

POWER EFFICIENT SMART HOME WITH VOICE ASSISTANCE USING NODEMCU

Submitted in partial fulfillment of the requirements for
the award of
Bachelor of Engineering degree in Computer Science and Engineering

by

K MANI BHUSHAN (Reg. No. 37110425)

M RAMA KRISHNA (Reg. No. 37110413)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A" by NAAC

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600 119**

MARCH - 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work of **K MANI BHUSHAN (Reg. No. 37110425)** and **M RAMA KRISHNA (Reg. No.36110776)** who carried out the project entitled "**POWER EFFICIENT SMART HOME WITH VOICE ASSISTANCE USING NODEMCU**" under my supervision from **November 2020** to **March 2021**.

Internal Guide

Mr. Albert Mayan J

Head of the Department

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **K MANI BHUSHAN** hereby declare that the Project Report entitled “**POWER EFFICIENT SMART HOME WITH VOICE ASSISTANCE USING NODEMCU**” is done by me under the guidance of **Mr.ALBERT MAYAN J.**, Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean**, School of Computing, **Dr. S. Vigneswari, M.E., Ph.D., and Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department** of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Mr. ALBERT MAYAN J.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

- In this article, the optimized hardware with reduced cost an IOT based using a voice-commanded smart two-way automated system has been proposed and implemented. The ESP8266 NodeMCU micro-controller board is used as a central unit of this system. The system when used as smart Home Automation, initiated with a voice command over a smart phone given by the user using Google Assistant with a co-interfaced IFTTT (If This Then That) and the Blynk app platform which made this feature possible.
- The multichannel relay module for loads is interfaced with the central unit. The central unit processes the data as per the user input. When used for Agricultural monitoring the environmental parameters including soil moisture, air temperature and humidity (DHT11) has been analyzed and displayed on the OLED screen.
- Water flow was controlled using the water motor as per soil moisture threshold value. Hypertext transfer protocol based ESP8266 Wi-Fi based NodeMCU is routed to the Wi-Fi network and communicated with cloud storage (Thing speak) and IOT platform Blynk.
- The data from the sensors of the specified environmental parameters have been collected, monitored and then sent to the storage cloud and Blynk through Wi-Fi. The paper focuses on achieving automation of two different fields with a single hardware system.

TABLE OF CONTENTS

	ABSTRACT	v
	LIST OF FIGURES	viii
CHAPTER No.	TITLE	PAGE No.
1.	INTRODUCTION	3
2.	LITERATURE SURVEY	12
3.	EXISTING SYSTEM	10
	3.1 EXISTING SYSTEM	13
	3.2 PROPOSED SYSTEM	
	3.4 ADVANTAGES OF SYSTEM	14
4.	BLOCK DIAGRAM	15

5.	HARDWARE USED	15
6.	INTERNET OF THINGS	16
7.	SOFTWARE REQUIREMENTS	63
8	RESULT	80
9.	CONCLUSION	81
10.	REFERENCE	81

LIST OF FIGURES

FIGURE No.	FIGURE NAME	PAGE No.
4.	BLOCK DIAGRAM	15
6.1	ACTIVITY DIAGRAM	49
6.2	RELAY	55
6.3	DHT11 SENSOR	56
6.4	“START” AND “RESPONSE” SIGNALS	57
6.5	TIMING DIFFERENCE FOR TRANSMITTING “1s” AND “0s”	58
6.6	START,RESPONSE AND DATA SIGNALS IN SEQUENCE	58
6.7	SOIL MOISTURE SENSOR	63

CHAPTER: 1

INTRODUCTION:

- In recent decades, the lifestyle of people in the world is changing due to the growth of technology. Information technology plays a pivotal role in this revolution. After the advent of the smartphone, the usage of internet is increasing in quick succession. It leads to the growth information technology and also enables the dream of home automation comes true.
- In this fast-moving world, people are more attached to smart technologies. People need all to be automated and easily usable. Because of this, homes of this century become more and more automated due to the ease it provides. Even though people are lucky to have new smart devices, Most of the home automation system is a bit too expensive. However, not everyone is wealthy enough. Hence, the necessity to find a cost-efficient smart home technology for simple users keeps increasing. Most of these home automation systems aim at those who want luxury.
- This paper proposes such an inexpensive system that reduces the effort put in by the user to control a device manually. The network-based wireless home automation system is getting wide popularity because they give comfort, protection, and security towards any types of users.
- The aim of this project to develop a wireless home automation system controlled using multiple language voice commands. The system uses Google Assistant to communicate with the ESP32 and the users. The user's control the home appliances like light, fan, and smart door unlocking with English or Malayalam voice commands. The elder and a differently abled person find it hard to get used to these changing technologies, this helps them to control devices using their local languages. Integrating Google Assistant technology to home automation systems make the system also user-friendly and comfortable to operate.

Some of the method are listed below:

-) Home Appliances Control Using A Remote Control
-) Home Appliances Control Using DTMF

) Home Appliance Control Using Voice Assistance

Control using a Remote Control:

The lights, fans can be automatically turned on/off with the help of a remote where there will be a sensor instead of going near to a switch board and putting on/off the switch. Companies like Legrand and Gold Medal already started these kinds of control system and they are at present available in the market.

Home Appliances Control using DTMF:

In this method, the control of home appliances can be done even though when we are elsewhere just by using the DTMF tone generated when the user pushes mobile phone keypad buttons or when connected to a remote mobile.

Home Appliance Control Using Voice Assistance:

In this article, the optimized hardware with reduced cost an IOT based using a voice-commanded smart two-way automated system has been proposed and implemented. The ESP8266 NodeMCU micro-controller board is used as a central unit of this system. The system when used as smart Home Automation, initiated with a voice command over a smartphone given by the user using Google Assistant

Executive Summary

The world has seen tremendous growth in telecom technology during the last decade. As a result of this, a multitude of new applications of the Information & Communication Technologies have emerged and changed the way we live, work, play, interact and even think. This has created a lot of momentum in many spheres that impact our lives. Latest trend is Machine-to-Machine (M2M) communication / Internet of Things (IoT) which has led to a new world of possibilities and opportunities. Smart Home is one of the focus areas in this initiative as is evident from the large number of IoT / M2M enabled nodes being created for this sector. While 'Smart' inherently means 'connected' in IoT world, Smart Homes could have multiple meanings for different people and even different situations. A Smart Home is a user's private space and each user may have different needs. The users spend a significant amount of time at their homes and may have different expectations depending on their background, taste, affordability and availability of common services. A Smart Home is an aggregation of all the needs of its occupants while they are inside and also when they are not. Remote control, Security, surveillance, remote

monitoring of premises including monitoring those who are sick, young, elderly, etc are all requirements of users. In order to meet these requirements, an integration at the Application level and scalability at the cloud level are needed. With this kind of diverse backgrounds of users and their requirements and tastes, defining a common platform for a Smart Home is a rather challenging task. What could perhaps be possible is to create a generic platform that accepts multiple technologies as its inputs and somehow combines these inputs at the Home Gateway level and sends the information about various sensors from all the vendors on a single high speed communication link. This document of Telecom Engineering Centre describes M2M/IoT Enablement in Homes to take into account the diverse needs of users as stated in previous paragraphs. It introduces the subject with brief illustration of M2M communication and its framework for Smart Homes. The report has identified multiple use cases in Smart Homes e.g. Video monitoring of home, Security & Alarm, Door control, HVAC control, Smart lighting for efficiency, Controlling appliances through Smart phones, Solar lighting system, smart (electricity, water and gas) metering etc. The report identifies key challenges: lack of standards and non-availability of high speed and reliable Internet services, indigenous manufacturing, etc. Standards will allow for a level playing field for all participants that will benefit the customers. In the end, way forward has been suggested wherein action points on various aspects like adoption of standards, development of devices, certification mechanism etc. have been brought out. It may be mentioned here that the needs relevant to individual apartments, homes, and small establishments like shops or small scale industries operating from small buildings are covered in this document. Industrial buildings and large complexes are not in the scope of this document. The facility management services of apartment blocks are more similar to management of large complexes, hence are generally excluded from the scope

CHAPTER: 2

LITERATURE SURVEY:

J. Lertlakkhanakul, J.W.Choi and M. Y.Kim, Building Data Model and Simulation Platform for Spatial Interaction Management in Smart Home, Automation in Construction, Vol. 17, Issue 8, November 2008, pp. 948-957

The most important source of motivation in continuity of technological

developments is to upgrade human living standards. The technological development provides and increases human-beings' safety and comfort directly and indirectly. Developing technologies for this purpose directly affects the life standards by means of smart home systems design. It is possible to classify smart home systems into two as local and remote. In this study, a smart home automation system design was carried out by using Delta DVP28SV model PLC (Programmable Logic Controller). Smart home system can be controlled in two different ways either by any internet-connected device or an operator panel assembled on PLC. Control of the ventilation, lighting and security units in the smart home were carried out. Instantaneous states and variations of the smart home system which is feedback based are monitored and can be changed from the user interface prepared with the C# programming language. Unusual circumstances occurred in security units have been reported to the user with SMS (Short Message Service).

R. Al-Ali and M. AL-Rousan, Java-based Home Automation System, IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, May 2004,

Controlling the office and electronic gadgets through an Infrared remote control is now in general. But the same controlling tasks can be done easily. Primary motive of proposing the new system of hand gesture remote control is to remove the need to look in to the remote and to search for a specific key for specific function. This project proposed a novel system to control office through hand gesture as a remote control device. The system will referred to as Hand mote in this project we have proposed a Controlling the office and electronic gadgets through an Infrared remote control is now in general. But the same controlling tasks can be done more easily. Primary motive of proposing the new system of hand gesture remote control is to remove the need to look in to the hand held remote and to search for a specific key for specific function. This project proposed a novel system to control office through hand gesture as a remote control device. The system will referred to as Hand mote in this project. We are using Arduino. At first it will connect to office WIFI then the gesture is recognize ,after that the Authentication of user is done, Then the mobile is connected to office through Arduino. And access of particular device of floor is given to user

R. J. C. Nunes and J. C. M. Delgado, An Internet Application for Home Automation, 10th Mediterranean Eletro-technical Conference, MeleCon 2000, Vol. I. pp. 298-301

The IoT allows objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems. It results improved efficiency, accuracy and economic benefit in addition to reduced human intervention. On the other hand, IoT systems could also be responsible for performing actions, not just sensing the things. Intelligent Shopping systems, for example could monitor specific users purchasing habits in a store by tracking their specific mobile phones. Other applications that the Internet of Things can provide enabling extended home security features and home automation. This paper relates smart home or home automation which induce technology for home atmosphere which is usage to provide ease and protection to its occupant's .Whole system was based on a number of open source hardware and software so that the cost of building the system could be kept low. One of the goals while designing the system was to replace traditional personal computer in the system integration. There were quite a few options to choose from including the popular ESP8266 units. We chose the latter because it's economical and has tremendous support in the online community. Each of our sensor nodes was a combination of Arduino and DS18B20 was used as a sample data acquisition sensor

D. H. Stefanov and Z. Bien, The Smart House for Older Persons and Persons with Physical Disabilities: Structure, Technology Arrangements, and Perspectives, IEEE Transactions On Neural Systems And Rehabilitation Engineering, Vol. 12, No. 2, June 2004, pp. 228-250

This paper describes a robotic and automation system presently under development for studying home automation and indoor robotic technologies as well as new service scenarios based on these technologies. The system consists of remote users, a home automation server, and home automation equipment and home robots. Alarms and data are sent outside the home to helpers and caretakers. A remote user connects to the home server from the Internet to interact with the home and the people residing there. A demonstration system, that is open to the public, has been built in a model home

The server is connected to a Linet network (LINET, 2004). Linet (Light network) is a single pair automation network that allows up to 200 devices

connected to it with free topology. Currently the network comprises of magnetic switches on doors, movement sensors, a presence-sensing floor and a bed sensor, a connection to the stove and to some other electrical devices. The network has its own controller board that has some basic programmable features, but more complex functions have to be performed on the server. The server reads the network state through the LAN and if needed, will send control commands back to the Linet controller

C. Douligeris, Intelligent Home Systems, IEEE Communications Magazine, Vol. 31, Issue 10, October 1993, pp. 52-61

We discuss the concept of adaptive middleware for augmented living spaces, with the aim to provide a framework to systematically outfit homes with the flexible intelligence to cooperatively optimize their shared resources. To exemplify this concept, we discuss the EMISS test bed and platform for rapid design, simulation and deployment of wireless sensor networks for the “adaptive home” beyond off-the-shelf control mechanisms for networked home appliances. Based on a combination of web and object technology, the system offers location independent, user-friendly access to customized energy-aware home control, as well as the basic ambient intelligence to make a home adapt to user behavior and environmental constraint. However, despite a plethora of academic and industrial approaches to enrich homes with such capabilities, an adaptive middleware framework for characterizing the design and deployment of sensor network support for assistive living spaces is still lacking. Available solutions widely differ in implementation and capabilities. This paper fills the gap by discussing a basic methodology and platform to deploy network middleware to retrofit living spaces with adaptive intelligence and dynamic service quality provisioning, for example to regulate energy consumption based on user patterns and environmental measurements. Intelligent systems in a home environment receive information such as continuous feeds from a number of dispersed devices, typically sensors arranged in a sensor network. The information streams must be analyzed, communicated both internally and externally, and take configuration input from users to regulate device behavior. Newer developments in outfitting homes with powerful telematics intelligence catering to their dwellers’ critical living needs go beyond the basic premises of networked home appliances, and introduce challenges such as context-awareness, Quality-of-Service

support, and multi-device adaptation. Making homes intelligent, aware servants to their inhabitants has been a common theme in previous work on the home of the future. In contrast to control bus systems such as Lux mate or EIB, which use centralized control and lack intelligence, smart approaches include for example neural network support to anticipate user needs and conserve energy. In the wake of a new generation of ambient intelligence applications and services, programming and configuring home-embedded systems with respect to the physical properties is a major challenge. Major questions concern the placement of adaptive capabilities in intelligent environments to recognize users and their operational needs, predicting adjustments in real-time to these needs based on contextual knowledge, and allowing access to control services and features in an unobtrusive, yet tangible and secure manner. We argue that middleware, as the coordinative and reusable software “glue” residing between applications, the network protocol stack and underlying operating systems, should provide this adaptively. Other middleware architectures for smart homes have been proposed, with a different focus on platform independence

Y.-J. Mon, C.-M. Lin and I. J. Rudas, Wireless Sensor Network (WSN) Control for Indoor Temperature Monitoring, Acta Polytechnica Hungarica, Vol. 9, No. 6, 2012, pp. 17-28

The adaptive network fuzzy inference system (ANFIS)-based wireless sensor network (WSN) is designed to serve as a monitor of controller of an indoor air-conditioning system. The WSN comprises sensors to monitor the temperature of the indoor space and the ANFIS controller is used to control the fans in order to obtain energy-saving benefits. By using the application programming interface (API) of WSNs, many applications have been developed. The experimental results demonstrate that good data transference and control performance have been achieved. In this paper, an adaptive network fuzzy inference system (ANFIS)-based wireless sensor network (WSN) control system is developed. A reduction in energy consumption is the main challenge of the WSN. The IEEE 802.15.4/Zigbee standard has been proposed by the Zigbee Alliance to develop standards for cost-effective and low-power consumption WSNs. By using the lower cost, lower power consumption Zigbee WSN and efficient ANFIS controller, many control applications can be achieved through the network

E. N. Yilmaz, Education Set Design for Smart Home Applications, Computer Applications in Engineering Education, Vol. 19, Issue 4, December 2006, pp

The most important source of motivation in continuity of technological developments is to upgrade human living standards. The technological development provides and increases human-beings' safety and comfort directly and indirectly. Developing technologies for this purpose directly affects the life standards by means of smart home systems design. It is possible to classify smart home systems into two as local and remote. In this study, a smart home automation system design was carried out by using Delta DVP28SV model PLC (Programmable Logic Controller). Smart home system can be controlled in two different ways either by any internet-connected device or an operator panel assembled on PLC. Control of the ventilation, lighting and security units in the smart home were carried out. Instantaneous states and variations of the smart home system which is feedback based are monitored and can be changed from the user interface prepared with the C# programming language. Unusual circumstances occurred in security units have been reported to the user with SMS (Short Message Service).

N. Sriskanthan and Tan Karand. "Bluetooth Based Home Automation System". Journal of Microprocessors and Microsystems, Vol. 26, pp.281-289, 2002

The past decade has seen significant advancement in the field of consumer electronics. Various 'intelligent' appliances such as cellular phones, air-conditioners, home security devices, home theatres, etc. are set to realize the concept of a smart home. They have given rise to a Personal Area Network in home environment, where all these appliances can be interconnected and monitored using a single controller. Busy families and individuals with physical limitation represent an attractive market for home automation and networking. A wireless home network that does not incur additional costs of wiring would be desirable. Bluetooth technology, which has emerged in late 1990s, is an

ideal solution for this purpose. This paper describes an application of Bluetooth technology in home automation and networking environment. It proposes a network, which contains a remote, mobile host controller and several client modules (home appliances). The client modules communicate with the host controller through Bluetooth devices

E. Yavuz, B. Hasan, I. Serkan and K. Duygu. “Safe and Secure PIC Based Remote Control Application for Intelligent Home”. International Journal of Computer Science and Network Security, Vol. 7, No. 5, May 2007

In this paper, secure PIC based remote control system for intelligent houses has been presented. With this implemented system, it is possible to safely control electricity operated domestic devices by the help of public or mobile phones from any places all over the world. Developed remote control device has been optically and electrically isolated to secure the system. In addition the system implemented and introduced in this paper has pin-check algorithm in order to enlarge security. In this paper, pin-check supported safe, secure and easy use remote control PIC microcontroller, which has RISC architecture, based design has been introduced. Electrical operated domestic devices have been controlled by public or mobile phones using DTMF signals using this system the main principle of offered system operation. The central unit of this system is PIC based remote control circuit which will be called as controller. This controller detects the number of ringing, then decodes DTMF signal and then checks pin numbers which are entered. When the pin numbers have been entered correctly, the controller gives to right to control devices. Both pin numbers and orders to control appliance have been transmitted via telephone line or electromagnetic waves as DTMF signal.

Amul Jadhav, S. Anand, Nilesh Dhangare, K.S. Wagh “Universal Mobile Application Development (UMAD) On Home Automation” Marathwada Mitra Mandal’s Institute of Technology, University of Pune, India Network and Complex Systems ISSN 2224-610X (Paper) ISSN 2225-0603 (Online) Vol 2, No.2, 2012

At present scenario the market is flooded with many cell phones compatibility issues intended with Operating System and hardware’s, so the applications are not made in a manner to suite large mass. Till now the applications made

were targeted to a particular Operating System only which restricted their usability. With the limitations of above in mind there is a need of a universal mobile application development (UMAD) platform. So that an application can be developed in a universal XML format which can be easily ported to any other mobile devices. This paper presents the design and implementation of the Home automation system on one of the Operating System and creation of a unique XML document that can be placed over the server which can be adapted by any other mobile device without any platform issues. The XML format which controls the layout of the screen remains common, only the part which needs to be coded on every platform is the downloading of the XML file from the server and parsing it. This reduces a lot of coding effort as the design part is coded only once, and the same file can be used by every other platform. We have taken Home Automation system as our application, in which all the household devices such as Bulb, Fan, and AC etc. all are controlled by a smartphone which is connected to a server containing the XML file via an internet connection. Every change made by the user on the smartphone affects the data in the XML file of server, which thus helps in continuous updating of data and all other users get an updated Graphical User Interface. We have taken Home Automation as one of our application, but the same principle can be implemented in any other applications like Mobile Themes, Games etc.

Rana, Jitendra Rajendra and Pawar, Sunil N., Zigbee Based Home Automation (April 10, 2010). Available at SSRN: <http://ssrn.com/abstract=1587245> or <http://dx.doi.org/10.2139/ssrn.1587245>

Today we are living in 21st century where automation is playing important role in human life. Home automation allows us to control household appliances like light, door, fan, AC etc. It also provides home security and emergency system to be activated. Home automation not only refers to reduce human efforts but also energy saving and time efficiency. The main objective of home automation and security is to help handicapped and old aged people who will enable them to control home appliances and alert them in critical situations. This paper put forwards the design of home automation and security system using ARM7 LPC2148 board. The design is based on a standalone embedded system board ARM7 LPC2148 at home. Home appliances are connected to the ARM7 and communication is established between the ARM7 and ARM9

with Bluetooth device. The home appliances are connected to the input / output ports of the embedded system board and their status is passed to the ARM7. We would develop an authentication to the system for authorized person to access home appliances. The device with low cost and scalable to less modification to the core is much important. It presents the design and implementation of automation system that can monitor and control home appliances via ARM9 S3C2440A board

R.Piyare, M.Tazi “Bluetooth Based Home Automation System Using Cell Phone”, 2011 IEEE 15th International Symposium on Consumer Electronics

Smart homes refers to energy efficient, time saving includes reduces the human efforts. Commercial content distribution network (CDNs) has Video-on-demand (VOD) services for on-demand capacity provisioning on smart television (Home Automation). The content has full control and customization, so they prefer self-managed content infrastructure. The initial capital investment for physical infrastructure was so expensive and quite difficult for management. The objective of key providers was to reduce the server rental cost by accessing through the efficient and inexpensive ESP8266 chip to the cloud platforms on which dynamic server provisioning to reduce the server rental cost which was the key objective for content providers. In this paper we addressed the challenges of reducing the cost of accessing the cloud Platforms. We present the construction of ESP8266 with the Arduino or microcontroller are attached to get the smart television, where all our choice of videos can be stored and Retrieved at any time. Ad fruit, Electro dragon, Spark fun helps to get the chip. Through the software development kit (SDK) in ESP8266 that allow the chip to be programmed which remove the need of the microcontroller. Generally accessing cloud facility will produce high cost but in this paper gives the replacement of the accessing the cloud with the ESP8266 serial chip which operated in low power consumption with the low cost because it has the three configurable sleep modes

EXISTING SYSTEM:

- **Design and Realization of Home Appliances Control System Based on The Android Smartphone** present the information about the remote appliances control system based on the Android smart phone is designed and realized.
- **A user logs into the smart phone interface, and clicks the buttons gently to send message commands which will be transmitted to home information Centre through the GSM network. Then the PIC processor recognizes the specified command, and controls the home appliance switches in the wireless radio frequency manner to achieve remote control of appliances ultimately. Exploiting Bluetooth on android mobile devices for home security application present the information about mobile device has been integrated into our everyday life.**
- **Home automation and security are becoming increasingly prominent features on mobile devices the mobile device and security system communicates via Bluetooth because a short-range-only communication system was desired.**
- **With the help of android mobile we can control task such as locking the doors, turning on/off lights remotely.**

PROPOSED SYSTEM:

- **Concluding, in this system, an IOT based hardware system is proposed which is used for smart home automation and also for agricultural monitoring with the same single MCU hardware.**
- **Unlike the other trends in traditional IOT based automation, this paper mainly focuses on hardware optimization and energy efficiency. For other devices, separate micro-controllers are used for home automation or Agriculture monitoring thereby saving energy using just single hardware.**

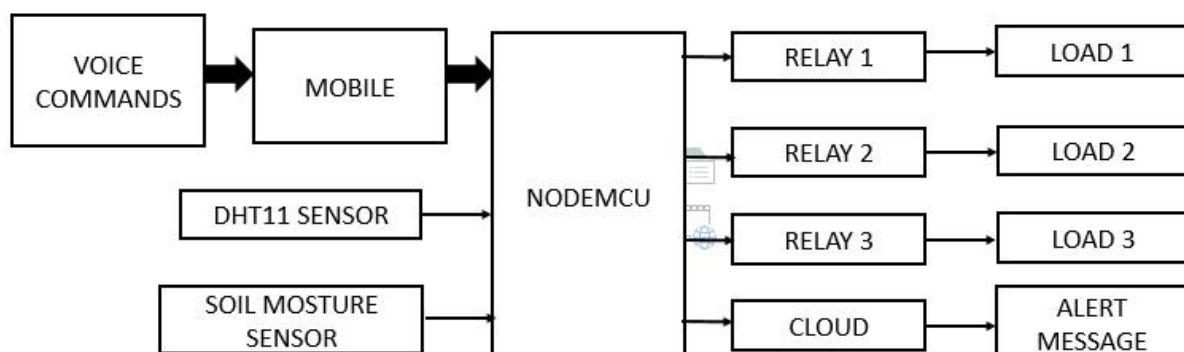
- **With easy user access and security, it would give a significant contribution to the advancement of IOT based automation systems.**

ADVANTAGES OF PROPOSED SYSTEM:

-) High secured
-) Long distance coverage
-) Real time controlling and monitoring
-) Control through mobile, pc and also the phablets
-) Low cost and expandable allowing a variety of devices to be controlled
-) Saves money and energy
-) All in one user friendly system
-) This system contain Raspberry pi as a controller so the system contain all the advantages of it.
-) This is noise free system.

CHAPTER: 4

BLOCK DIAGRAM:



CHAPTER: 5

HARDWARE USED:

-) Nodemcu
-) DHT11 sensor
-) Soil moisture sensor
-) 4-CHANNEL RELAY
-) HOME APPLIANCE
-) POWER SUPPLY

SOFTWARE USED:

Arduino ide
Arduino c

CHAPTER: 6**IOT:****Internet of things:**

The Internet of things (IOT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IOT-GSI) defined the IOT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" and for these purposes a "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks". The IOT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting

in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IOT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IOT will consist of about 30 billion objects by 2020. Typically, IOT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a smart grid, and expanding to areas such as smart cities. "Things", in the IOT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring, or field operation devices that assist fire fighters in search and rescue operations. Legal scholars suggest regarding "Things" as an "inextricable mixture of hardware, software, data and service". These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include home automation (also known as smart home devices) such as the control and automation of lighting, heating (like smart thermostat), ventilation, air conditioning (HVAC) systems, and appliances such as washer/dryers, robotic vacuums, air purifiers, ovens, or refrigerators/freezers that use Wi-Fi for remote monitoring. As well as the expansion of Internet-connected automation into a plethora of new application areas, IOT is also expected to generate large amounts of data from diverse

locations, with the consequent necessity for quick aggregation of the data, and an increase in the need to index, store, and process such data more effectively. IOT is one of the platforms of today's Smart City, and Smart Energy Management Systems

HISTORY

As of 2016, the vision of the Internet of things has evolved due to a convergence of multiple technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems. This means that the traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things (IOT). The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's seminal 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IOT. In 1994 Reza Raji described the concept in IEEE Spectrum as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1996 several companies proposed solutions like Microsoft's at Work or Novell's NEST. However, only in 1999 did the field start gathering momentum. Bill Joy envisioned Device to Device (D2D) communication as part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999. The concept of the Internet of things became popular in 1999, through the Auto-ID Centre at MIT and related

market-analysis publications. Radio-frequency identification (RFID) was seen by Kevin Ashton (one of the founders of the original Auto-ID Centre) as a prerequisite for the Internet of things at that point. Ashton prefers the phrase "Internet for Things. If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Besides using RFID, the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes and digital watermarking. In its original interpretation, one of the first consequences of implementing the Internet of things by equipping all objects in the world with minuscule identifying devices or machine-readable identifiers would be to transform daily life. For instance, instant and ceaseless inventory control would become ubiquitous. A person's ability to interact with objects could be altered remotely based on immediate or present needs, in accordance with existing end-user agreements. For example, such technology could grant motion-picture publishers much more control over end-user private devices by remotely enforcing copyright restrictions and digital rights management, so the ability of a customer who bought a Blu-ray disc to watch the movie could become dependent on the copyright holder's decision, similar to Circuit City's failed DIVX.

APPLICATIONS:

According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 20.8 billion devices on the Internet of things by 2020. ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of things by 2020. As per a 2014 survey and study done by Pew Research Internet Project, a large majority of the technology experts and engaged Internet users who responded—83 percent—agreed with the notion that the Internet/Cloud of Things, embedded and wearable computing (and the corresponding dynamic systems will have widespread and beneficial effects by 2025. As such, it is clear that the IOT will consist of a very large number of devices being connected to the Internet. In an active

move to accommodate new and emerging technological innovation, the UK Government, in their 2015 budget, allocated £40,000,000 towards research into the Internet of things. The former British Chancellor of the Exchequer George Osborne, posited that the Internet of things is the next stage of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances. The ability to network embedded devices with limited CPU, memory and power resources means that IOT finds applications in nearly every field. [48] Such systems could be in charge of collecting information in settings ranging from natural ecosystems to buildings and factories, thereby finding applications in fields of environmental sensing and urban planning. On the other hand, IOT systems could also be responsible for performing actions, not just sensing things. Intelligent shopping systems, for example, could monitor specific users' purchasing habits in a store by tracking their specific mobile phones. These users could then be provided with special offers on their favourite products, or even location of items that they need, which their fridge has automatically conveyed to the phone. Additional examples of sensing and actuating are reflected in applications that deal with heat, water, electricity and energy management, as well as cruise-assisting transportation systems. Other applications that the Internet of things can provide is enabling extended home security features and home automation. The concept of an "Internet of living things" has been proposed to describe networks of biological sensors that could use cloud-based analyses to allow users to study DNA or other molecules. However, the application of the IOT is not only restricted to these areas. Other specialized use cases of the IOT may also exist. An overview of some of the most prominent application areas is provided here.

ENVIRONMENTAL MONITORING :

Environmental monitoring applications of the IOT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats. Development of resource constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IOT devices in this application typically span a large geographic area and can also be mobile. It has been argued that the standardization IOT brings to wireless sensing will revolutionize this area.

INFRASTRUCTURE MANAGEMENT:

Monitoring and controlling operations of urban and rural infrastructures like bridges, railway tracks, on- and offshore- wind-farms is a key application of the IOT. The IOT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities. IOT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IOT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IOT.

MANUFACTURING NETWORK:

Control and management of manufacturing equipment, asset and situation

management, or manufacturing process control bring the IOT within the realm of industrial applications and smart manufacturing as well. The IOT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together. Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IOT. But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Smart industrial management systems can also be integrated with the Smart Grid, thereby enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors. The National Science Foundation established an Industry/University Cooperative Research Centre on intelligent maintenance systems (IMS) in 2001 with a research focus to use IOT-based predictive analytics technologies to monitor connected machines and to predict machine degradation, and further to prevent potential failures. The vision to achieve near-zero breakdown using IOT-based predictive analytics led the future development of e-manufacturing and e-maintenance activities. The term IIOT (Industrial Internet of Things) is often encountered in the manufacturing industries, referring to the industrial subset of the IOT. IIOT in manufacturing could generate so much business value that it will eventually lead to the fourth industrial revolution, so the so-called Industry 4.0. It is estimated that in the future, successful companies will be able to increase their revenue through Internet of things by creating new business models and improve productivity, exploit analytics for innovation, and transform workforce. The potential of growth by implementing IIOT will generate \$12 trillion of global GDP by 2030 while connectivity and data acquisition are imperative for IIOT, they should not

be the purpose, rather the foundation and path to something bigger. Among all the technologies, predictive maintenance is probably a relatively "easier win" since it is applicable to existing assets and management systems. The objective of intelligent maintenance systems is to reduce unexpected downtime and increase productivity. And to realize that alone would generate around up to 30% over total maintenance costs. Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. Cyber-physical systems can be designed by following the 5C (connection, conversion, cyber, cognition, configuration, architecture), and it will transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes. An IOT-enabled intelligent system of such cases has been demonstrated by the NSF Industry/University Collaborative Research Centre for Intelligent Maintenance Systems (IMS) at University of Cincinnati on a band saw machine in IMTS 2014 in Chicago. Band saw machines are not necessarily expensive, but the band saw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics, it can be only determined by experience when the band saw belt will actually break. The developed prognostics system will be able to recognize and monitor the degradation of band saw belts even if the condition is changing, so that users will know in near real time when is the best time to replace band saw. This will significantly improve user experience and operator safety, and save costs on replacing band saw belts before they actually break. The developed analytical algorithms were realized on a cloud server, and was made accessible via the Internet and on mobile devices.

ENERGY MANAGEMENT :

Integration of sensing and actuation systems, connected to the Internet, is

likely to optimize energy consumption as a whole. It is expected that IOT devices will be integrated into all forms of energy consuming devices (switches, power outlets, bulbs, televisions, etc.) and be able to communicate with the utility supply company in order to effectively balance power generation and energy usage. Such devices would also offer the opportunity for users to remotely control their devices, or centrally manage them via a cloud based interface, and enable advanced functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). Besides home based energy management, the IOT is especially relevant to the Smart Grid since it provides systems to gather and act on energy and power-related information in an automated fashion with the goal to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Using advanced metering infrastructure (AMI) devices connected to the Internet backbone, electric utilities can not only collect data from end-user connections, but also manage other distribution automation devices like transformers and re closers.

MEDICAL AND HEALTHCARE:

IOT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fit bit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. Other consumer devices to encourage healthy

living, such as, connected scales or wearable heart monitors, are also a possibility with the IOT. More and more end-to-end health monitoring IOT platforms are coming up for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

BUILDING AND HOME AUTOMATION:

IOT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation and building automation systems. In this context, three main areas are being covered in literature: The integration of the internet with building energy management systems in order to create energy efficient and IOT driven “smart buildings”. The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviours. The integration of smart devices in the built environment and how they might be used in future applications.

TRANSPORTATION:

The IOT can assist in integration of communications, control, and information processing across various transportation systems. Application of the IOT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter and intra vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance.

METROPOLITAN SCALE DEPLOYMENTS :

There are several planned or ongoing large-scale deployments of the IOT, to enable better management of cities and systems. For example, Songdo, South Korea, the first of its kind fully equipped and wired smart city, is near

completion. Nearly everything in this city is planned to be wired, connected and turned into a constant stream of data that would be monitored and analysed by an array of computers with little, or no human intervention. Another application is a currently undergoing project in Santander, Spain. For this deployment, two approaches have been adopted. This city of 180,000 inhabitants, has already seen 18,000 city application downloads for their smartphones. This application is connected to 10,000 sensors that enable services like parking search, environmental monitoring, and digital city agenda among others. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behaviour that aims at maximizing the impact of each notification. Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City; work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California; and smart traffic management in western Singapore. French company, Sigfox, commenced building an ultra-narrowband wireless data network in the San Francisco Bay Area in 2014, the first business to achieve such a deployment in the U.S. It subsequently announced it would set up a total of 4000 base stations to cover a total of 30 cities in the U.S. by the end of 2016, making it the largest IOT network coverage provider in the country thus far. Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7. The network was designed and engineered by Fluidmesh Networks, a Chicago-based company developing wireless networks for critical applications. The NYWW network is currently providing coverage on the Hudson River, East River, and Upper New York Bay. With the wireless network in place, NY Waterway is able to take control of its fleet and passengers in a way that was not previously possible. New applications can include security, energy and fleet management, digital signage, public Wi-Fi,

paperless ticketing and others.

CONSUMER APPLICATION:

A growing portion of IOT devices are created for consumer use. Examples of consumer applications include connected car, entertainment, residences and smart homes, wearable technology, quantified self, connected health, and smart retail. Consumer IOT provides new opportunities for user experience and interfaces. Some consumer applications have been criticized for their lack of redundancy and their inconsistency, leading to a popular parody known as the “Internet of Shit.” Companies have been criticized for their rush into IOT, creating devices of questionable value, and not setting up stringent security standards.

UNIQUE ADDRESSABILITY OF THINGS:

The original idea of the Auto-ID Centre is based on RFID-tags and unique identification through the Electronic Product Code however this has evolved into objects having an IP address or URI. An alternative view, from the world of the Semantic Web focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralized servers acting for their human owners.

Integration with the Internet implies that devices will use an IP address as a unique identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IOT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required. Internet of things devices additionally will benefit from the stateless address auto-configuration present in IPv6, as it reduces the configuration overhead on the hosts, and the IETF 6LoWPAN header compression. To a large extent, the future of the Internet of things will not be

possible without the support of IPv6; and consequently the global adoption of IPv6 in the coming years will be critical for the successful development of the IOT in the future. A combination of these ideas can be found in the current GS1/EPC global EPC Information Services (EPCIS) specifications. This system is being used to identify objects in industries ranging from aerospace to fast moving consumer products and transportation logistics.

TRENDS AND CHARACTERISTICS

INTELLIGENCE:

Ambient intelligence and autonomous control are not part of the original concept of the Internet of things. Ambient intelligence and autonomous control do not necessarily require Internet structures, either. However, there is a shift in research to integrate the concepts of the Internet of things and autonomous control, with initial outcomes towards this direction considering objects as the driving force for autonomous IOT. In the future the Internet of things may be a non-deterministic and open network in which auto-organized or intelligent entities (Web services, SOA components), virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments. Autonomous behaviour through the collection and reasoning of context information as well as the objects ability to detect changes in the environment, faults affecting sensors and introduce suitable mitigation measures constitute a major research trend, clearly needed to provide credibility to the IOT technology. Modern IOT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation but more sophisticated forms of intelligence are requested to permit sensor units to be deployed in real environments.

ARCHITECTURE:

The system will likely be an example of event-driven architecture, bottom-up made (based on the context of processes and operations, in real-time) and

will consider any subsidiary level. Therefore, model driven and functional approaches will coexist with new ones able to treat exceptions and unusual evolution of processes (multi-agent systems, B-ADSC, etc.). In an Internet of things, the meaning of an event will not necessarily be based on a deterministic or syntactic model but would instead be based on the context of the event itself: this will also be a semantic web. Consequently, it will not necessarily need common standards that would not be able to address every context or use: some actors (services, components, avatars) will accordingly be self-referenced and, if ever needed, adaptive to existing common standards (predicting everything would be no more than defining a "global finality" for everything that is just not possible with any of the current top-down approaches and standardizations). Building on top of the Internet of things, the web of things is an architecture for the application layer of the Internet of things looking at the convergence of data from IOT devices into Web applications to create innovative use-cases. In order to program and control the flow of information in the Internet of things, a predicted architectural direction is being called BPM Everywhere which is a blending of traditional process management with process mining and special capabilities to automate the control of large numbers of coordinated devices.

NETWORK ARCHITECTURE:

The Internet of things requires huge scalability in the network space to handle the surge of devices. IETF 6LoWPAN would be used to connect devices to IP networks. With billions of devices being added to the Internet space, IPv6 will play a major role in handling the network layer scalability. IETF's Constrained Application Protocol, Zero MQ, and MQTT would provide lightweight data transport. "MQ" in "MQTT" came from IBM's MQ Series message queuing product line. Fog computing is a viable alternative to prevent such large burst of data flow through Internet. The edge devices' computation power can be used to analyse and process data, thus providing easy real time scalability.

COMPLEXITY:

In semi-open or closed loops (i.e. value chains, whenever a global finality can be settled) IOT will often be considered and studied as a complex system due to the huge number of different links, interactions between autonomous actors, and its capacity to integrate new actors. At the overall stage (full open loop) it will likely be seen as a chaotic environment (since systems always have finality). As a practical approach, not all elements in the Internet of things run in a global, public space. Subsystems are often implemented to mitigate the risks of privacy, control and reliability. For example, Domestic Robotics (Domotics) running inside a smart home might only share data within and be available via a local network.

Size considerations

The Internet of things would encode 50 to 100 trillion objects, and be able to follow the movement of those objects. Human beings in surveyed urban environments are each surrounded by 1000 to 5000 trackable objects.

Space considerations

In the Internet of things, the precise geographic location of a thing—and also the precise geographic dimensions of a thing—will be critical. Therefore, facts about a thing, such as its location in time and space, have been less critical to track because the person processing the information can decide whether or not that information was important to the action being taken, and if so, add the missing information (or decide to not take the action). (Note that some things in the Internet of things will be sensors, and sensor location is usually important. The GeoWeb and Digital Earth are promising applications that become possible when things can become organized and connected by location. However, the challenges that remain include the constraints of variable spatial scales, the need to handle massive amounts of data, and an indexing for fast search and neighbour operations. In the Internet of things, if things are able to take actions on their own initiative, this human-centric

mediation role is eliminated. Thus, the time-space context that we as humans take for granted must be given a central role in this information ecosystem. Just as standards play a key role in the Internet and the Web, geospatial standards will play a key role in the Internet of things.

Sectors

There are three core sectors of the IOT: enterprise, home, and government, with the Enterprise Internet of Things (EIOT) being the largest of the three. By 2019, the EIOT sector is estimated to account for nearly 40% or 9.1 billion devices.

SOLUTION TO "BASKET OF REMOTES"

According to the CEO of Cisco, the commercial opportunity for "connected products ranging from cars to household goods" is expected to be a \$USD 19 trillion. Many IOT devices have a potential to take a piece of this market. Jean-Louis Gasee (Apple initial alumni team, and BeOS co-founder) has addressed this topic in an article on Monday Note, where he predicts that the most likely problem will be what he calls the "basket of remotes" problem, where we'll have hundreds of applications to interface with hundreds of devices that don't share protocols for speaking with one another. There are multiple approaches to solve this problem, one of them called the "predictive interaction", where cloud or fog based decision makers will predict the user's next action and trigger some reaction. For user interaction, new technology leaders are joining forces to create standards for communication between devices. While AllJoyn alliance is composed of the top 20 World technology leaders, there are also big companies that promote their own protocol like CCF from Intel. Manufacturers are becoming more conscious of this problem, and many companies have begun releasing their devices with open APIs. Many of these APIs are used by smaller companies looking to take advantage of quick integration.

FRAMEWORKS

-) Thread – Network protocol based on the IEEE 802.15.4 standard, similar to Zigbee, providing IPv6 addressing.
-) Transport Layer Security (network protocol) | TLS – Network security protocol.
-) Wi-Fi – Widely used technology for local area networking based on the IEEE 802.11 standard, where devices may communicate through a shared access point.
-) Wi-Fi Direct – Variant of the Wi-Fi standard for peer-to-peer communication, eliminating the need for an access point.
-) Z-Wave – Communication protocol providing short-range, low-latency data transfer at rates and power consumption lower than Wi-Fi. Used primarily for home automation.
-) Zigbee – Communication protocols for personal area networking based on the IEEE 802.15.4 standard, providing low power consumption, low data rate, low cost, and high throughput.

MEDIUM-RANGE WIRELESS:

-) Hallow – Variant of the Wi-Fi standard providing extended range for low-power communication at a lower data rate.
-) LTE-Advanced – High-speed communication specification for mobile networks. Provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency.

LONG-RANGE WIRELESS:

-) Low-power wide-area networking (LPWAN) – Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission.
-) Very small aperture terminal (VSAT) – Satellite communication technology using small dish antennas for narrowband and broadband data.

WIRED:

-) Ethernet – General purpose networking standard using twisted pair and fibre optic links in conjunction with hubs or switches.
-) Multimedia over Coax Alliance (MOCA) – Specification enabling whole-home distribution of high definition video and content over existing coaxial cabling.
-) Power-line communication (PLC) – Communication technology using electrical wiring to carry power and data. Specifications such as Home Plug utilize PLC for networking IOT devices.

SIMULATION:

IOT modelling and simulation (and emulation) is typically carried out at the design stage before deployment of the network. Network simulators like OPNET, Net Sim and NS2 can be used to simulate IOT networks. Digital Twins may also be implemented to produce updates on the status and health of an asset, based upon sensor readings integrated with a computational model of the asset.

POLITICS AND CIVIC ENGAGEMENT:

Some scholars and activists argue that the IOT can be used to create new models of civic engagement if device networks can be open to user control and interoperable platforms. Philip N. Howard, a professor and author, writes that political life in both democracies and authoritarian regimes will be shaped by the way the IOT will be used for civic engagement. For that to happen, he argues that any connected device should be able to divulge a list of the "ultimate beneficiaries" of its sensor data and that individual citizens should be able to add new organizations to the beneficiary list. In addition, he argues that civil society groups need to start developing their IOT strategy for making use of data and engaging with the public.

GOVERNMENT REGULATION ON IOT:

One of the key drivers of the IOT is data. The success of the idea of connecting devices to make them more efficient is dependent upon access to and storage & processing of data. For this purpose, companies working on

IOT collect data from multiple sources and store it in their cloud network for further processing. This leaves the door wide open for privacy and security dangers and single point vulnerability of multiple systems. The other issues pertain to consumer choice and ownership of data and how it is used. Presently the regulators have shown more interest in protecting the first three issues identified above. Current regulatory environment: A report published by the Federal Trade Commission (FTC) in January 2015 made the following three recommendations:

-) Data security – At the time of designing IOT companies should ensure that data collection, storage and processing would be secure at all times. Companies should adopt a “defence in depth” approach and encrypt data at each stage.
-) Data consent – users should have a choice as to what data they share with IOT companies and the users must be informed if their data gets exposed.
-) Data minimization – IOT companies should collect only the data they need and retain the collected information only for a limited time.

However, the FTC stopped at just making recommendations for now. According to an FTC analysis, the existing framework, consisting of the FTC Act, the Fair Credit Reporting Act, and the Children’s Online Privacy Protection Act, along with developing consumer education and business guidance, participation in multi stake holder efforts and advocacy to other agencies at the federal, state and local level, is sufficient to protect consumer rights.

A resolution passed by the Senate in March 2015, is already being considered by the Congress. This resolution recognized the need for formulating a National Policy on IOT and the matter of privacy, security and spectrum. Furthermore, to provide an impetus to the IOT ecosystem, in March 2016, a bipartisan group of four Senators proposed a bill, The Developing Innovation and Growing the Internet of Things (DIGIT) Act, to direct the Federal Communications Commission to assess the need for more spectrum to

connect IOT devices

Several standards for the IOT industry are actually being established relating to automobiles because most concerns arising from use of connected cars apply to healthcare devices as well. In fact, the National Highway Traffic Safety Administration (NHTSA) is preparing cyber security guidelines and a database of best practices to make automotive computer systems more secure.

CRITICISM AND CONTROVERSIES:

PLATFORM FRAGMENTATION:

IOT suffers from platform fragmentation and lack of technical standards a situation where the variety of IOT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications that work consistently between different inconsistent technology ecosystems hard. Customers may be hesitant to bet their IOT future on a proprietary software or hardware devices that uses proprietary protocols that may fade or become difficult to customize and interconnect. IOT amorphous computing nature is also a problem for security, since patches to bugs found in the core operating system often do not reach users of older and lower-price devices. One set of researchers say that the failure of vendors to support older devices with patches and updates leaves more than 87% of active devices vulnerable.

PRIVACY, AUTONOMY, AND CONTROL:

Philip N. Howard, a professor and author, writes that the Internet of things offers immense potential for empowering citizens, making government transparent, and broadening information access. Howard cautions, however, that privacy threats are enormous, as is the potential for social control and political manipulation. Concerns about privacy have led many to consider the possibility that big data infrastructures such as the Internet of things and Data Mining are inherently incompatible with privacy. Writer Adam Greenfield

claims that these technologies are not only an invasion of public space but are also being used to perpetuate normative behaviour, citing an instance of billboards with hidden cameras that tracked the demographics of passers-by who stopped to read the advertisement. The Internet of Things Council compared the increased prevalence of digital surveillance due to the Internet of things to the conceptual panopticon described by Jeremy Bentham in the 18th Century. The assertion was defended by the works of French philosophers Michel Foucault and Gilles Deleuze. In *Discipline and Punish: The Birth of the Prison* Foucault asserts that the panopticon was a central element of the discipline society developed during the Industrial Era. Foucault also argued that the discipline systems established in factories and school reflected Bentham's vision of panopticism. In his 1992 paper "Postscripts on the Societies of Control," Deleuze wrote that the discipline society had transitioned into a control society, with the computer replacing the panopticon as an instrument of discipline and control while still maintaining the qualities similar to that of panopticism.

The privacy of households could be compromised by solely analyzing smart home network traffic patterns without dissecting the contents of encrypted application data, yet a synthetic packet injection scheme can be used to safely overcome such invasion of privacy. Peter-Paul Verbeek, a professor of philosophy of technology at the University of Twente, Netherlands, writes that technology already influences our moral decision making, which in turn affects human agency, privacy and autonomy. He cautions against viewing technology merely as a human tool and advocates instead to consider it as an active agent. Justin Brookman, of the Centre for Democracy and Technology, expressed concern regarding the impact of IOT on consumer privacy, saying that "There are some people in the commercial space who say, 'Oh, big data — well, let's collect everything, keep it around forever, we'll pay for somebody to think about security later.' The question is whether we want to have some

sort of policy framework in place to limit that." Tim O'Reilly believes that the way companies sell the IOT devices on consumers are misplaced, disputing the notion that the IOT is about gaining efficiency from putting all kinds of devices online and postulating that "IOT is really about human augmentation. The applications are profoundly different when you have sensors and data driving the decision-making." Editorials at WIRED have also expressed concern, one stating "What you're about to lose is your privacy. Actually, it's worse than that. You aren't just going to lose your privacy, you're going to have to watch the very concept of privacy be rewritten under your nose." The American Civil Liberties Union (ACLU) expressed concern regarding the ability of IOT to erode people's control over their own lives. The ACLU wrote that "There's simply no way to forecast how these immense powers – disproportionately accumulating in the hands of corporations seeking financial advantage and governments craving ever more control – will be used. Chances are big data and the Internet of Things will make it harder for us to control our own lives, as we grow increasingly transparent to powerful corporations and government institutions that are becoming more opaque to us." In response to rising concerns about privacy and smart technology, in 2007 the British Government stated it would follow formal Privacy by Design principles when implementing their smart metering program. The program would lead to replacement of traditional power meters with smart power meters, which could track and manage energy usage more accurately. However the British Computer Society is doubtful these principles were ever actually implemented. In 2009 the Dutch Parliament rejected a similar smart metering program, basing their decision on privacy concerns. The Dutch program later revised and passed in 2011.

DATA STORAGE AND ANALYTICS:

A challenge for producers of IOT applications is to clean, process and interpret the vast amount of data which is gathered by the sensors. There is a

solution proposed for the analytics of the information referred to as Wireless Sensor Networks. These networks share data among sensor nodes that are send to a distributed system for the analytics of the sensory data. Another challenge is the storage of this bulk data. Depending on the application there could be high data acquisition requirements which in turn lead to high storage requirements. Currently the internet is already responsible for 5% of the total energy generated and this consumption will increase significantly when we start utilizing applications with multiple embedded sensors.

SECURITY:

Concerns have been raised that the Internet of things is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary. Most of the technical security issues are similar to those of conventional servers, workstations and smartphones, but the firewall, security update and anti-malware systems used for those are generally unsuitable for the much smaller, less capable, IOT devices. According to the Business Insider Intelligence Survey conducted in the last quarter of 2014, 39% of the respondents said that security is the biggest concern in adopting Internet of things technology. In particular, as the Internet of things spreads widely, cyber-attacks are likely to become an increasingly physical (rather than simply virtual) threat. In a January 2014 article in Forbes, cyber-security columnist Joseph Steinberg listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and trunk releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the on-board network. In some cases, vehicle computer systems are Internet-connected, allowing them to be exploited remotely. By 2008 security researchers had shown the ability to remotely control pacemakers without

authority. Later hackers demonstrated remote control of insulin pumps and implantable cardioverter defibrillators. David Pogue wrote that some recently published reports about hackers remotely controlling certain functions of automobiles were not as serious as one might otherwise guess because of various mitigating circumstances; such as the bug that allowed the hack having been fixed before the report was published, or that the hack required security researchers having physical access to the car prior to the hack to prepare for it. The U.S. National Intelligence Council in an unclassified report maintains that it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers... An open market for aggregated sensor data could serve the interests of commerce and security no less than it helps criminals and spies identify vulnerable targets. Thus, massively parallel sensor fusion may undermine social cohesion, if it proves to be fundamentally incompatible with Fourth-Amendment guarantees against unreasonable search." In general, the intelligence community views the Internet of things as a rich source of data. As a response to increasing concerns over security, the Internet of Things Security Foundation (IOTSF) was launched on 23 September 2015. IOTSF has a mission to secure the Internet of things by promoting knowledge and best practice. Its founding board is made from technology providers and telecommunications companies including BT, Vodafone, Imagination Technologies and Pen Test Partners. In addition, large IT companies are continuously developing innovative solutions to ensure the security for IOT devices. As per the estimates from KBV Research, the overall IOT security market would grow at 27.9% rate during 2016-2022 as a result of growing infrastructural concerns and diversified usage of Internet of things. In 2016, a distributed denial of service attack powered by Internet of things devices running the Mirai malware took down a DNS provider and major web sites.

DESIGN:

Given widespread recognition of the evolving nature of the design and management of the Internet of things, sustainable and secure deployment of IOT solutions must design for "anarchic scalability." Application of the concept of anarchic scalability can be extended to physical systems (i.e. controlled real-world objects), by virtue of those systems being designed to account for uncertain management futures. This "hard anarchic scalability" thus provides a pathway forward to fully realize the potential of Internet of things solutions by selectively constraining physical systems to allow for all management regimes without risking physical failure. Brown University computer scientist Michael Littman has argued that successful execution of the Internet of things requires consideration of the interface's usability as well as the technology itself. These interfaces need to be not only more user-friendly but also better integrated: "If users need to learn different interfaces for their vacuums, their locks, their sprinklers, their lights, and their coffeemakers, it's tough to say that their lives have been made any easier."

ENVIRONMENTAL SUSTAINABILITY IMPACT:

A concern regarding Internet of things technologies pertains to the environmental impacts of the manufacture, use, and eventual disposal of all these semiconductor-rich devices. Modern electronics are replete with a wide variety of heavy metals and rare-earth metals, as well as highly toxic synthetic chemicals. This makes them extremely difficult to properly recycle. Electronic components are often incinerated or placed in regular landfills. Furthermore, the human and environmental cost of mining the rare-earth metals that are integral to modern electronic components continues to grow. With production of electronic equipment growing globally yet little of the metals (from end-of-life equipment) are being recovered for reuse, the environmental impacts can be expected to increase. Also, because the concept of Internet of things entails adding electronics to mundane devices (for example, simple light switches), and because the major driver for replacement of electronic

components is often technological obsolescence rather than actual failure to function, it is reasonable to expect that items that previously were kept in service for many decades would see an accelerated replacement cycle if they were part of the IOT. For example, a traditional house built with 30 light switches and 30 electrical outlets might stand for 50 years, with all those components still original at the end of that period. But a modern house built with the same number of switches and outlets set up for IOT might see each switch and outlet replaced at five-year intervals, in order to keep up to date with technological changes. This translates into a ten-fold increase in waste requiring disposal.

INTENTIONAL OBSOLESCENCE OF DEVICES:

The Electronic Frontier Foundation has raised concerns that companies can use the technologies necessary to support connected devices to intentionally disable or "brick" their customers' devices via a remote software update or by disabling a service necessary to the operation of the device. In one example, home automation devices sold with the promise of a "Lifetime Subscription" were rendered useless after Nest Labs acquired Revolv and made the decision to shut down the central servers the Revolv devices had used to operate. As Nest is a company owned by Alphabet (Google's parent company), the EFF argues this sets a "terrible precedent for a company with ambitions to sell self-driving cars, medical devices, and other high-end gadgets that may be essential to a person's livelihood or physical safety." Owners should be free to point their devices to a different server or collaborate on improved software. But such action violates the United States DMCA section 1201, which only has an exemption for "local use". This forces tinkerers who want to keep using their own equipment into a legal grey area. EFF thinks buyers should refuse electronics and software that prioritize the manufacturer's wishes above their own. Examples of post-sale manipulations

include Google Nest Revolv, disabled privacy settings on Android, Sony disabling Linux on PlayStation 3, and enforced EULA on Wii U.

CONFUSING TERMINOLOGY:

Kevin Lonergan at Information Age, a business-technology magazine, has referred to the terms surrounding IOT as a “terminology zoo”. The lack of clear terminology is not “useful from a practical point of view” and a “source of confusion for the end user”. A company operating in the IOT space could be working in anything related to sensor technology, networking, embedded systems, or analytics. According to Lonergan, the term IOT was coined before smart phones, tablets, and devices as we know them today existed, and there is a long list of terms with varying degrees of overlap and technological convergence: Internet of Things (IOT), Internet of Everything (IOE), Industrial Internet, Pervasive Computing, Pervasive Sensing, Ubiquitous Computing, Cyber-Physical Systems (CPS), Wireless Sensor Networks (WSN), Smart Objects, Cooperating Objects, Machine-to-Machine (M2M), Ambient Intelligence (AMI), Operational Technology (OT), and Information Technology (IT). Regarding IIOT, an industrial sub-field of IOT, the Industrial Internet Consortium’s Vocabulary Task Group has created a “common and reusable vocabulary of terms” to ensure “consistent terminology” across publications issued by the Industrial Internet Consortium. IOT One has created an IOT Terms Database including a New Term Alert to be notified when a new term is published. As of March 2017, this database aggregates 711 IOT-related terms, however, without any attempts to reduce terminological ambiguity and complexity.

IOT ADOPTION BARRIERS:

COMPLEXITY AND UNCLEAR VALUE PROPOSITIONS:

Despite a shared belief in the potential of IOT, industry leaders and consumers are facing barriers to adopt IOT technology more widely. Dan Yarmoluk from ATEK Access Technologies has written that “the IOT industry

appears heavily focused on gadgets and not making them relevant to the particular business verticals" and "can appear expensive and intimidating." Mike Farley has argued in Forbes that many IOT solutions are either too complex or lack a clear use case for end-users. "Instead of convincing consumers that they need complex systems to serve needs they don't have, we should fix real problems people struggle with every day." Many gadgets in the consumer IOT space have appealed to early adopters, yet failed to demonstrate relevance to ordinary people's lives. In order to overcome barriers, "we need to stop making toys no one cares about and instead work on building simple solutions to real, everyday problems for real people." A recent study by Ericsson regarding the adoption of IOT among Danish companies, has suggested that many are struggling "to pinpoint exactly where the value of IOT lies for them". A company must identify where the value of IOT lies in order to capture it, otherwise non-action is the consequence. This indicates that a major roadblock to IOT adoption is not technical but analytical in nature.

PRIVACY AND SECURITY CONCERNS:

According to a recent study by Noura Aleisa and Karen Renaud at the University of Glasgow, "the Internet of Things' potential for major privacy invasion is a concern" with much of research "disproportionally focused on the security concerns of IOT." Among the "proposed solutions in terms of the techniques they deployed and the extent to which they satisfied core privacy principles", only very few turned out to be fully satisfactory. Louis Basenese, investment director at Wall Street Daily, has criticized the industry's lack of attention to security issues: "Despite high-profile and alarming hacks, device manufacturers remain undeterred, focusing on profitability over security. Consumers need to have ultimate control over collected data, including the option to delete it if they choose...Without privacy assurances, wide-scale consumer adoption simply won't happen." In a post-Snowden world of global

surveillance disclosures, consumers take a more active interest in protecting their privacy and demand IOT devices to be screened for potential security vulnerabilities and privacy violations before purchasing them. According to the 2016 Accenture Digital Consumer Survey, in which 28000 consumers in 28 countries were polled on their use of consumer technology, security “has moved from being a nagging problem to a top barrier as consumers are now choosing to abandon IoT devices and services over security concerns.” The survey revealed that “out of the consumers aware of hacker attacks and owning or planning to own IoT devices in the next five years, 18 percent decided to terminate the use of the services and related services until they get safety guarantees.” This suggests that consumers increasingly perceive privacy risks and security concerns to outweigh the value propositions of IoT devices and opt to postpone planned purchases or service subscriptions.

TRADITIONAL GOVERNANCE STRUCTURES:

A study issued by Ericsson regarding the adoption of Internet of things among Danish companies identified a "clash between IOT and companies' traditional governance structures, as IOT still presents both uncertainties and a lack of historical precedence." Among the respondents interviewed, 60 percent stated that they "do not believe they have the organizational capabilities, and three of four do not believe they have the processes needed, to capture the IOT opportunity." This has led to a need to understand organizational culture in order to facilitate organizational design processes and to test new innovation management practices. A lack of digital leadership in the age of digital transformation has also stifled innovation and IOT adoption to a degree that many companies, in the face of uncertainty, "were waiting for the market dynamics to play out", or further action in regards to IOT "was pending competitor moves, customer pull, or regulatory requirements." Some of these companies risk being "Kodak was a market leader until digital disruption eclipsed film photography with digital photos" - failing to "see the

disruptive forces affecting their industry" and "to truly embrace the new business models the disruptive change opens up." Scott Anthony has written in Harvard Business Review that Kodak "created a digital camera, invested in the technology, and even understood that photos would be shared online" but ultimately failed to realize that "online photo sharing was the new business, not just a way to expand the printing business.

ARDUINO NODE MCU:

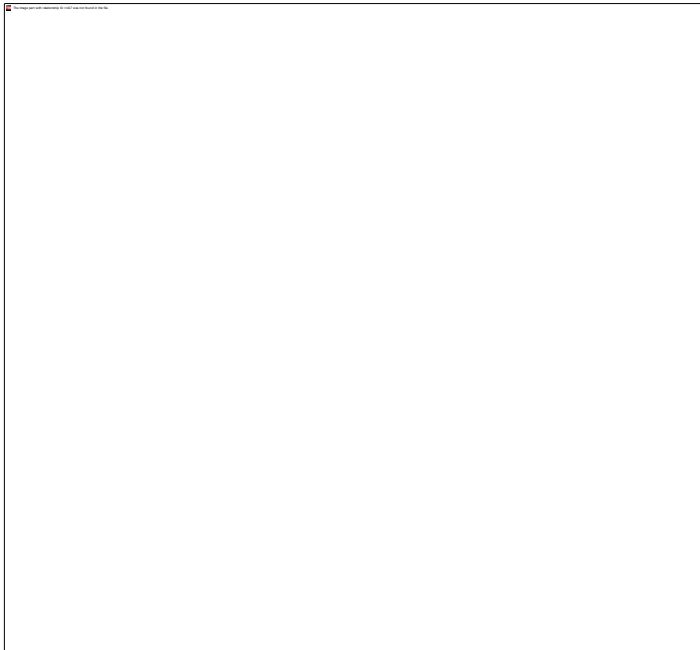


FIG.6.1 .ACTIVITY DIADRAM

NodeMCU is an open source IoT platform. It includes firmware which runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module. The term "NodeMCU" by default refers to the firmware rather than the development kits. The firmware uses the Lua scripting language. It is based on the eLua project, and built on the Espressif Non-OS SDK for ESP8266. It uses many open source projects, such as lua-cjson and SPIFFS

NodeMCU was created shortly after the ESP8266 came out. On December 30, 2013, Espressif Systems began production of the ESP8266. The ESP8266 is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT applications. NodeMCU started on 13 Oct 2014, when Hong committed the first file of nodemcu-firmware to GitHub. Two months later, the project expanded to include an open-hardware platform when developer Huang R committed the gerber file of an ESP8266 board, named devkit v0.9. Later that month, Tuan PM ported MQTT client library from Contiki to the ESP8266 SoC platform, and committed to NodeMCU

project, then NodeMCU was able to support the MQTT IoT protocol, using Lua to access the MQTT broker. Another important update was made on 30 Jan 2015, when Devsaurus ported the u8glib to NodeMCU project, enabling NodeMCU to easily drive LCD, Screen, OLED, even VGA displays.

In summer 2015 the creators abandoned the firmware project and a group of independent contributors took over. By summer 2016 the NodeMCU included more than 40 different modules. Due to resource constraints users need to select the modules relevant for their project and build a firmware tailored to their needs.

ESP8266 Arduino Core

As Arduino.cc began developing new MCU boards based on non-AVR processors like the ARM/SAM MCU and used in the Arduino Due, they needed to modify the Arduino IDE so that it would be relatively easy to change the IDE to support alternate toolchains to allow Arduino C/C++ to be compiled for these new processors. They did this with the introduction of the Board Manager and the SAM Core. A "core" is the collection of software components required by the Board Manager and the Arduino IDE to compile an Arduino C/C++ source file for the target MCU's machine language. Some ESP8266 enthusiasts developed an Arduino core for the ESP8266 WiFi SoC, popularly called the "ESP8266 Core for the Arduino IDE". This has become a leading software development platform for the various ESP8266-based modules and development boards, including NodeMCUs.

Power (USB / Barrel Jack)

Every Arduino board needs a way to be connected to a power source. The Arduino UNO can be powered from a USB cable coming from your computer or a wall power supply that is terminated in a barrel jack. In the picture above the USB connection is labelled **(1)** and the barrel jack is labelled.

NOTE: Do NOT use a power supply greater than 20 Volts as you will overpower (and thereby destroy) your Arduino. The recommended voltage for most Arduino models is between 6 and 12 Volts.

Pins (5V, 3.3V, GND, Analog, Digital, PWM, AREF)

The pins on your Arduino are the places where you connect wires to construct a circuit (probably in conjunction with a breadboard and some wire. They usually have black plastic ‘headers’ that allow you to just plug a wire right into the board. The Arduino has several different kinds of pins, each of which is labelled on the board and used for different functions.

-) **GND (3):** Short for 'Ground'. There are several GND pins on the Arduino, any of which can be used to ground your circuit.
-) **5V (4) & 3.3V (5):** As you might guess, the 5V pin supplies 5 volts of power, and the 3.3V pin supplies 3.3 volts of power. Most of the simple components used with the Arduino run happily off of 5 or 3.3 volts.
-) **Analog (6):** The area of pins under the 'Analog In' label (A0 through A5 on the UNO) are Analog In pins. These pins can read the signal from an analog sensor (like a temperature sensor) and convert it into a digital value that we can read.
-) **Digital (7):** Across from the analog pins are the digital pins (0 through 13 on the UNO). These pins can be used for both digital input (like telling if a button is pushed) and digital output (like powering an LED).
-) **PWM (8):** You may have noticed the tilde (~) next to some of the digital pins (3, 5, 6, 9, 10, and 11 on the UNO). These pins act as normal digital pins, but can also be used for something called Pulse-Width Modulation (PWM). We have a tutorial on PWM, but for now, think of these pins as being able to simulate analog output (like fading an LED in and out).
-) **AREF (9):** Stands for Analog Reference. Most of the time you can leave this pin alone. It is sometimes used to set an external reference voltage (between 0 and 5 Volts) as the upper limit for the analog input pins.

Reset Button

Just like the original Nintendo, the Arduino has a reset button **(10)**. Pushing it will temporarily connect the reset pin to ground and restart any code that is loaded on the Arduino. This can be very useful if your code doesn't repeat, but you want to test it multiple times. Unlike the original Nintendo however, blowing on the Arduino doesn't usually fix any problems.

Power LED Indicator

Just beneath and to the right of the word "UNO" on your circuit board, there's a tiny LED next to the word 'ON' **(11)**. This LED should light up whenever you plug your Arduino into a power source. If this light doesn't turn on, there's a good chance something is wrong. Time to re-check your circuit!

TX RX LEDs

TX is short for transmit, RX is short for receive. These markings appear quite a bit in electronics to indicate the pins responsible for serial communication. In our case, there are two places on the Arduino UNO where TX and RX appear – once by digital pins 0 and 1, and a second time next to the TX and RX indicator LEDs **(12)**. These LEDs will give us some nice visual indications whenever our Arduino is receiving or transmitting data (like when we're loading a new program onto the board).

Main IC

The black thing with all the metal legs is an IC, or Integrated Circuit **(13)**. Think of it as the brains of our Arduino. The main IC on the Arduino is slightly different from board type to board type, but is usually from the AT mega line of IC's from the ATMEL company. This can be important, as you may need to know the IC type (along with your board type) before loading up a new program from the Arduino software. This information can usually be found in

writing on the top side of the IC. If you want to know more about the difference between various IC's, reading the datasheets is often a good idea.

Voltage Regulator

The voltage regulator **(14)** is not actually something you can (or should) interact with on the Arduino. But it is potentially useful to know that it is there and what it's for. The voltage regulator does exactly what it says – it controls the amount of voltage that is let into the Arduino board. Think of it as a kind of gatekeeper; it will turn away an extra voltage that might harm the circuit. Of course, it has its limits, so don't hook up your Arduino to anything greater than 20 volts.

The Arduino Family

Arduino makes several different boards, each with different capabilities. In addition, part of being open source hardware means that others can modify and produce derivatives of Arduino boards that provide even more form factors and functionality. If you're not sure which one is right for your project, check this guide for some helpful hints. Here are a few options that are well-suited to someone new to the world of Arduino

Arduino Uno (R3)

The Uno is a great choice for your first Arduino. It's got everything you need to get started, and nothing you don't. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a USB connection, a power jack, a reset button and more. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started.

Relay:

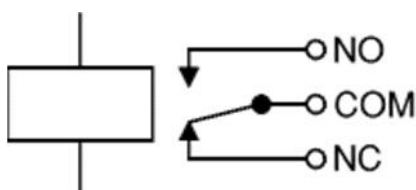
A relay is an electrically operated switch. Current flowing through the coil of the relay creates a magnetic field which attracts a lever and changes the switch contacts. The coil current can be on or off so relays have two switch positions and they are double throw (changeover) switches. Relays allow one circuit to switch a second circuit which can be completely separate from the first. For example a low voltage battery circuit can use a relay to switch a 230V AC mains circuit. There is no electrical connection inside the relay between the two circuits; the link is magnetic and mechanical.

The coil of a relay passes a relatively large current, typically 30mA for a 12V relay, but it can be as much as 100mA for relays designed to operate from lower voltages. Most ICs (chips) cannot provide this current and a transistor is usually used to amplify the small IC current to the larger value required for the relay coil. The maximum output current for the popular 555 timer IC is 200mA so these devices can supply relay coils directly without amplification.



6.2 .RELAY

Relays are usually SPDT or DPDT but they can have many more sets of switch contacts, for example relays with 4 sets of changeover contacts are readily available. Most relays are designed for PCB mounting but you can solder wires directly to the pins providing you take care to avoid melting the plastic case of the relay. The animated picture shows a working relay with its coil and switch contacts. You can see a lever on the left being attracted by magnetism when the coil is switched on. This lever moves the switch contacts. There is one set of contacts (SPDT) in the foreground and another behind them, making the relay DPDT.



The relay's switch connections are usually labeled COM, NC and NO:

-) **COM** = Common, always connect to this, it is the moving part of the switch.
-) **NC** = Normally Closed, COM is connected to this when the relay coil is **off**.
-) **NO** = Normally Open, COM is connected to this when the relay coil is **on**.
-) **DHT11 sensor**
-) Measurement and control of temperature and relative humidity finds applications in numerous areas. These days devices are available which have both temperature and humidity sensors with signal conditioning, ADC, calibration and communication interface all built inside them. The use of such smart sensors greatly simplify the design and reduces the overall cost. We discussed in past about Humidity and temperature measurements with Sensirion's SHT1x/SHT7x sensors. These sensors are capable of measuring both temperature and relative humidity and provide fully calibrated digital outputs. While SHT1x/SHT7x are very accurate sensors, they are still expensive for hobbyists use. This articles discusses the DHT11 sensor which also provides calibrated digital outputs for temperature and humidity but is relatively lot cheaper than the Sensirion sensors. The DHT11 sensor uses a proprietary 1-wire protocol which we will be exploring here and implementing with the PIC16F628A microcontroller that will receive the temperature and humidity values from the sensor and display them on a 16×2 character LCD.
-) **About DHT11 sensor**
-) The DHT11 sensor comes in a single row 4-pin package and operates from 3.5 to 5.5V power supply. It can measure temperature from 0-50 °C with an accuracy of $\pm 2^{\circ}\text{C}$ and relative humidity ranging from 20-95% with an accuracy of $\pm 5\%$. The sensor provides fully calibrated digital outputs for the two measurements. It has got its own proprietary 1-wire protocol, and therefore, the communication between the sensor and a microcontroller is not possible through a direct interface with any of its peripherals. The protocol must be implemented in the firmware of the MCU with precise timing required by the sensor. The following timing diagrams describe the data transfer protocol between a MCU and the DHT11 sensor. The MCU initiates data transmission by issuing a “Start” signal. The MCU pin must be configured as output for this purpose. The MCU first pulls the data line low for at least 18 ms and then pulls it high for next 20-40 μs before it releases it.

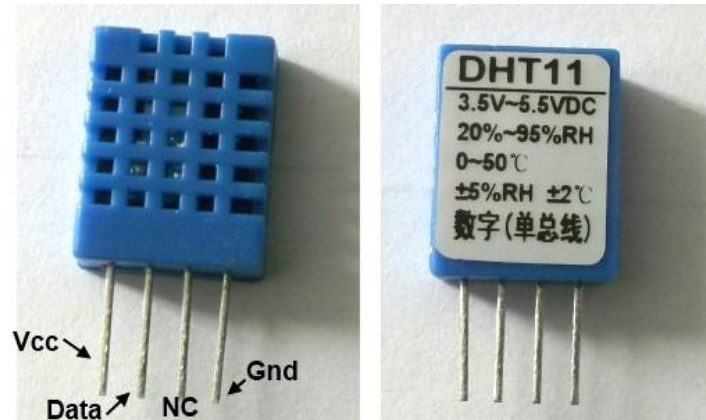


FIG.6.3.DHT11 SENSOR

DHT11 sensor comes in a single row 4-pin package

Next, the sensor responds to the MCU “Start” signal by pulling the line low for 80 μ s followed by a logic high signal that also lasts for 80 μ s. Remember that the MCU pin must be configured to input after finishing the “Start” signal. Once detecting the response signal from the sensor, the MCU should be ready to receive data from the sensor. The sensor then sends 40 bits (5 bytes) of data continuously in the data line. Note that while transmitting bytes, the sensor sends the most significant bit first.

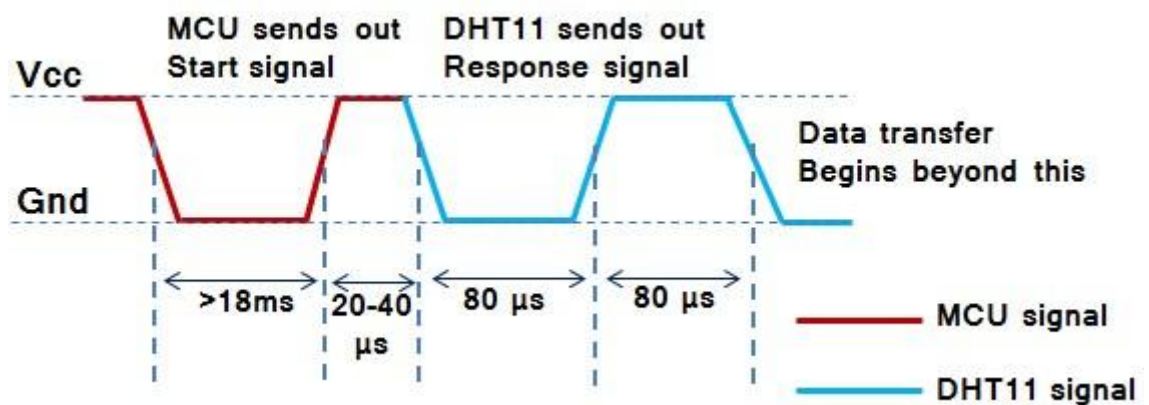


FIG.6.4."Start" and "Response" signals

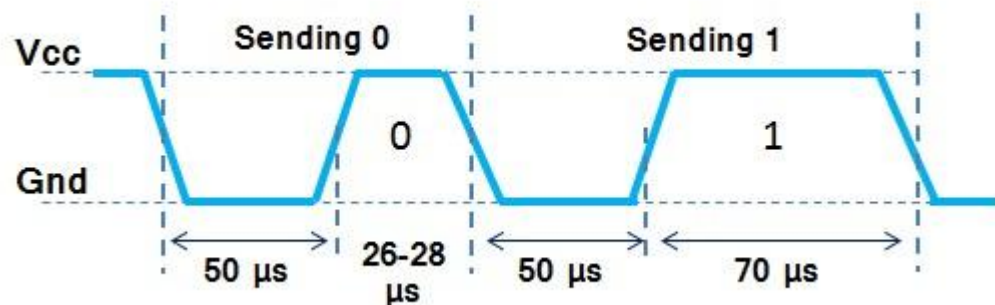
The 40-bit data from the sensor has the following structure.

Data (40-bit) = Integer Byte of RH + Decimal Byte of RH + Integer Byte of Temp. + Decimal Byte of Temp. + Checksum Byte

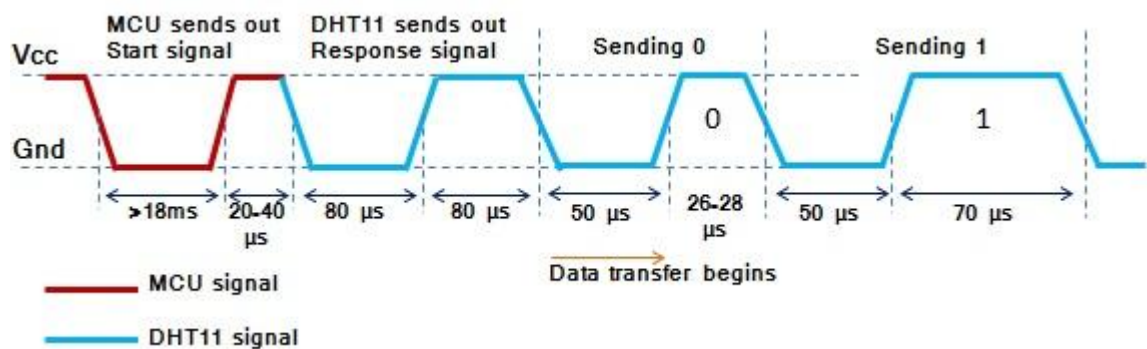
For DHT11 sensor, the decimal bytes of temperature and humidity measurements are always zero. Therefore, the first and third bytes of received data actually give the numeric values of the measured relative humidity (%) and temperature ($^{\circ}$ C). The last byte is the checksum byte

which is used to make sure that the data transfer has happened without any error. If all the five bytes are transferred successfully then the checksum byte must be equal to the last 8 bits of the sum of the first four bytes, i.e.,

-) Checksum = Last 8 bits of (Integer Byte of RH + Decimal Byte of RH + Integer Byte of Temp. + Decimal Byte of Temp.)
-) Now let's talk about the most important thing, which is signalling for transmitting "0" and "1". In order to send a bit of data, the sensor first pulls the line low for 50 μ s. Then it raises the line to high for 26-28 μ s if it has to send "0", or for 70 μ s if the bit to be transmitted is "1". So it is the width of the positive pulse that carries information about 1 and 0.



) FIG.6.5. Timing difference for transmitting "1s" and "0s"



) FIG.6.6. Start, Response and Data signals in sequence

-) At the end of the last transmitted bit, the sensor pulls the data line low for 50 μ s and then releases it. The DHT11 sensor requires an external pull-up resistor to be connected between its Vcc and the data line so that under idle condition, the data line is always pulled high. After finishing the data transmission and releasing the data line, the DHT11 sensor goes to the low-power consumption mode until a new "Start" signal arrives from the MCU.

SERIAL COMMUNICATION

4.1 INTRODUCTION:

Serial communication is basically the transmission or reception of data one bit at a time. Today's computers generally address data in bytes or some multiple thereof. A byte contains 8 bits. A bit is basically either a logical 1 or zero. Every character on this page is actually expressed internally as one byte. The serial port is used to convert each byte to a stream of ones and zeroes as well as to convert a stream of ones and zeroes to bytes. The serial port contains a electronic chip called a Universal Asynchronous Receiver/Transmitter (UART) that actually does the conversion.

The serial port has many pins. We will discuss the transmit and receive pin first. Electrically speaking, whenever the serial port sends a logical one (1) a negative voltage is effected on the transmit pin. Whenever the serial port sends a logical zero (0) a positive voltage is affected. When no data is being sent, the serial port's transmit pin's voltage is negative (1) and is said to be in a MARK state. Note that the serial port can also be forced to keep the transmit pin at a positive voltage (0) and is said to be the SPACE or BREAK state. (The terms MARK and SPACE are also used to simply denote a negative voltage (1) or a positive voltage (0) at the transmit pin respectively).

When transmitting a byte, the UART (serial port) first sends a START BIT which is a positive voltage (0), followed by the data (general 8 bits, but could be 5, 6, 7, or 8 bits) followed by one or two STOP Bits which is a negative(1) voltage. The sequence is repeated for each byte sent. Figure 1 shows a diagram of what a byte transmission would look like.

At this point you may want to know what the duration of a bit is. In other words, how long does the signal stay in a particular state to define a bit. The answer is simple. It is dependent on the baud rate. The baud rate is the number of times the signal can switch states in one second. Therefore, if the line is operating at 9600 baud, the line can switch states 9,600 times per second. This means each bit has the duration of $1/9600$ of a second or about $100\mu\text{sec}$. when transmitting a character there are other characteristics other than the baud rate that must be known or that must be setup. These characteristics define the entire interpretation of the data stream.

The first characteristic is the length of the byte that will be transmitted. This length in general can be anywhere from 5 to 8 bits.

The second characteristic is parity. The parity characteristic can be even, odd, mark, space, or none. If even parity, then the last data bit transmitted will be a logical 1 if the data transmitted had an even amount of 0 bits. If odd parity, then the last data bit transmitted will be a logical 1 if the data transmitted had an odd amount of 0 bits. If MARK parity, then the last transmitted data bit will always be a logical 1. If SPACE parity, then the last transmitted data bit will always be a logical 0. If no parity then there is no parity bit transmitted.

The third characteristic is the amount of stop bits. This value in general is 1 or 2. Assume we want to send the letter 'A' over the serial port. The binary representation of the letter 'A' is 01000001. Remembering that bits are transmitted from least significant bit (LSB) to most significant bit (MSB), the bit stream transmitted would be as follows for the line characteristics 8 bits, no parity, 1 stop bit and 9600 baud. LSB (0 1 0 0 0 0 0 1 0 1) MSB

The above represents (Start Bit) (Data Bits) (Stop Bit). To calculate the actual byte transfer rate simply divide the baud rate by the number of bits that must be transferred for each byte of data. In the case of the above example, each character requires 10 bits to be transmitted for each character. As such, at 9600 baud, up to 960 bytes can be transferred in one second.

The above discussion was concerned with the "electrical/logical" characteristics of the data stream. We will expand the discussion to line protocol. Serial communication can be half duplex or full duplex. Full duplex communication means that a device can receive and transmit data at the same time. Half duplex means that the device cannot send and receive at the same time. It can do them both, but not at the same time. Half duplex communication is all but outdated except for a very small focused set of applications.

Half duplex serial communication needs at a minimum two wires, signal ground and the data line. Full duplex serial communication needs at a minimum three wires, signal ground, transmit data line, and receive data line. The RS232 specification governs the physical and electrical characteristics of serial communications. This specification defines several additional signals that are asserted (set to logical 1) for information and control beyond the data signal.

These signals are the Carrier Detect Signal (CD), asserted by modems to signal a successful connection to another modem, Ring Indicator (RI), asserted by modems to signal the phone ringing, Data Set Ready (DSR), asserted by modems to show their presence, Clear To Send (CTS), asserted by modems if they can receive data, Data Terminal Ready (DTR), asserted by terminals to show their presence, Request To Send (RTS), asserted by terminals if they can receive data. The section RS232 Cabling describes these signals and how they are connected.

The above paragraph alluded to hardware flow control. Hardware flow control is a method that two connected devices use to tell each other electronically when to send or when not to send data. A modem in general drops (logical 0) its CTS line when it can no longer receive characters. It re-asserts it when it can receive again. A terminal does the same thing instead with the RTS signal. Another method of hardware flow control in practice is to perform the same procedure in the

previous paragraph except that the DSR and DTR signals.

Note that hardware flow control requires the use of additional wires. The benefit to this however is crisp and reliable flow control. Another method of flow control used is known as software flow control. This method requires a simple 3 wire serial communication link, transmit data, receive data, and signal ground. If using this method, when a device can no longer receive, it will transmit a character that the two devices agreed on. This character is known as the XOFF character. This character is generally a hexadecimal 13. When a device can receive again it transmits an XON character that both devices agreed to. This character is generally a hexadecimal 11.

4.2 NULL MODEM:

Serial communications with RS232. One of the oldest and most widely spread communication methods in computer world. The way this type of communication can be performed is pretty well defined in standards. I.e. with one exception. The standards show the use of **DTE/DCE** communication, the way a computer should communicate with a peripheral device like a modem. For your information, **DTE** means *Data Terminal Equipment* (computers etc.) where **DCE** is the abbreviation of *Data Communication Equipment* (modems).

One of the main uses of serial communication today where no modem is involved—a *serial null modem* configuration with **DTE/DTE** communication—is not so well defined, especially when it comes to flow control. The terminology *null modem* for the situation where two computers communicate directly is so often used nowadays, that most people don't realize anymore the origin of the phrase and that a null modem connection is an exception, not the rule.

In history, practical solutions were developed to let two computers talk with each other using a null modem serial communication line. In most situations, the original modem signal lines are reused to perform some sort of handshaking. Handshaking can increase the maximum allowed communication speed because it gives the computers the ability to control the flow of information. A high amount of incoming data is allowed if the computer is capable to handle it, but not if it is busy performing other tasks. If no flow control is implemented in the null modem connection, communication is only possible at speeds at which it is sure the receiving side can handle the amount information even under worst case conditions.

SOIL MOISTURE SENSOR:

Soil moisture sensors measure the volumetric water content in soil.[1] Since the direct

gravimetric measurement of free soil moisture requires removing, drying, and weighting of a sample, soil moisture sensors measure the volumetric water content indirectly by using some other property of the soil, such as electrical resistance, dielectric constant, or interaction with neutrons, as a proxy for the moisture content. The relation between the measured property and soil moisture must be calibrated and may vary depending on environmental factors such as soil type, temperature, or electric conductivity. Reflected microwave radiation is affected by the soil moisture and is used for remote sensing in hydrology and agriculture. Portable probe instruments can be used by farmers or gardeners.

Soil moisture sensors typically refer to sensors that estimate volumetric water content. Another class of sensors measure another property of moisture in soils called water potential; these sensors are usually referred to as soil water potential sensors and include tensiometers and gypsum blocks.

Agriculture:

Measuring soil moisture is important for agricultural applications to help farmers manage their irrigation systems more efficiently. Knowing the exact soil moisture conditions on their fields, not only are farmers able to generally use less water to grow a crop, they are also able to increase yields and the quality of the crop by improved management of soil moisture during critical plant growth stages.

Landscape irrigation

In urban and suburban areas, landscapes and residential lawns are using soil moisture sensors to interface with an irrigation controller. Connecting a soil moisture sensor to a simple irrigation clock will convert it into a "smart" irrigation controller that prevents irrigation cycles when the soil is already wet, e.g. following a recent rainfall event.

Golf courses are using soil moisture sensors to increase the efficiency of their irrigation systems to prevent over-watering and leaching of fertilizers and other chemicals into the ground.

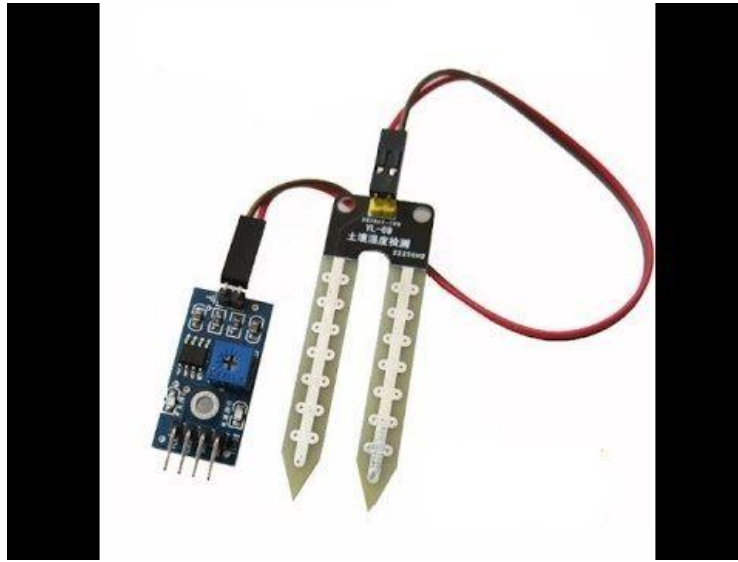
Research

Soil moisture sensors are used in numerous research applications, e.g. in agricultural science and horticulture including irrigation planning, climate research, or environmental science including solute transport studies and as auxiliary sensors for soil respiration measurements.

Simple sensors for gardeners

Relatively cheap and simple devices that do not require a power source are available for

checking whether plants have sufficient moisture to thrive. After inserting a probe into the soil for approximately 60 seconds, a meter indicates if the soil is too dry, moist or wet for plant.



**FIG.6.7 SOIL
MOISTURE
SENSOR**

CHAPTER: 7

SOFTWARE REQUIREMENTS:

Internet of things

The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" and for these purposes a "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication

networks". The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a smart grid, and expanding to areas such as smart cities. "Things", in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring, or field operation devices that assist firefighters in search and rescue operations. Legal scholars suggest regarding "Things" as an "inextricable mixture of hardware, software, data and service". These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include home automation (also known as smart home devices) such as the control and automation of lighting, heating (like smart thermostat), ventilation, air conditioning (HVAC) systems, and appliances such as washer/dryers, robotic vacuums, air purifiers, ovens, or refrigerators/freezers that use Wi-Fi for remote monitoring. As well as the expansion of Internet-connected automation into a plethora of new application areas, IoT is also expected to generate large amounts of data from diverse locations, with the consequent necessity for quick aggregation of the data, and an increase in the need to index, store, and process such data more effectively. IoT is one of the platforms of today's Smart City, and Smart Energy Management Systems

History

As of 2016, the vision of the Internet of things has evolved due to a convergence of multiple technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems. This means that the traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things (IoT). The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's seminal 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT. In 1994 Reza Raji described the concept in IEEE Spectrum as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1996 several companies proposed solutions like Microsoft's at Work or Novell's NEST. However, only in 1999 did the field start gathering momentum. Bill Joy envisioned Device to Device (D2D) communication as part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999. The concept of the Internet of things became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications. Radio-frequency identification (RFID) was seen by Kevin Ashton (one of the founders of the original Auto-ID Center) as a prerequisite for the Internet of things at that point. Ashton prefers the phrase "Internet for Things." If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Besides using RFID, the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes and digital watermarking. In its original interpretation, one of the first consequences of implementing the Internet of things by equipping all objects in the world with minuscule identifying devices or machine-readable identifiers would be to transform daily life. For instance, instant and ceaseless inventory control would become ubiquitous. A person's ability to interact with objects could be altered remotely based on immediate or present needs, in accordance with existing end-user agreements. For example, such technology could grant motion-picture publishers much more control over end-user private devices by remotely enforcing copyright

restrictions and digital rights management, so the ability of a customer who bought a Blu-ray disc to watch the movie could become dependent on the copyright holder's decision, similar to Circuit City's failed DIVX.

Applications

According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 20.8 billion devices on the Internet of things by 2020. ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of things by 2020. As per a 2014 survey and study done by Pew Research Internet Project, a large majority of the technology experts and engaged Internet users who responded—83 percent—agreed with the notion that the Internet/Cloud of Things, embedded and wearable computing (and the corresponding dynamic systems) will have widespread and beneficial effects by 2025. As such, it is clear that the IoT will consist of a very large number of devices being connected to the Internet. In an active move to accommodate new and emerging technological innovation, the UK Government, in their 2015 budget, allocated £40,000,000 towards research into the Internet of things. The former British Chancellor of the Exchequer George Osborne, posited that the Internet of things is the next stage of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances. The ability to network embedded devices with limited CPU, memory and power resources means that IoT finds applications in nearly every field. [48] Such systems could be in charge of collecting information in settings ranging from natural ecosystems to buildings and factories, thereby finding applications in fields of environmental sensing and urban planning. On the other hand, IoT systems could also be responsible for performing actions, not just sensing things. Intelligent shopping systems, for example, could monitor specific users' purchasing habits in a store by tracking their specific mobile phones. These users could then be provided with special offers on their favorite products, or even location of items that they need, which their fridge has automatically conveyed to the phone. Additional examples of sensing and actuating are reflected in applications that deal with heat, water, electricity and energy management, as well as cruise-assisting transportation systems. Other applications that the Internet of things can provide is enabling extended home security features and home automation. The concept of an "Internet of living things" has been proposed to describe networks of biological sensors that could use cloud-based analyses to allow users to study DNA or other molecules. However, the application of the IoT is not only restricted to these

areas. Other specialized use cases of the IoT may also exist. An overview of some of the most prominent application areas is provided here.

Media

In order to hone the manner in which things, media and big data are interconnected, it is first necessary to provide some context into the mechanism used for media process. It has been suggested by Nick Couldry and Joseph Turow that practitioners in media approach big data as many actionable points of information about millions of individuals. The industry appears to be moving away from the traditional approach of using specific media environments such as newspapers, magazines, or television shows and instead tap into consumers with technologies that reach targeted people at optimal times in optimal locations. The ultimate aim is of course to serve, or convey, a message or content that is (statistically speaking) in line with the consumer's mindset. For example, publishing environments are increasingly tailoring the messages (advertisements) and content (articles) to appeal to consumers that have been exclusively gleaned through various data-mining activities. The media industries process big data in a dual, interconnected manner: Targeting of consumers (for advertising by marketers) Data-capture. Thus, the Internet of things creates an opportunity to measure, collect and analyse an ever-increasing variety of behavioural statistics. Cross-correlation of this data could revolutionise the targeted marketing of products and services. For example, as noted by Danny Meadows-Klue, the combination of analytics for conversion tracking with behavioural targeting has unlocked a new level of precision that enables display advertising to be focused on the devices of people with relevant interests. Big data and the IoT work in conjunction. From a media perspective, data is the key derivative of device interconnectivity, whilst being pivotal in allowing clearer accuracy in targeting. The Internet of things therefore transforms the media industry, companies and even governments, opening up a new era of economic growth and competitiveness. The wealth of data generated by this industry (i.e. big data) will allow practitioners in advertising and media to gain an elaborate layer on the present targeting mechanisms used by the industry.

Environmental monitoring

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality,

atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats. Development of resource constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically span a large geographic area and can also be mobile. It has been argued that the standardization IoT brings to wireless sensing will revolutionize this area.

Infrastructure management

Monitoring and controlling operations of urban and rural infrastructures like bridges, railway tracks, on- and offshore- wind-farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities. IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IoT.

Manufacturing Network

control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well. The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together. Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT. But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Smart industrial management systems can also be integrated with the Smart Grid, thereby enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors. The National Science Foundation established an

Industry/University Cooperative Research Center on intelligent maintenance systems (IMS) in 2001 with a research focus to use IoT-based predictive analytics technologies to monitor connected machines and to predict machine degradation, and further to prevent potential failures. The vision to achieve near-zero breakdown using IoT-based predictive analytics led the future development of e-manufacturing and emaintenance activities. The term IIoT (Industrial Internet of Things) is often encountered in the manufacturing industries, referring to the industrial subset of the IoT. IIoT in manufacturing could generate so much business value that it will eventually lead to the fourth industrial revolution, so the so-called Industry 4.0. It is estimated that in the future, successful companies will be able to increase their revenue through Internet of things by creating new business models and improve productivity, exploit analytics for innovation, and transform workforce. The potential of growth by implementing IIoT will generate \$12 trillion of global GDP by 2030. While connectivity and data acquisition are imperative for IIoT, they should not be the purpose, rather the foundation and path to something bigger. Among all the technologies, predictive maintenance is probably a relatively "easier win" since it is applicable to existing assets and management systems. The objective of intelligent maintenance systems is to reduce unexpected downtime and increase productivity. And to realize that alone would generate around up to 30% over total maintenance costs. Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. Cyber-physical systems can be designed by following the 5C (connection, conversion, cyber, cognition, configuration) architecture, and it will transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes. An IoT-enabled intelligent system of such cases has been demonstrated by the NSF Industry/University Collaborative Research Center for Intelligent Maintenance Systems (IMS) at University of Cincinnati on a band saw machine in IMTS 2014 in Chicago. Band saw machines are not necessarily expensive, but the band saw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics, it can be only determined by experience when the band saw belt will actually break. The developed prognostics system will be able to recognize and monitor the degradation of band saw belts even if the condition is changing, so that users will know in near real time when is the best time to

replace band saw. This will significantly improve user experience and operator safety, and save costs on replacing band saw belts before they actually break. The developed analytical algorithms were realized on a cloud server, and was made accessible via the Internet and on mobile devices.

Energy management

Integration of sensing and actuation systems, connected to the Internet, is likely to optimize energy consumption as a whole. It is expected that IoT devices will be integrated into all forms of energy consuming devices (switches, power outlets, bulbs, televisions, etc.) and be able to communicate with the utility supply company in order to effectively balance power generation and energy usage. Such devices would also offer the opportunity for users to remotely control their devices, or centrally manage them via a cloud based interface, and enable advanced functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). Besides home based energy management, the IoT is especially relevant to the Smart Grid since it provides systems to gather and act on energy and power-related information in an automated fashion with the goal to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Using advanced metering infrastructure (AMI) devices connected to the Internet backbone, electric utilities can not only collect data from end-user connections, but also manage other distribution automation devices like transformers and reclosers.

Medical and healthcare

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. Other consumer devices to encourage healthy

living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT. More and more end-to-end health monitoring IoT platforms are coming up for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

Building and home automation

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation and building automation systems. In this context, three main areas are being covered in literature : The integration of the internet with building energy management systems in order to create energy efficient and IOT driven “smart buildings” . The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviors . The integration of smart devices in the built environment and how they might be used in future applications .

Transportation

The IoT can assist in integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter and intra vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance.

Metropolitan scale deployments

There are several planned or ongoing large-scale deployments of the IoT, to enable better management of cities and systems. For example, Songdo, South Korea, the first of its kind fully equipped and wired smart city, is near completion. Nearly everything in this city is planned to be wired, connected and turned into a constant stream of data that would be monitored and analyzed by an array of computers with little, or no human intervention. Another application is a currently undergoing project in Santander, Spain. For this deployment, two approaches have been adopted. This city of 180,000 inhabitants, has already seen 18,000 city application downloads for their smartphones. This application is connected to 10,000 sensors that enable services like parking search, environmental monitoring, digital city agenda among others. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behavior

that aims at maximizing the impact of each notification. Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City; work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California; and smart traffic management in western Singapore. French company, Sigfox, commenced building an ultra-narrowband wireless data network in the San Francisco Bay Area in 2014, the first business to achieve such a deployment in the U.S. It subsequently announced it would set up a total of 4000 base stations to cover a total of 30 cities in the U.S. by the end of 2016, making it the largest IoT network coverage provider in the country thus far. Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7. The network was designed and engineered by Fluidmesh Networks, a Chicago-based company developing wireless networks for critical applications. The NYWW network is currently providing coverage on the Hudson River, East River, and Upper New York Bay. With the wireless network in place, NY Waterway is able to take control of its fleet and passengers in a way that was not previously possible. New applications can include security, energy and fleet management, digital signage, public Wi-Fi, paperless ticketing and others.

Consumer application

A growing portion of IoT devices are created for consumer use. Examples of consumer applications include connected car, entertainment, residences and smart homes, wearable technology, quantified self, connected health, and smart retail . Consumer IoT provides new opportunities for user experience and interfaces. Some consumer applications have been criticized for their lack of redundancy and their inconsistency, leading to a popular parody known as the "Internet of Shit." Companies have been criticized for their rush into IoT, creating devices of questionable value, and not setting up stringent security standards.

Unique addressability of things

The original idea of the Auto-ID Center is based on RFID-tags and unique identification through the Electronic Product Code however this has evolved into objects having an IP address or URI. An alternative view, from the world of the Semantic Web focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralized servers

acting for their human owners.

Integration with the Internet implies that devices will use an IP address as a unique identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IoT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required. Internet of things devices additionally will benefit from the stateless address auto-configuration present in IPv6, as it reduces the configuration overhead on the hosts, and the IETF 6LoWPAN header compression. To a large extent, the future of the Internet of things will not be possible without the support of IPv6; and consequently the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future. A combination of these ideas can be found in the current GS1/EPCglobal EPC Information Services (EPCIS) specifications. This system is being used to identify objects in industries ranging from aerospace to fast moving consumer products and transportation logistics.

Trends and characteristics

Intelligence

Ambient intelligence and autonomous control are not part of the original concept of the Internet of things. Ambient intelligence and autonomous control do not necessarily require Internet structures, either. However, there is a shift in research to integrate the concepts of the Internet of things and autonomous control, with initial outcomes towards this direction considering objects as the driving force for autonomous IoT. In the future the Internet of things may be a non-deterministic and open network in which auto-organized or intelligent entities (Web services, SOA components), virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments. Autonomous behavior through the collection and reasoning of context information as well as the objects ability to detect changes in the environment, faults affecting sensors and introduce suitable mitigation measures constitute a major research trend, clearly needed to provide credibility to the IoT technology. Modern IoT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation but more sophisticated forms of intelligence are requested to permit sensor units to be deployed in real environments.

Architecture

The system will likely be an example of event-driven architecture, bottom-up made (based on the context of processes and operations, in real-time) and

will consider any subsidiary level. Therefore, model driven and functional approaches will coexist with new ones able to treat exceptions and unusual evolution of processes (multi-agent systems, B-ADSc, etc.). In an Internet of things, the meaning of an event will not necessarily be based on a deterministic or syntactic model but would instead be based on the context of the event itself: this will also be a semantic web. Consequently, it will not necessarily need common standards that would not be able to address every context or use: some actors (services, components, avatars) will accordingly be self-referenced and, if ever needed, adaptive to existing common standards (predicting everything would be no more than defining a "global finality" for everything that is just not possible with any of the current top-down approaches and standardizations). Building on top of the Internet of things, the web of things is an architecture for the application layer of the Internet of things looking at the convergence of data from IoT devices into Web applications to create innovative use-cases. In order to program and control the flow of information in the Internet of things, a predicted architectural direction is being called BPM Everywhere which is a blending of traditional process management with process mining and special capabilities to automate the control of large numbers of coordinated devices.

Network architecture

The Internet of things requires huge scalability in the network space to handle the surge of devices. IETF 6LoWPAN would be used to connect devices to IP networks. With billions of devices being added to the Internet space, IPv6 will play a major role in handling the network layer scalability. IETF's Constrained Application Protocol, ZeroMQ, and MQTT would provide lightweight data transport. "MQ" in "MQTT" came from IBM's MQ Series message queuing product line. Fog computing is a viable alternative to prevent such large burst of data flow through Internet. The edge devices' computation power can be used to analyse and process data, thus providing easy real time scalability.

Complexity

In semi-open or closed loops (i.e. value chains, whenever a global finality can be settled) IoT will often be considered and studied as a complex system due to the huge number of different links, interactions between autonomous actors, and its capacity to integrate new actors. At the overall stage (full open loop) it will likely be seen as a chaotic environment (since systems always have finality). As a practical approach, not all elements in the Internet of things run in a global, public space. Subsystems are often implemented to mitigate the risks of privacy, control and reliability. For example, Domestic Robotics

(Domotics) running inside a smart home might only share data within and be available via a local network.

Size considerations

The Internet of things would encode 50 to 100 trillion objects, and be able to follow the movement of those objects. Human beings in surveyed urban environments are each surrounded by 1000 to 5000 trackable objects.

Space considerations

In the Internet of things, the precise geographic location of a thing—and also the precise geographic dimensions of a thing—will be critical. Therefore, facts about a thing, such as its location in time and space, have been less critical to track because the person processing the information can decide whether or not that information was important to the action being taken, and if so, add the missing information (or decide to not take the action). (Note that some things in the Internet of things will be sensors, and sensor location is usually important. The GeoWeb and Digital Earth are promising applications that become possible when things can become organized and connected by location. However, the challenges that remain include the constraints of variable spatial scales, the need to handle massive amounts of data, and an indexing for fast search and neighbor operations. In the Internet of things, if things are able to take actions on their own initiative, this human-centric mediation role is eliminated. Thus, the time-space context that we as humans take for granted must be given a central role in this information ecosystem. Just as standards play a key role in the Internet and the Web, geospatial standards will play a key role in the Internet of things.

Sectors

There are three core sectors of the IoT: enterprise, home, and government, with the Enterprise Internet of Things (EIoT) being the largest of the three. By 2019, the EIoT sector is estimated to account for nearly 40% or 9.1 billion devices.

A Solution to "basket of remotes"

According to the CEO of Cisco, the commercial opportunity for "connected products ranging from cars to household goods" is expected to be a \$USD 19 trillion. Many IoT devices have a potential to take a piece of this market. Jean-Louis Gassée (Apple initial alumni team, and BeOS co-founder) has addressed this topic in an article on Monday Note, where he predicts that the most likely problem will be what he calls the "basket of remotes" problem, where we'll have hundreds of applications to interface with hundreds of devices that don't share protocols for speaking with one another. There are

multiple approaches to solve this problem, one of them called the "predictive interaction", where cloud or fog based decision makers will predict the user's next action and trigger some reaction. For user interaction, new technology leaders are joining forces to create standards for communication between devices. While AllJoyn alliance is composed of the top 20 World technology leaders, there are also big companies that promote their own protocol like CCF from Intel. Manufacturers are becoming more conscious of this problem, and many companies have begun releasing their devices with open APIs. Many of these APIs are used by smaller companies looking to take advantage of quick integration.

Frameworks

IoT frameworks might help support the interaction between "things" and allow for more complex structures like distributed computing and the development of distributed applications. Currently, some IoT frameworks seem to focus on real-time data logging solutions, offering some basis to work with many "things" and have them interact. Future developments might lead to specific software-development environments to create the software to work with the hardware used in the Internet of things. Companies are developing technology platforms to provide this type of functionality for the Internet of things. Newer platforms are being developed, which add more intelligence. REST is a scalable architecture that allows things to communicate over Hypertext Transfer Protocol and is easily adopted for IoT applications to provide communication from a thing to a central web server. MQTT is a publish-subscribe architecture on top of TCP/IP that allows bidirectional communication between a thing and an MQTT broker

Enabling technologies for IoT

There are many technologies that enable IoT. Crucial to the field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfill:

Short-range wireless

-) Bluetooth low energy (BLE) – Specification providing a low power variant to classic Bluetooth with a comparable communication range.
-) Light-Fidelity (Li-Fi) – Wireless communication technology similar to the Wi-Fi standard, but using visible light communication for increased bandwidth.
-) Near-field communication (NFC) – Communication protocols enabling two electronic devices to communicate within a 4 cm range.

-) QR codes and barcodes – Machine-readable optical tags that store information about the item to which they are attached.
-) Radio-frequency identification (RFID) – Technology using electromagnetic fields to read data stored in tags embedded in other items.
-) Thread – Network protocol based on the IEEE 802.15.4 standard, similar to ZigBee, providing IPv6 addressing.
-) Transport Layer Security (network protocol)|TLS – Network security protocol.
-) Wi-Fi – Widely used technology for local area networking based on the IEEE 802.11 standard, where devices may communicate through a shared access point.
-) Wi-Fi Direct – Variant of the Wi-Fi standard for peer-to-peer communication, eliminating the need for an access point.
-) Z-Wave – Communication protocol providing short-range, low-latency data transfer at rates and power consumption lower than Wi-Fi. Used primarily for home automation.
-) ZigBee – Communication protocols for personal area networking based on the IEEE 802.15.4 standard, providing low power consumption, low data rate, low cost, and high throughput.

Medium-range wireless

-) HaLow – Variant of the Wi-Fi standard providing extended range for low-power communication at a lower data rate.
-) LTE-Advanced – High-speed communication specification for mobile networks. Provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency.

Long-range wireless

-) Low-power wide-area networking (LPWAN) – Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission.
-) Very small aperture terminal (VSAT) – Satellite communication technology using small dish antennas for narrowband and broadband data.

Wired

-) Ethernet – General purpose networking standard using twisted pair and fiber optic links in conjunction with hubs or switches.
-) Multimedia over Coax Alliance (MoCA) – Specification enabling whole-home distribution of high definition video and content over existing coaxial cabling.

-) Power-line communication (PLC) – Communication technology using electrical wiring to carry power and data. Specifications such as HomePlug utilize PLC for networking IoT devices.

CHAPTER: 8

RESULT:

We were able to successfully control the lights and fans of a room. We saw the updates on the website about the light or fans getting on and off with live updates to admin. The Dashboard has number of users connected to the system and who has the access privilege to a particular switch. The Home automation was successful in showing the unit Bill and the amount of voltage consumed by a particular user.

The Live Graphical representation of Number of user connected versus time, Voltage versus time, Amount of bill till now versus time. Tasker is working correctly. Three task with different dates and time were spotted working on given time. Last date and time of use of particular switch was recorded and displayed on website at the time of testing.

CHAPTER: 9

CONCLUSION:

I implemented a smart home automation device is undeniably resource which can make a home environment as well as the surroundings where the electronic appliances are connected automated. People can connect their electronic appliances through smart home controlling device and setup controlling actions through their smart phones or PC's or tablets.

CHAPTER: 10

REFERENCE:

[1] Y. Liu, "Study on Smart Home System Based on Internet of Things Technology," in Informatics and Management Science IV. vol. 207, W. Du, Ed., ed: Springer London, 2013, pp. 73-81.

- [2] M. A. Al-Qutayri and J. S. Jeedella, "Integrated Wireless Technologies for Smart Homes Applications," in Smart Home Systems, M. A. Al-Qutayri, Ed., ed: InTech, 2010.
- [3] C. Chiu-Chiao, H. Ching Yuan, W. Shiau-Chin, and L. Cheng-Min, "Bluetooth-Based Android Interactive Applications for Smart Living," in Innovations in Bioinspired Computing and Applications (IBICA), 2011 Second International Conference on, 2011, pp. 309-312.
- [4] Anushri Aware, Sonali Vaidya, Priyanka Ashture, Varsha Gaiwal, "Home Automation using Android App and Cloud Network", International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015.
- [5] Prachi T. Deokar, Dr. Manoj S. Nagmode, "Cloud Server Based Home Automation System Using Android Phone", (IJIRSE) International Journal of Innovative Research in Science & Engineering
- [6] Fukuoka-shi, "Design and Implementation of Improved Authentication System for Android Smartphone Users", IEEE International Conference on Advanced Information Networking and Applications Workshops, 2012
- [7] Carelin Felix, I. Jacob Raglend, "Home Automation Using GSM", Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011)
- [8] Fukuoka-shi, "Design and Implementation of Improved Authentication System for Android Smartphone Users", IEEE International Conference on Advanced Information Networking and Applications Workshops, 2012.
- [9] Rajeev Piyare, "Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone", International Journal of Internet of Things 2013, 2(1): 5-11
- [10] Alper Gurek, Caner Gur, Cagri Gurakin, Mustafa Akdeniz, Senem Kumova Metin, Ilker Korkmaz, "An Android Based Home Automation System", 2013 IEEE
- [11] Azmul Hasan, Abdullah Al Mamun Khan, Nezam Uddin, Abu Farzan Mitul, "Design and Implementation of Touchscreen and Remote Control Based Home Automation System", Proceedings of 2013 2nd International Conference on Advances in Electrical Engineering (ICAEE 2013) 19-21 December, 2013, Dhaka, Bangladesh

[12] Humaid AlShu'eili, Gourab Sen Gupta, Subhas Mukhopadhyay, "Voice Recognition Based Wireless Home Automation System", 2011 4 International Conference on Mechatronics (ICOM), 17-19 May 2011, Kuala Lumpur, Malaysia

[13] Andreas Rosendahl, J. Felix Hampe, Goetz Botterweck, "Mobile Home Automation – Merging Mobile Value Added Services and Home Automation Technologies", Sixth International Conference on the Management of Mobile Business (ICMB 2007)

[14] Jaya Bharathi chintalapati, Srinivasa Rao T.Y.S, "Remote computer access through Android mobiles", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3, September 2012

[15] Nikhil Singh, Shambhu Shankar Bharti, Rupal Singh, Dushyant Kumar Singh, "REMOTELY CONTROLLED HOME AUTOMATION SYSTEM", IEEE International Conference on Advances in Engineering & Technology Research (ICAETR - 2014)