

ABSTRACT

Smart home system is very popular in modern days that give many kind of application that make everything is simple and easy to control. In modern day, home appliances are using wireless technology and can be accessed by internet that will make residents life easier and organized. IoT-based Home Automation System is designed to assist the people with physical disabilities and elderly to provide support as well as to control the electrical appliances and monitor the room temperature using mobile application. The design is using embedded controller board and the home appliances are physically connected to output ports of this board via relays.

The Home Automation is a wireless home automation system that is supposed to be implemented in existing home environments, without any changes in the infrastructure. Home Automation let the user to control the home from his or her computer and assign actions that should happen depending on time or other sensor readings such as light, temperature or sound from any device in the Home Automation network. In the advancement of technologies controlling and monitoring electrical appliances using laptop, computer with the help of internet connection is possible. The main objective of internet of things is used to help specially challenged people and old age people to control electrical appliances and security purpose. IoT is very useful for these people in crucial situations.

There are two ways to access these process WIFI connectivity (or) it is connected to a router. This process is done in low cost & controlling many devices in a simple circuit.

Keywords: Internet of Things, automation, sensors, WIFI, Home Automation.

I. INTRODUCTION

1.1 Overview of Internet of Things

The internet of things (IoT) becoming a rapidly increasingly growth topic of conversation both in workplace and outside of it. It's a concept that not only has the potential to impact how we live but also how we work. This is the concept of basically connecting any device with an on and off switch to the Internet. This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices and sensors and actuators to the internet where the devices are intelligently linked together to enable new forms of communication amongst people and themselves almost anything else you . The survey Gartner says that by 2020 there will be over 26 billion to 64 billion connected device. The IoT is a giant network of connected of "things", which is related with people-people, people-things, and things-things. Significant advancement of IoT over the last couple of years has created a new dimension to the world of information and Communication technologies. The increasing technology is leading to anyone, anytime, anywhere connectivity of things with expectation which will extend and create an entirely advanced dynamic network of IoT. The IoT technology can be used for new innovation concepts that can be wide used for development space for smart homes system in order to provide intelligence, comfort, safety and improved quality of life.

1.2 Home automation Techniques

Smart home automation is very popular due to its numerous benefits in promising area, these techniques will controls all the electronic devices which will reduce the human involvement to get minimize. It will provide

various benefits such as greater safety, comfort, and security, a more rational use of energy and other resources thus contributing to a significant savings. This research application domain is very important and it will implement in future as it offers very powerful means for supporting and helping special needs of the elderly and people with disabilities for monitoring and control of home appliances. There are a number of factors that needs to be considered when designing a smart home system [7].

The system is very friendly with the dramatic increase in smart phone users, smart phones have gradually turned into all-purpose portable devices where the people can provide for their daily use. In this paper, a low cost wireless controlled smart home system for controlling and monitoring the home environment is presented. Embedded micro-web server with real IP connectivity is used for accessing and controlling of appliances and other devices remotely from an Android based app, which can be used from any Android supported device. The Raspberry pi is used for the micro webserver thus eliminating the use of PC and the system requires user authentication in order to access home automation system in smart home. Voice activation for switching applications may also incorporate to aid users especially for the elderly and the disabled persons.

Smart homes require sophistication control in its different gadgets which are basically electronic appliances. This has revolutionized the area of home automation with respect to a rapid increased level of affordability and simplicity through the integration of home appliances with smart phone and tablet connectivity [3]. Smart phones are already feature-perfect and can be made to communicate or interact with the other devices in an ad hoc network which has the connectivity options like Bluetooth and wifi. With the advent of mobile phones, Mobile applications development has seen a major outbreak. To Utilizing this opportunity for a smart home, we select the mobile phone commonly because it is found in normal household can be joined in a temporary network inside a home with the electronic equipment's. Android, by Google Inc. provides the platform for the development of the mobile applications for the Android devices. According to the International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker, Android maintained its position in global market share. Bluetooth is a short-range wireless communication technology that comes in handy as the solution while communicating over an adhoc network environment like connecting the home appliances with home environment with mobile phones [7].

The job of a sensor is to convert a physical quantity into numerical data. A single sensor or a number of different types of sensor can be integrated into one single device to collect data from the same spot which can be referred as a sensor node. When many sensor nodes are organized into a distributed network to collect the data from a large indoor environment we call this a sensor network. A data communication link through wire can be established for each of these nodes to transmit collected data to a central data collection sink node. The use of wire has become primitive and proved to be cumbersome for the sensor nodes residing far from the user.

1.3 Objectives of HAS (Home Automation Systems)

- 1) **Controlling Home Appliances via Application:** To develop an application that includes the features of switches mode application. Switch Mode can be used to control the switches of home appliances.
- 2) **Real Time Video Streaming from Web Camera:** To receives the quality video for the camera to the android application. Internal block diagram of Wireless Temperature sensor.
- 3) **Secure Connection Channels between Application and Raspberry pi:** Use of secure protocols over Wi-Fi so that other devices cannot control the home appliances. There are some Options for securing the connection in SSL over TCP, SSH.
- 4) **Controlled by any device capable of Wi-Fi (Android, IOS, PC):** To make the home appliances flexible in control, any device can be capable of using Wi-Fi based connectivity which will control the home appliances from remote location.
- 5) **Extensible platform for future enhancement:** The application is to be highly extensible, with possibility of adding features in the future as needed.

1.4 Machine Learning

Machine learning is a sub field of computer science, a type of Artificial Intelligence,(AI), that provides machines with the ability to learn without explicit programming. Machine learning evolved from pattern recognition and Computational Learning Theory. There, some essential concepts of machine learning are discussed as well as, the frequently applied machine learning algorithms for smart data analysis. A learning algorithm takes a set of samples as an input named a training set. In general, there exist three main categories of learning: supervised, unsupervised, and reinforcement [54, 55, 56]. In an informal sense, in supervised

learning, the training set consists of samples of input vectors together with their corresponding appropriate target vectors, also known as labels. In unsupervised learning, no labels are required for the training set. Reinforcement learning deals with the problem of learning the appropriate action or sequence of actions to be taken for a given situation in order to maximize payoff. This article focuses on supervised and unsupervised learning since they have been and are being widely applied in IoT smart data analysis. The objective of supervised learning is to learn how to predict the appropriate output vector for a given input vector. Applications where the target label is a finite number of discrete categories are known as classification tasks. Cases where the target label is composed of one or more continuous variables are known as regression [57]. Defining the objective of unsupervised learning is difficult. One of the major objectives is to identify the sensible clusters of similar samples within the input data, known as clustering. Moreover, the objective may be the discovery of a useful internal representation for the input data by preprocessing the original input variable in order to transfer it into a new variable space. This preprocessing stage can significantly improve the result of the subsequent machine learning algorithm and is named feature extraction.

II. LITERATURE REVIEW

Design and Implementation of Security for Smart Home based on GSM technology was discussed by Govinda et al. (2014) that provides two methods to implement home security using IoT [1]. One is using web cameras such that whenever there is any motion detected by the camera, it sounds an alarm and sends a mail to the owner. This method of detecting intrusion is quite good, albeit somewhat expensive due to the cost of the cameras involved in the process. The cameras need to be of good quality which means it should have a wide range and the picture quality should be high enough to detect movement. Also if you go for movable cameras such as dome cameras they will cost even more than the fixed ones.

SMS based system using GSM was proposed by Karri and Daniel (2005) propose to use internet services to send messages or alert to the house owner instead of the conventional SMS.[2] Jayashri and Arvind (2013) have implemented a fingerprint based authentication system to unlock a door [3]. This system helps users by only allowing the users whose fingerprint are authorized by the owner of the house. This system can also be used to monitor who all have used the sensor to gained entry into the house. The system is coupled with a few more home protection features such as gas leakage and fire accidents. Although a good system, fingerprint sensors are expensive and complex (as they need increased sensor resolution) to integrate into an IoT setup. Some experts also argue that only relying on a fingerprint sensor is not wise as it is relatively easy to lift someone's fingerprints and replicate them, which is why it is always advised to use fingerprint scanners in a two factor authentication systems where an additional layer of security is available in the form of PIN, passcode, voice recognition, etc.

Some researchers proposed an idea of robust IoT home security system where a fault in of one component in the system does not lead to the failure of the whole system [4]. The idea of using multiple devices which may or may not be directly compatible with each other but can be made to work in such a way that they can replace an existing component of the system in case of a fault. In tandem to this, the model has the ability to use overlap between various devices which would result in preserving energy thus making the model more efficient. An example provided of the said model would use temperature sensor, WiFi module and a door sensor to replace a faulty camera. The authors are successful in an effort to demonstrate the given example. However such systems are useful for people with energy efficiency in mind and for those who need a high degree of robustness with their security systems and are willing to expend more money than usual.

Laser rays and LDR sensor are used to detect intrusion using their movement was proposed in 2016 [5]. The way the system works is that a laser is focused towards a LDR sensor and the moment that the contact of laser to LDR sensor breaks, the alarm connected to the sensor goes off alerting the neighbours and sends a SMS to the owner. This system solves the problem of covering the places which are out of range from the fixed cameras but faces the same difficulties which are faced with systems consisting of GSM modules to send text messages, which is that the delivery of message is dependent on network coverage. Also due to the nature of lasers being a straight beam, it can be avoided by intruders who know about the system and are capable of dodging the lasers, rendering the whole system useless.

A novel way to design an electronic lock using Morse code and IoT technology [6]. The authors claim that this as an original idea which have not been tried before and is the first of its kind "optical Morse code-based electronic locking system". This system uses LED's (Light emitting diodes) as an encrypting medium to send

signals. To make it more accessible to general public, the LED in smart phones has been used. On the receiver's side is a photosensitive resistor as well as a microcontroller such as arduino processor which has the ability to decrypt the optical signal after receiving them from the LED. Upon decoding the signal it can then upload the current condition of the lock to a cloud from where the owner can monitor the system. The authors have experimented the system in real time and it has proved to work under different illumination environments with all the functions working as they were intended to. The authors also claim to have an easy and user-friendly interface. The IoT system developed here works very well and can be used by anyone and is very convenient due to the use of mobile phones as LED, which also makes it a cost expensive alternative[7]. Anitha et al (2016) proposed an home automation system using artificial intelligence and also proposed a model for cyber security systems [8,9].

III. WORKING PRINCIPLE

There are various techniques to control home appliances such as IOT based home automation over the cloud, home automation under WiFi through android apps from any smartphone, Arduino based home automation, home automation by android application based remote control, home automation using digital control, RF based home automation system and touch screen based home automation. Wireless home automation using IOT is an innovative application of internet of things developed to control home appliances remotely over the cloud. Wi-Fi (Wireless Fidelity) is a wireless networking technology used for exchanging the information between two or more devices without using cables or wires. There are various Wi-Fi technologies like Wi-Fi 802.11a, 802.11b, 802.11g and 802.11n. Here, in this project Wi-Fi module is used to receive commands from the internet and activate loads through TRIAC & Optocoupler by executing a program written within the Wi-Fi module. Hence, no microcontroller is used in this project to drive loads.

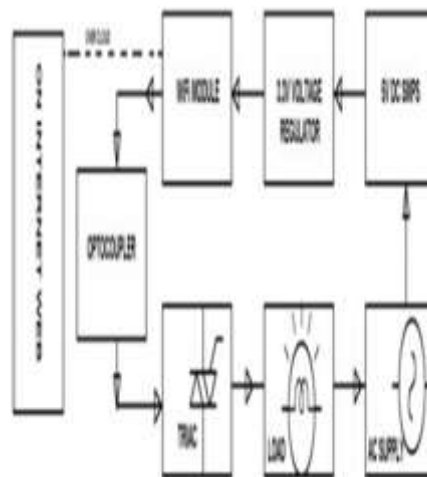


Fig 1: Block Diagram

IV. MATERIALS AND METHODS

Various hardware materials are required to have an home automation system. Some of the essential components are listed below to have an idea about the proposed system.

Components required

- ESP-12 WiFi Module
- LM1117-3.3V
- Sugar Cube Relay – Qty.4
- Resistors 10K, 1K,4.7K
- Capacitor 1000uF, 10uF, 104 (0.1uF)
- PBT-2 Connectors Qty. 5
- ULN2003
- Arduino Board
- Arduino IDE
- 12V Power Supply

4.1. Arduino Uno

Arduino is an open source, PC paraphernalia and programming organization, endeavour, and client group that plans and produce microcontroller packs for constructing programmed devices and intelligent object that can detect and control questions in the real world. The inception of the Arduino extend began at the Interaction Design Institute in Ivrea, Italy. The equipment reference plans are appropriated under a Creative Commons Attribution Share. Arduino Uno is shown in figure 1.

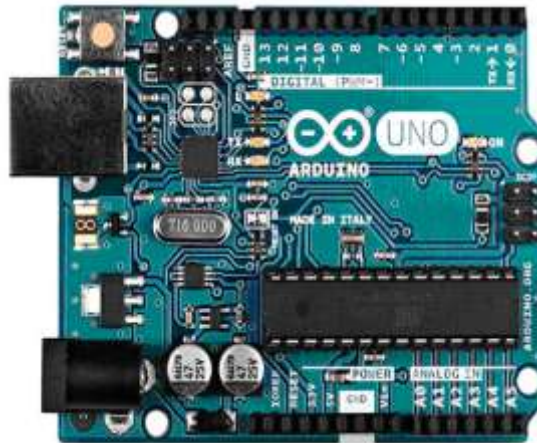


Figure 2. Arduino Uno.

4.2. ESP8266 (WiFi Module)

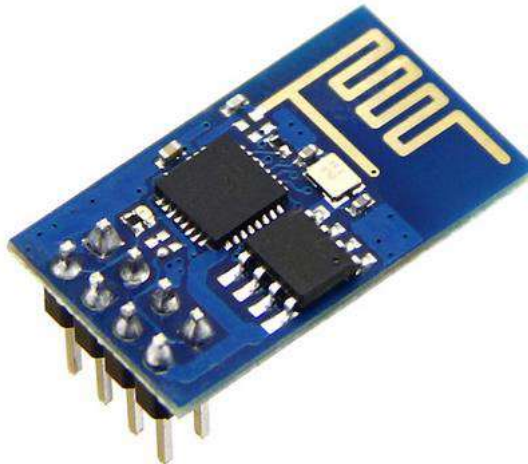


Figure 3. ESP8266 (WiFi Serial Transceiver)

The ESP8266 is an ease Wi-Fi chip with full TCP/IP stack and MCU (Micro Controller Unit) capacity created by Chinese . These are the primary arrangement of modules made with the ESP8266 by the outsider producer AI-Thinker and remain the most generally available. They are large alluded to as "ESP-xx modules". To shape a workable advancement framework they require extra parts, particularly a serial TTL-to-USB connector and an outside 3.3 volt control supply. The ESP8266 is shown in figure 3.

4.3. Jump wires

A breadboard is utilized to build and test circuits expeditiously afore finalizing any circuit design. The breadboard has many apertures into which route components like ICs and resistors can be connected. The apertures are generally spaced 0.1" apart to put up standard DIP machinery. A typical breadboard that includes top and bottom power distribution rails is shown below figure 4. Jump wires are generally used to establish connectivity with bread board as shown in figure 4.



Figure 4. Jump Wires.

V. PROPOSED WORKING MODEL

Before we begin connecting the hardware, we have to get the ESP8266 set up by flashing the latest version of the firmware available for the module. This is because the chip comes with an older version of the AT command firmware pre-installed out of the box which cannot communicate with the Blynk libraries efficiently and will give an error with our code. To flash the latest firmware, download the ESP8266 flasher tool and the latest firmware from the internet which would be in the bin format and set up the ESP8266 to the Arduino Uno as described below in figure 5.

ESP8266	ARDUINO UNO
GND	GND
GP2	Not Connected
GP0	GND
RX	RX
TX	TX
CHPD	3.3 V
RST	Not Connected
VCC	3.3 V

Figure 5. Setup to enable ESP8266 Flash mode

Once the ESP8266 has been flashed with the latest firmware, other components can be added to the configuration. For this we will need a breadboard to connect the microcontroller, reed sensor, buzzer and the ESP8266 using the jumper wires. The breadboard is used to interface between the various components available. It also makes it easy to connect multiple inputs to a single pin on the arduino board.

Following sketch shown in figure 6, which has been constructed using the Fritzing software shows how the components are supposed to be connected together using the breadboard and the jumper wires. The final configuration need not be identical to the given sketch, although the pins on each device needs to be connected to the same corresponding pins on the Arduino Uno board. The architecture diagram is shown in figure 7.

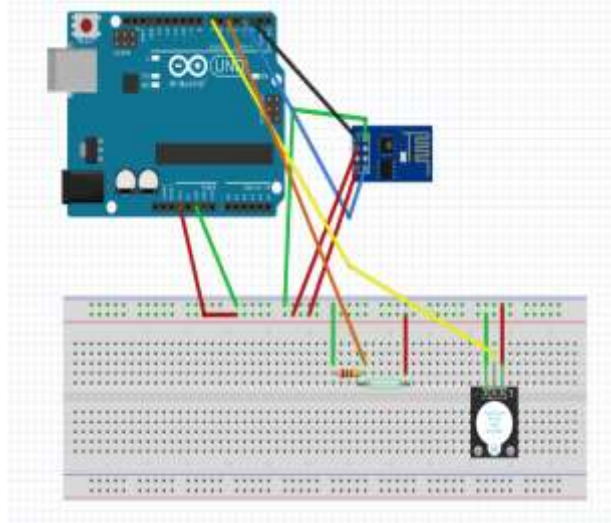


Figure 6. Sketch Diagram

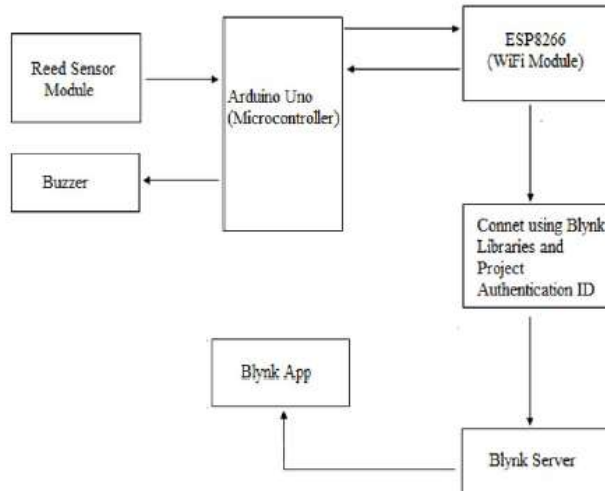


Figure 7. Architecture diagram of the proposed model



Figure 8. Final hardware of the proposed model



VI. CONCLUSION AND FUTURE SCOPE

The sensors placed on the door informs the home owner as soon as the door is opened by sending a Push notification. The user will get this notification irrespective of whether the phone is locked or unlocked or even if any other app is opened at the moment. This was the main objective of the project, which is the user feels safe and not worry about any intrusion or break-ins when he is away from home. This setup can also be used in commercial offices where some areas are restricted for certain personnel, such a system will immediately inform the administrator of any unauthorized personnel trying to access such an area. Therefore the extensibility and applicability of such a system is only limited only by the imagination.

Another important component of the project is the connectivity between the ESP8266 (WiFi module) and the Blynk server. The system successfully connected to the Blynk server using the authentication token and the Blynk libraries. As a result, we were able to get the notification on our smart phones as soon as there was any change in the status of the reed module sensor. Also the additional ability to control the alarm remotely is very beneficial and can be very useful in some unforeseen circumstances. It was also observed that the Blynk app worked smoothly and carried out all communication between the hardware and the app very accurately. The developed system can also be used to in industrial and commercial applications such as offices, warehouses and other areas where some areas are reserved for authorized personnel only or other places where safety and precautions are of primary concerns such as internet server room of a big MNC from where corporate data can be stolen. The system can also be easily upgraded to add extra safety features such as cameras, motion detection sensors, etc. for increased safety. The system can also further be developed by adding an RFID scanner so that the authorized users need only carry a RFID or NFC tag with them on their person. The RFID scanner will work by scanning the tag wirelessly and if the user is authorized to enter, the alarm system will be disabled for some time so that the user can enter.

VII. REFERENCES

- [1] Sirsath N. S, Dhole P. S, Mohire N. P, Naik S. C & Ratnaparkhi N.S Department of Computer Engineering, 44, Vidyanagari, Parvati, Pune-411009, India University of Pune, "Home Automation using Cloud Network and Mobile Devices".
- [2] A. R. Al-Ali and M. AL-Rousan, Java-based Home Automation System, IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, May 2004,
- [3] Charith Perera, Student Member, IEEE, Arkady Zaslavsky, Member, IEEE, Peter Christen, and Dimitrios Georgakopoulos, Member, IEEE "Context Aware Computing for The Internet of Things: A Survey". IEEE COMMUNICATIONS SURVEYS & TUTORIAL.
- [4] Charith Perera_y, Arkady Zaslavskyy, Peter Christen_ and Dimitrios Georgakopoulosy Research School of Computer Science, The Australian National University, Canberra, ACT 0200, Australia yCSIRO ICT Center, Canberra, ACT 2601, Australia " CA4IOT: Context Awareness for Internet of Things".
- [5] Bill N. Schilit, Norman Adams, and Roy Want, "Context-Aware Computing Applications".
- [6] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, a Marimuthu Palaniswamia, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions".
- [7] S.P. Pande, Prof. Pravin Sen, "Review On: Home Automation System For Disabled People Using BCI" in IOSR Journal of Computer Science (IOSR-JCE) e- ISSN: 2278-0661, p-ISSN: 2278-8727 PP 76-80.
- [8] Basil Hamed, "Design & Implementation of Smart House Control Using LabVIEW" at International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, January 2012.
- [9] Basma M. Mohammad El-Basioni¹, Sherine M. Abd El-kader² and Mahmoud Abdelmonim Fakhreldin³, "Smart Home Design using Wireless Sensor Network and Biometric Technologies" at Volume 2, Issue 3, March 2013.
- [10] Inderpreet Kaur, "Microcontroller Based Home Automation System With Security" at IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 1, No. 6, December 2010.
- [11] Rosslin John Robles and Tai-hoon Kim, "Review: Context Aware Tools for Smart Home Development", International Journal of Smart Home, Vol.4, No.1, January, 2010.
- [12] Hitendra Rawat, Ashish Kushwah, Khyati Asthana, Akanksha Shivhare, "LPG Gas Leakage Detection & Control System", National Conference on Synergetic Trends in engineering and Technology (STET-2014) International Journal of Engineering and Technical Research ISSN: 2321-0869, Special Issue.
- [13] Nicholas D., Darrell B., Somsak S., "Home Automation using Cloud Network and Mobile Devices",



IEEE Southeastcon 2012, Proceedings of IEEE.

- [14] Chan, M., Campo, E., Esteve, D., Fourniols, J.Y., "Smart homes-current features and future perspectives," *Maturitas*, vol. 64, issue 2, pp. 90-97, 2009.
- [15] Grieco A., Occhipinti, E. and Colombini, D. (1989) Work Postures and Musculo-Skeletal Disorder in VDT Operators. *Bollettino de Oculistica*, Suppl. 7, 99-111.
- [16] Pahlavan, K., Krishnamurthy, P., Hatami, A., Ylianttila, M., Makela, J.P., Pichna, R. and Vallstron, J. (2007) Handoff in Hybrid Mobile Data Networks. *Mobile and Wireless Communication Summit*, 7, 43-47..

CITE AN ARTICLE

B., & Sharma, N. (2018). SMART HOME SECURITY SOLUTIONS BASED ON INTERNET OF THINGS (IOT) USING WIFI INTERFACE. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, 7(5), 389-397.