Review On: Home Automation Based Upon Internet of Things

[1]Ashwini Rohidas Pawar, [2]Prof. V.M.Umale

Department of EXTC, S.S.G.M.C.E, Shegaon, (India)

ABSTRACT

Home automation is becoming popular due to their enormous benefits. Home automation refers to the control of home appliances and domestic features by local networking and or by remote control. Artificial Intelligence provides us the framework for real-time decision and automation for Internet of Things (IoT).This paper surveys the different intelligent home automation systems and technologies from a various features standpoint. The work focuses on concept of home automation where the monitoring is facilitating through camera installed in users home. Heterogeneous home-automation systems and technologies considered in review with central controller based (Arduino, Raspberry pi or Intel Galileo), web based, email based, Bluetooth-based, mobile-based, SMS based, Zigbee based, Dual Tone Multi Frequency-based, cloud-based and the Internet.

Keywords: Home Automation, Internet Of Things (Iot), Smart Home, Iot Architecture, Iot Issues.

I INTRODUCTION

Kevin Ashton, the Executive Director of Auto-ID Labs at MIT, was the first to describe the Internet of Things, while making a presentation for Procter & Gamble in the year 1999. Kevin Ashton believed Radio Frequency Identification (RFID) was a condition for the Internet of Things. In his presentation, he concluded if all devices were "connected," computers could manage, track, and list them. Up to some limits, the connecting or tagging of things has been achieved through technologies such as digital watermarking, barcodes, and QR codes. Inventory control is one of the more obvious advantages of the Internet of Things (IoT). One of the most important component in developing a functional IoT was the IPV6 and its noticeable ability is to increase address space. Steve Leibson, of the Computer History Museum, states, "The address space expansion means that we could assign an IPV6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths." In other words, we are not going to run out of internet addresses anytime soon. The IoT, as a concept, wasn't officially named until 1999. One of the examples of an IoT is from the early 1980s, and was of a Coca Cola machine, located at Carnegie Melon University. Local programmers would connect by Internet to the refrigerated appliance, and check to see if there was a drink available, and if it was cold, before making the trip [11]. Till date, the IoT has evolved into a system using multiple technologies, ranging from the Internet to wireless communication and from micro-electromechanical systems (MEMS) to embedded systems. The conventional fields of automation including the automation of home's, wireless sensor networks, GPS, control systems, and others, all support the IoT. This survey paper on IoT mainly focuses on how to enable general objects to see, hear, and smell the physical world for themselves, and make them connected to share the observations. In that sense, monitoring and decision making can be moved from the humans to the machines.

It is not that easy to define the Internet of Things because it has become an umbrella term for many realities which, in the end, have little in common, depending on how we look at it. However IoT may be characterized by 7 crucial elements [12]. Figure [1]

1. Connectivity: These are devices, sensors, that are to be connected: to an item, to each other, actuators, a process and to 'the Internet' or another network.
2. Things: Anything that can be marked or connected as such as it's designed to be connected. From sensors and household appliances to tagged livestock. Devices can contain sensors or sensing materials can be attached to devices and items.
3. Data: Data is the glue of the Internet of Things, the first step towards action and intelligence.
4. Communication: Devices get connected so they can communicate data and this data can be analyzed.
5. Intelligence: The aspect of intelligence as in the sensing capabilities in IoT devices and the intelligence gathered from data analytics (also artificial intelligence).
6. Action: The consequence of intelligence. This can be manual action, action based upon debates regarding phenomena (for instance in climate change decisions) and automation, often the most important piece.
7. Ecosystem: The place of the Internet of Things from a perspective of other technologies, communities, goals and the picture in which the Internet of Things fits. The Internet of Everything dimension, the platform dimension and the need for solid partnerships.

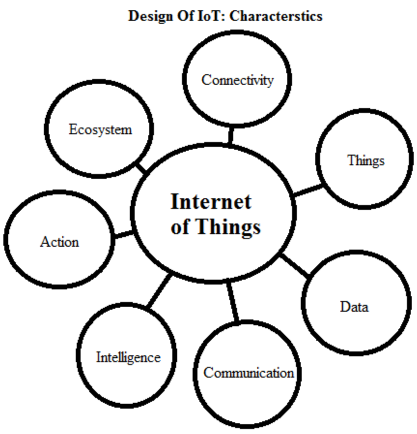

Figure 1: Seven crucial elements of IoT

The Internet of Things is defined as a network of connected devices with 1) unique identifiers in the form of an IP address which 2) have embedded technologies or are equipped with technologies that enable them to sense, gather data and communicate about the environment in which they reside and/or themselves.

II ARCHITECTURE OF IOT

Architecture of IoT [10] is broadly classified into 4 layers.

1. Sensor Layer

   This is lowest layer of IOT Architecture, which consists of sensor networks, embedded systems, RFID tags and readers or other soft sensors which are different forms of sensors deployed in the field. Each of these sensors has identification and information storage (e.g. RFID tags), information collection (e.g. sensor networks), etc. [Figure.2]

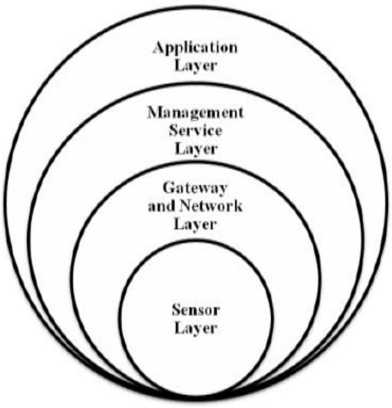

Figure 2: Layered IoT Architecture

2. Access Gateway and Network Layer

   This layer is responsible for transferring the information collected by sensors to the next layer. It should support scalable, flexible, standards universal protocol for transferring data from heterogeneous devices (Different types of sensor nodes). This Layer should have high performance and robust network. It should also support multiple organizations to communicate independently.

3. Management Service Layer

   This layer acts as an interface between the Gateway -Network layer and application layer in bidirectional mode. It is responsible for device management and information management and responsible for capturing large amount of the raw data and extracting relevant information from the stored data as well from the real time data.

4. Application Layer

   This is the top most layer of IoT which provides a user interface to access various applications to different users. The applications can be used in various sectors like transportation, health care, agriculture, supply chain, government, retail etc

.

III LITERATURE SURVEY

Previous Research work on existing Home Automation Systems:

Vikram.N, Harish K.S, Nihaal M.S,Raksha Umesh4, Shetty Aashik Ashok Kumar[1] explains a methodology to provide a low cost home automation system using wireless fidelity (WiFi). A WiFi based Wireless Sensor network (WSN) is designed for monitoring and controlling the environment, safety and electrical parameters of smart interconnected home. The user can exercise harmless control over the devices in smart home via the Arduino application based Graphical user interface (GUI) on a Smartphone. This paper finds out the new method for automating home appliances by analysing their ability to be interlinked. The experimental trick involves the use of ESP8266 WiFi module, Atmel ATmega microcontrollers, nrf24co1 +RF module, sensors, SPDT relays, TRIAC for the voltage regulation. Each microcontroller is provided with a RF module for the purpose of communication with other microcontroller. One microcontroller is configured as HUB and the remaining as sensor nodes. Tree network topology is used in present work. All the sensors readings will be communicated to the HUB via the RF module. Data received at HUB is sent through the UART serial port to the WiFi module. The WiFi module sends data to the sensor where it is stored and can be retrieved for future use. The additional benefits of this method are its security features which includes fire alarm, motion detection and gas leakage detection. Switching and regulation of loads are done through 8 channel relay board and 3 channel solid state relay dimmer. Voltage measurement is done by step down transformer and current sensing is done by Hall effect based ACS-712. Java platform is used for the automation.

Praveen Kumar, Umesh Chandra Pati[2] in their proposed home automation technology provides smart monitoring and control of the home appliances as well as door permission system for interaction between the visitor and home/office owner. Using this technology the consumer can reduce wastage of electrical power by regular monitoring of home appliances or proper on/off scheduling of the devices. In this system the combination of Raspberry Pi model B and Arduino mega 2560 are used. The programming languages used for coding are Python and C language. This smart home system can be accessed on smart phone using IP address. The server of the smart home is hosted on Raspberry Pi model B which sends and receives the data from the remote user. The user can monitor the status and can control the appliances using smart phone or laptop on IP address.

Soliman, Tobi Abiodun, Tarek Hamouda, Jiehan Zhou, Chung-Horng Lung[3] presents an approach to the development of smart home applications by integrating IoT with web services and cloud computing. The approach focuses on

1. Embedding intelligence into sensors and actuators using Arduino platform.

2. Networking smart things using Zigbee technology.

3. Facilitating interactions with smart things using cloud services.

4. Improving data exchange efficiencies using JSON data format.

The microcontroller enabled sensors are used for measuring home conditions such as temperature, humidity at the front end and microcontroller enabled actuators for monitoring home appliances such as light, doors, fans and air conditioners. This approach uses Platform as a Service (PaaS) and Software as a Service (SaaS) in cloud computing for processing data at the back end. The system uses RFID cards which allows the tracking the users presence in a home. This architecture is based on Cloud Computing resources to implement web applications responsible for reading sensors, storing readings and monitoring home applications over internet.

Eleni Isa, Nicolas Sklavos [4]in their system implemented on a microcontroller module, through an embedded platform. Systems operation is also based on camera and sensors inputs. Each time the involved end users and the security officer can be informed for attacks, operation mode changes etc through sms communication via the available GSM network. The circuit board mainly includes a microcontroller device, digital and analog pins as well as other peripheral components. The system is based on R3 Board ATmega 328 in conjunction with an R3 Ethernet shield. The system starts only with user authentication based on password policies, if password is wrong in 3 attempts then the system is set to alarm state. In this state camera capture a photo, play a character sound through the speaker finally send a small text message to user and dedicated security office.

Ho-Kyeong Ra, Sangsoo Jeong, Hee Jung Yoon, and Sang Hyuk Son[5] designed smart home automation frame work (SHAF). The real world example is performed and demonstrated hear. In this design Raspberry Pi with Zigbee is used as smart home central service and Arduino with Zigbee is used as sensor nodes. In the demonstration the user press the button on smart phone application to send command and request for smart home status update. After getting a command from the user server node sends command to the sensor node for the update. After receiving the request at each sensor node the verification of the received message is done. If the verification is succeeded for the particular request then the node sends the actuation signal to turn on the light.

IV SYSTEM COMPARISION

The various platforms are compared as shown in figure [3] for the parameters such as speed, cost,etc. and take best out of it.

Board Parameters	**Arduino Uno**	**Raspberry Pi 3**	**Intel Edition**
Price	INR 2100	INR 2400	INR 3500
Size	7.6*1.9*6.4 cm	8.5*5.6*1.7 cm	3.55*2.5*0.39

GPIO	14	40	40
Clock speed	16 MHz	1.2 GHz	500 MHz, 100MHz
On board n/w	None	10/100 Mbps Ethernet socket	Dual-band (2.4 and 5 GHz) WiFi, Bluetooth 4.0
Multitasking	No	Yes	Yes
Input voltage	7 to 12 V	5V	3.3 to 5V
Flash memory	32 KB	Micro SD card	4 GB embedded multimedia card
USB	One, input only	Four, peripherals OK	One, peripherals OK
OS	None	Linux distributions	Yocto Linux v1.6

Figure 3: Comparison of board parameters

By comparing the parameters we come to know that Raspberry Pi 3 is better option for us to use in our design in terms of clock speed, memory, USB, etc. Also the systems are compared as shown in figure [4].

Paper	**Model used**	**Speed**	**Components**
‘A Low Cost Home Automation System Using Wi-Fi Based Wireless Sensor Network Incorporating Internet of Things(IoT)’, 2017	ATmega microcontroller	1 MIPS per MHz	MQ2 sensor, LM393 sensor, PIR sensor, rain sensor M009, SPDT switch , ESP8266 WiFi module
‘ IoT Based Monitoring and Control of Appliances for Smart Home’, 2016	Raspberry Pi 2, Arduino Mega 2560 board	900 MHz (RBPi 2), 16MHz (arduino)	Mike, push button, keyboard, mouse, speakers, LCD screen, 4.2 inch touch screen, Pi camera, relay board
‘Smart Home: Integrating Internet of Things with Web Services and Cloud Computing’, 2013	Arduino and Zigbee technology	16 MHz (arduino), variable from 20 Kbps to 250 Kbps (Zigbee)	Humidity sensor DHT22, light sensor VCNC4000, actuators (for light, fan, AC, etc...), RFID card
‘Smart Home Automation: GSM Security System Design & Implementation’, 2015	ATmega microcontroller	1 MIPS (microprocessor without interlocked pipeline stages) per MHz	R3 board ATmega 328, R3 Ethernet shield, GSM shield, camera, micro SD card, keypad, sensor LCD, speaker
‘WiP Abstract: SHAF: Framework for Smart Home Sensing and Actuation’ 2016	Raspberry Pi B, Arduino, Zigbee technology	600 MHz (RBPi B)	Light sensor, humidity sensor

Figure 4: Comparison of systems

To improve the various parameters such as speed, cost, accuracy of systems we will use advanced version of Raspberry Pi having higher speed than earlier versions. We are having various security issues such as door security, fire security, gas explosions and shot circuits. We will implement security system by considering the above mentioned issues.

IV METHODOLOGY

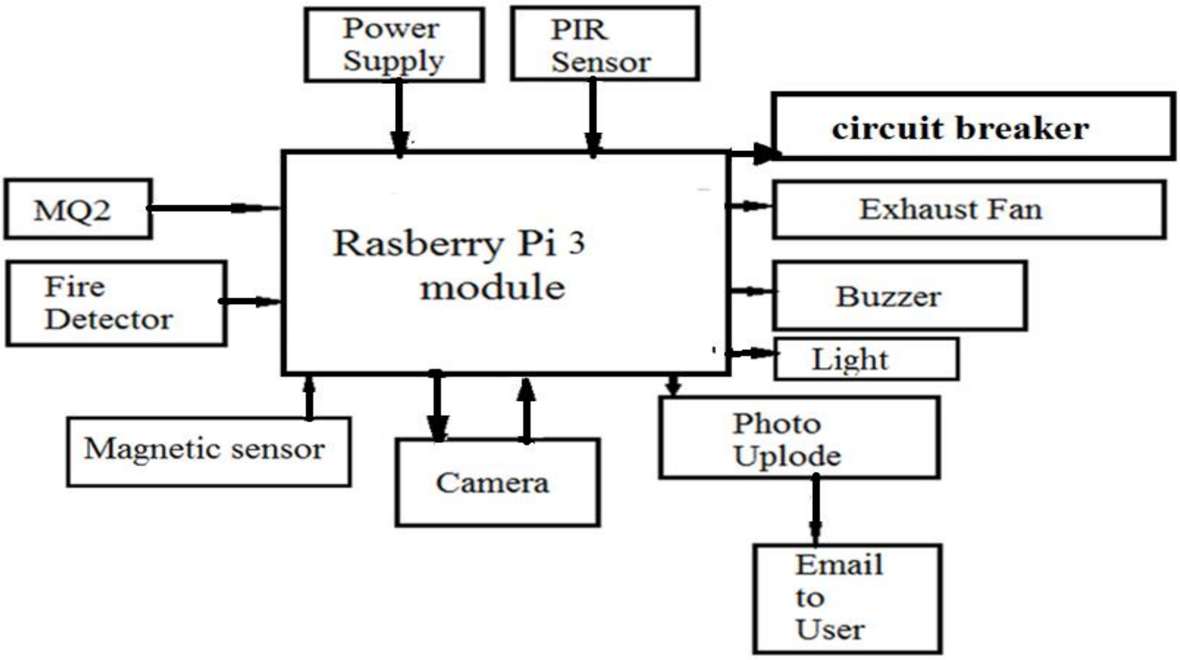

Figure 5: System block diagram

In our system which we are going to implement we will be taking various sensors for gas leakage, fire, motion detection, etc. and sending mail to the user according to conditions.

V CONCLUSION

This paper reviews the recent researches on IoT in home automation. We firstly introduce various work done from papers and found out the scope to improve the system then by comparison we have selected a module that is Raspberry Pi 3 having faster clock speed of 1.2 to 2 GHz and introduced our system.

REFRENCES

[1] Vikram.N, Harish K.S, Nihaal M.S,Raksha Umesh4, Shetty Aashik Ashok Kumar, 'A Low Cost Home Automation System Using Wi-Fi Based Wireless Sensor Network Incorporating Internet of Things(IoT)' 2017 IEEE 7th International Advance Computing Conference, (pg -174 to 178)

[2] Praveen Kumar, Umesh Chandra Pati ‘ IoT Based Monitoring and Control of Appliances for Smart Home’ IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India, (pg -1145 to 1150)

[3] Moataz Soliman, Tobi Abiodun, Tarek Hamouda, Jiehan Zhou, Chung-Horng Lung ‘Smart Home: Integrating Internet of Things with Web Services and Cloud Computing’ 2013 IEEE International Conference on Cloud Computing Technology and Science, (pg -317 to 320)

[4] Eleni Isa, Nicolas Sklavos ‘Smart Home Automation: GSM Security System Design & Implementation’ ResearchGate Conference Paper · January 2017, (pg -1 to 4)

[5] Ho-Kyeong Ra, Sangsoo Jeong, Hee Jung Yoon, and Sang Hyuk Son ‘WiP Abstract: SHAF: Framework for Smart Home Sensing and Actuation’, 2016 IEEE 22nd International Conference on Embedded and Real-Time Computing Systems and Applications, (pg - 258)

[6] T. Reichherzer, A. Mishra, E. Kalaimannan, N. Wilde ‘A Case Study on the Trade-Offs between Security, Scalability, and Efficiency in Smart Home Sensor Networks’, 2016 International Conference on Computational Science and Computational Intelligence, (pg -22 to 28)

[7] Li Da Xu, Senior Member, IEEE, Wu He, and Shancang Li, ‘Internet of Things in Industries: A Survey’ ,IEEE Transactions on Industrial Informatics, Vol. 10, No. 4, November 2014 (pg – 2233 to 2243)

[8] Vaibhav Sharma, Chirag Fatnani , Pranjal katara,Vishnu shankar , ‘Advanced Low-cost Security System Using Sensors, Arduino and GSM Communication Module’ **,**Proceedings of IEEE TechSym 2014 Satellite Conference, VIT University, 7th-8th March (pg – 12 & 13)

[9] Sean Dieter Tebje Kelly, Nagender Kumar Suryadevara, and Subhas Chandra Mukhopadhyay, Fellow, IEEE , ‘Towards the Implementation of IoT for Environmental Condition Monitoring in Homes’, IEEE Sensors Journal, Vol. 13, No. 10, October 2013(pg - 3846 to 3853)

[10] ZHANG Ying-conga, YU Jingb, ― A Study on the Fire IOT Development Strategy‖ , Int. J. of Safety and Security Eng., *Vol. 4*, No. 2 (2014),pp-135–142

[11] Keith D. Foote, an article on “A Brief History of the Internet of Things”, August 16, 2016, available on: http://www.dataversity.net/brief-history-internet-things/

[12] An article available on:https://www.i-scoop.eu/internet-of-things/