementation

The core of a home automation system consists of two main hardware components. Home server and node mcu.

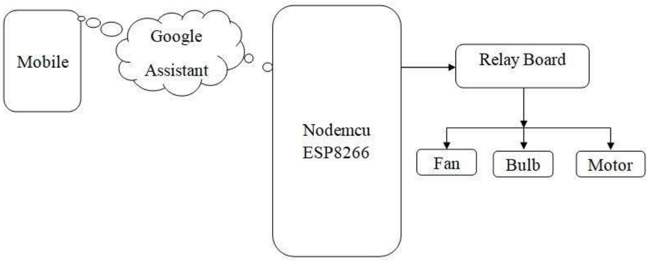

Fig. (d)

The node Mcu board is a low cost WiFi module, a stand-alone SystemOnChip with an integrated TCP / IP protocol stack that can provide microcontrollers with access to WiFi networks. The ESP8266 can host applications or offload all WiFi network functions to another application processor. The chip first became known to Western manufacturers in August 2014 using the ESP01 module from a third-party manufacturer, AiThinker. This small module allows the microcontroller to connect to a WiFi network and use Hayesstyle commands to establish a simple TCP / IP connection. Initially, however, there was little English documentation on the chip and the commands it accepts. The fact that it is very low priced and contains very few external components in the module, suggests that it could ultimately be very cheap, and many hackers have modules, chips.

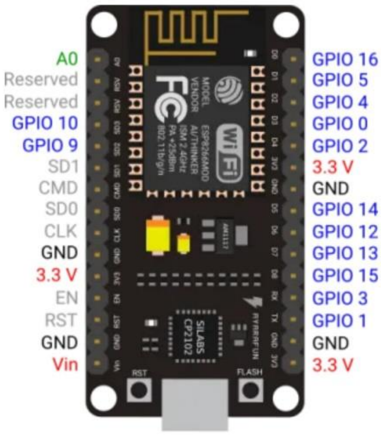

Fig. (e)

The relay is an electric switch. It consists of a row of input terminals and a row of operating contact terminals for one or more control signals. The switch may have any number of contacts or multiple contact forms, such as make contacts, break contacts, or combinations. Relay are used where it is necessary to control a circuit by an independent lowpower signal, or where several circuits must be controlled by one signal. Relays were first used in longdistance telegraph circuits as signal repeaters: they refresh the signal coming from one circuit by transmitting it on another circuit. Relays were used extensively in telephone exchanges and early computers to perform logical operations.

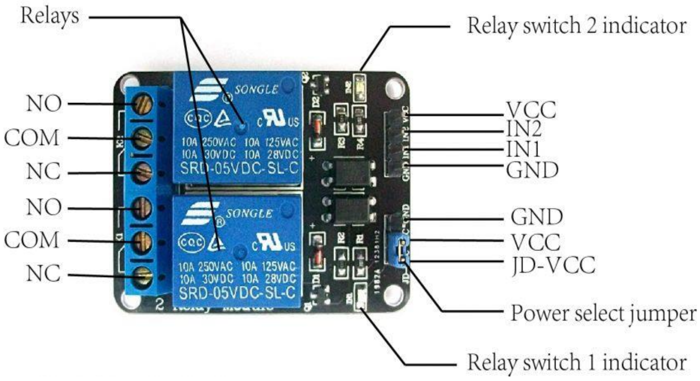

Fig (f)

IFTTT is a freeware web based service that creates chain of simple conditional statements called applet is triggered by changes that occur within other web services such as Gmail etc. For example, an applet can send an email message when a user tweets with a hashtag, or copy a photo to a user's archive on Facebook when someone tags the photo user. In addition to web-based applications, this service runs on iOS and Android. The trigger is the "this" part of the applet. These are the elements that trigger the action. For example, you can receive notifications from RSS feeds based on keywords or phrases. The action is the "that" part of the applet. These are the outputs that result from the input of the trigger.

Fig (g)

The breadboard is a build base for prototyping electronic devices. Originally, the term literally meant a breadboard, a piece of polished wood used to slice bread. By the 1970s, solder-free breadboards were available, and today the term "breadboard" is often used to refer to it.

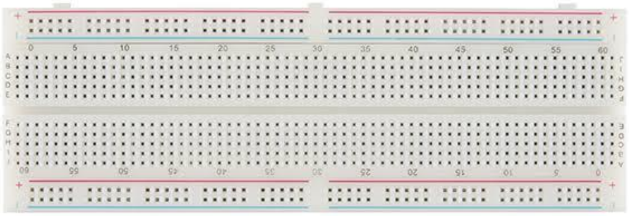

Fig (h)

V. Conclusions and future work

IOT-based home security and automation is very useful for remote users. Any home can be monitored and controlled using the prototype implemented in this document. This IOT-based system is a component of all Internet-based diverse applications. The system developed in this document is a cost-effective solution for IoT applications. The modules used to form it are lightweight, easy to use and inexpensive. It also enables easy operation and quick access to information. This allows users to access files from anywhere in the world via their computer. As more data is generated by things, not just people, the productivity gains on the Internet extend to things as well as people. This is a prototype that provides a reliable, low-cost and efficient IoT application solution worldwide. This means that our system can be applied to many other uses. Some of them are shown below.

- A healthcare system that monitors the health of patients.
- Mass monitoring
- Traffic management and route optimization in terms of intelligent transportation systems.
- Infrastructure monitoring that monitors the building's infrastructure to prevent danger.
- A water management system for checking water quality and its leaks and other similar conditions.
- SCADA system for monitoring substations. Monitoring system.
- Boundary monitoring system for monitoring noise pollution and air pollution.
- A smart greenhouse system for controlling its parameters over the internet.

VI. ACKNOWLEDGEMENT

We are highly grateful to our college Babu Banarasi Das Institute of Technology & Management for providing us robust environment to dive deep into this project and also thankful to our management, mentors and faculties for their guidance and support.

VII. REFERENCES

[1] Internet of things – A Hands-on Approach, Arshdeep Bahga and Vijay Madishetti, University press, 2015, ISBN: 9788173719547.

[2] Advanced Microprocessors and Peripherals – A. K. Ray and K. M. Bhurchandani, MHE, 2nd edition, 2006.

[3] Modern digital electronics – RP Jain – 4/e – MC GRAW HILL EDUCATION, 2010.

[4] Electronics devices and circuits – Salivahanan, MC GRAW HILL EDUCATION, 4th edition, 2010.

[5] The Guardian. How Can Privacy Survive in the Era of the Internet of Things? April 7, 2015, sec. Technology.

[6] Dave Evans, The internet of things, How the next evaluation is changing everything, April, 2011.

[7] Ms. Sejal, V. Gawande, Dr. Prashant, R. Deshmukh. “Raspberry Pi Technology.” Conference held at IETE Amravati Centre, Maharashtra, India.

[8] Polsonetti, Chantal. “Know the Difference Between IoT and M2M.” Automation World, July 15, 2014.

[9] Margerett Rouse, website definition, Last updated in 2005(Tech Target), Accessed on: September 6, 2015.

[10] Z. Alansari, N. B. Anuar, A. Kamsin, M. R. Belgaum, J. Alshaer, S. Soomro, and M. H. Miraz, “Internet of Things: Infrastructure, Architecture, Security and Privacy”, in 2018 International Conference on Com- puting, Electronics Communications Engineering (iCCECE), pp. 150– 155, Aug 2018, DOI: 10.1109/iCCECOME.2018.8658516.

[11] J. A. Chaudhry, K. Saleem, P. S. Haskell-Dowland, and M. H. Miraz, “A Survey of Distributed Certificate Authorities in MANETs,” Annals of Emerging Technologies in Computing (AETiC), vol. 2, no. 3, pp. 11– 18, 2018, DOI: 10.33166/AETiC.2018.03.002.

[12] A. S. A. Daia, R. A. Ramadan, and M. B. Fayek, “Sensor Networks Attacks Classifications and Mitigation”, Annals of Emerging Technologies in Computing (AETiC), vol. 2, no. 4, pp. 28–43, 2018, DOI: 10.33166/AETiC.2018.04.003.

[13] Z. Alansari, N. B. Anuar, A. Kamsin, S. Soomro, M. R. Belgaum, M. H. Miraz, and J. Alshaer, “Challenges of Internet of Things and Big Data Integration”, in Emerging Technologies in Computing (M. H. Miraz, P. Ex- cell, A. Ware, S. Soomro, and M. Ali, eds.), (Cham), pp. 47–55, Springer International Publishing, 2018, DOI: 10.1007/978-3-319- 95450-9_4.