

SMART ELECTRIC BOARD MONITORING AND WATER FLOW SYSTEM USING IOT

Submitted in partial fulfilment of the requirements for the award of
Bachelor of Engineering degree in Electronics & Communication Engineering
by

P. DOLA SAI RAGHAVENDHRA (Reg. No. 37130113)



**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING
SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING**

SATHYABAMA

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

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL 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 ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the Bonafide work of **P. Dola Sai Raghavendra (Reg No: 37130113)** who carried out the project entitled "**SMART ELECTRIC BOARD MONITORING AND WATER FLOW SYSTEM USING INTERNET OF THINGS**" under our supervision from December 2021 to April 2021.

Internal Guide

Dr. T. Vino M.E., Ph.D.,

HEAD OF DEPARTMENT

Dr. T. Ravi M.E., Ph.D.,

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I P. DOLA SAI RAGHAVENDRA (37130113) hereby declare that the Project Report entitled SMART ELECTRIC BOARD MONITORING & WATER FLOW SYSTEM USING IOT done by me under the guidance of Dr. T. VINO M.E., Ph.D., at Sathyabama institute of science and technology is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in ELECTRONICS AND COMMUNICATION ENGINEERING.

DATE:

PLACE:

P. DOLA SAI RAGHAVENDRA

(37130113)

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. N. M. NANDITHA, M.E., Ph.D.**, Dean, School of Electrical and Electronics and **Dr. T. RAVI, M.E., Ph.D.**, Head of the Department, Dept. of Electronics and Communication 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 our Project Guide **Dr. T. VINO, M.E., Ph.D.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my projectwork.

I wish to express our thanks to all Teaching and Non-teaching staff members of the Department of Electronics and Communication Engineering who were helpful in many ways for the completion of the project.

ABSTRACT

As in everywhere automation is required to reduce the work and curbing electricity theft in India, which accounts for 80% of the power losses. While the nation strives to mark a new golden era, the power sector suffers contributing to blackouts and costs \$17 billion in lost revenue annually, according to calculations by Bloomberg. With the nation-wide production at over 250GW, as on August 2016 , weak infrastructure accounts for various losses – transmission, distribution, aggregate technical and commercial losses due to these is occurs by power thefting our paper mainly focused on to identify these power thefting and calculate the units from the appliance and it gives the notification depend upon the consumption and electrical appliance may control through the internet at anywhere in the world there is no distance parameter for that and manual reset to start the function again. The main objectives of this system are described clearly as follows: theft of electricity increases the costs paid by customers and can have serious safety consequences. Detecting electricity theft has been traditionally addressed by physical checks of tamper-evident seals by field personnel and by using balance meters. Identify the theft by sending alert SMS to the owner. Sent meter readings and rate every month to the owner. Adding with these setup an efficient Internet of Things (IOT) is defined, which portraits the global connection environment to the users and allow them to view the status of meter reading and theft associations globally from anywhere at any time. Theft of electricity has a material impact on customers in terms of cost and safety. We consider that the existing regulatory framework does not adequately encourage suppliers .

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No.
	ABSTRACT	5
	LIST OF FIGURES	10
1	INTRODUCTION	12
2	LITERATURE SURVEY	
	2.1 LITERATURE REVIEW OF INTERNET OF THINGS	13
	2.2 LITERATURE REVIEW OF SMART ELECTRIC BOARD	14
3	EXISTING SYSTEM AND PROPOSED STSTEM	16
	3.1 EXISTING SYSTEM	16
	3.2 PROPOSED SYSTEM	17
	3.2.1 OPERATION OF THE PROPOSED SYSTEM	18
	3.2.2 ADVANTAGES	18
	3.3 BLOCK DIAGRAM	19
	3.4 REQUIREMENTS	19
	3.4.1 HARDWARE REQUIREMENTS	19
	3.4.2 SOFTWARE REQUIREMENTS	20
4	IOT: INTERNET OF THINGS	21
	4.1 INTRODUCTION	21
	4.2 HISTORY	22
	4.3 APPLICATIONS	24
	4.4 MEDIA	25
	4.5 ENVIROMENTAL MONITORING	26
	4.6 INFRASTRUCTURE MANAGEMENT	26
	4.7 MANUFACTURING NETWORK	27
	4.8 ENERGY MANAGEMENT	28
	4.9 MEDICAL AND HEALTHCARE	29

4.10	BUILDING AND HOME AUTOMATION	29
4.11	TRANSPORTATION	29
4.12	METROPOLITAN SCALE	
	DEPLOYMENTS	30
4.13	CONSUMER APPLICATION	31
4.14	UNIQUE ADDRESSABILITY OF THING	31
4.15	TRENDS AND CHARACTERISTICS	32
4.15.1	INTELLIGENCE	32
4.15.2	ARCHITECTURE	33
4.15.3	NETWORK ARCHITECTURE	33
4.16	COMPLEXITY	34
4.16.1	SIZE CONSIDERATIONS	34
4.16.2	SPACE CONSIDERATIONS	34
4.16.3	SECTORS	35
4.16.4	SOLUTION TO "BASKET OF REMOTES"	35
4.17	FRAMEWORKS	35
4.17.1	ENABLING TECHNOLOGIES FOR IOT	36
4.17.2	SHORT-RANGE WIRELESS	
4.17.3	MEDIUM-RANGE WIRELESS	36
4.17.4	LONG-RANGE WIRELESS	37
4.17.5	WIRED	37
4.18	SIMULATION	37
4.19	CRITICISM AND CONTROVERSIES	37
4.19.1	PLATFORM FRAGMENTATION	39
4.19.2	PRIVACY, AUTONOMY, AND CONTROL	39
4.19.3	DATA STORAGE AND ANALYTICS	39

4.19.4	SECURITY	40
4.20	DESIGN	41
4.21	ENVIRONMENTAL SUSTAINABILITY IMPACT	42
4.22	INTENTIONAL OBSOLESCENCE OF DEVICES	43
4.23	CONFUSING TERMINOLOGY	
4.24	IOT ADOPTION BARRIERS	44
4.24.1	COMPLEXITY AND UNCLEAR VALUE PROPOSITIONS	44
4.24.2	PRIVACY AND SECURITY CONCERNS	45
4.25	TRADITIONAL GOVERNANCE STRUCTURES	46
4.26	ARDUINO INTRODUCTION	
4.26.1	WHAT DOES IT DO?	47
4.26.2	WHAT'S ON THE BOARD	47
4.26.2.1	POWER (USB / Barrel Jack)	48
4.26.2.2	PINS (5V, 3.3V, GND, Analog, Digital, PWM, AREF)	49
4.26.2.3	RESET BUTTON	
4.26.2.4	POWER LED INDICATOR	50
4.26.2.5	TX RX LEDs	50
4.26.2.6	MAIN IC	50
4.26.2.7	VOLTAGE REGULATOR	50
4.26.2.8	ARDUINO UNO(R3)	51
4.26.3	WHY ARDUINO?	51
4.26.4	USING ARDUINO IDE	52
4.27	ESP8266 NODEMCU WI-IF KIT	52
4.28	RELAYS	64

	4.29 WATER FLOW SYSTEM	66
	4.29.1 WATER FLOW SENSOR	68
	4.29.2 WORKING PRINCIPLE	68
	4.29.3 APPLICATION OF WATER FLOW SENSOR	69 70
5	RESULTS AND CONCLUSION	71
	5.1 OUTPUT	71
	5.2 CONCLUSION	75
6	REFERENCE	76

LIST OF FIGURES

FIGURE NO.	TITLE OF FIGURES	PAGE No.
3.1	Block diagram	19
3.2	Power theft identification	19
4.1	Introduction	22
4.2	IOT-Application	25
4.3	Consumer Application0	31
4.4	Design	42
4.5	What on the Arduino Board?	48
4.6	Arduino Board	54
4.7	Connecting a Battery	56
4.8	Preference	58
4.9	Boards Manger	59
4.10.1	Setup 1	60
4.10.2	Setup 2	60
4.10.3	Setup3	61
4.10.4	Setup4	62
4.11	Heart beat sensor	64
4.12	NodeMCU wi-fi kit	65
4.13	Pin definition	66
4.14	Relay	67
4.15	Waterflow Sensor	68
5.1	Output 1	71
5.2	Output 2	72
5.3	Output 3	73

5.4	Output 4	74
5.5	Output 5	75

CHAPTER-1

INTRODUCTION:

The smart EB is an advanced platform to the way we receive electricity today. In earlier times the demand for electricity was substantial compared to that presently. Since the demand for electricity has tremendously increased, a redesign of the current grid system is much needed. With the technology available in these modern times, the smart grid could be designed in such a manner, that it uses digital communications technology to detect and react to local changes in usage. The system will feature a two-way dialog where electricity and information can be exchanged between the consumer and utility.

This can increase or decrease the amount of energy a consumer needs by analyzing the feedback of the two-way dialog. In this system a smart energy meter is installed in every consumer unit and a server is maintained at the service provider side. Both the meter and the server are equipped with which facilitates communication between the two ends using Server. The Arduino gets the tariff data from the Energy meter and sends the acquired data to the server.

The server in the transmission system is connected with the cloud, through this we can able to monitor and control the EB lines of every consumer through Internet. This system also serves to shut off the EB Line to the consumers who are not paying their monthly bills properly. The process can be easy and maintenance then even more secure this system also helps the consumers to monitor their daily usage of current through Internet.

The transfer of electricity and information between consumer and utility would increase efficiency, reliability and security. The smart grid also enables renewable energy technology to be integrated into the system for a greener, more environmentally friendly method.

CHAPTER-2

LITERATURE SURVEY

2.1 LITERATURE REVIEW OF INTERNET OF THINGS:

One of the main problems with the IoT is that it is so vast and such a broad concept that there is no proposed, uniform architecture. In order for the idea of IoT to work, it must consist of an assortment of sensor, network, communications and computing technologies, amongst others. Here, some of IoT architectures or models are given by several researchers, authors and practitioners.

European FP7 Research Project

1. This is to be used as a blueprint for IoT concrete architecture design
2. Model: Architectural Reference Model (ARM).
3. Developed By: Project partners of the European FP7 Research Project IoT- A
4. Derived From: Business considerations, application-based requirements.
5. current technologies.

Qian Xiaocong, Zhang Jidong Architecture

According to Qian Xiaocong and Zhang Jidong (2012), the traditional IoT is formed by three layers. The bottom is perception layer, whose function is cognizing and collecting information of objects. The middle is transportation layer which consists of OFC, mobile phone networks, and fixed telephone networks, broadcasting networks, and closed IP data networks for each carrier. And finally the top is application layer, where abundant applications run. Typical applications include in this layer are smart traffic, precise agriculture, intelligent logistics, smart industry, environment protection, mining monitor, remote nursing, safety defence, smart government etc.

2.2 LITERATURE REVIEW OF SMART ELECTRIC BOARD:

A New Intrusion Prevention System for Protecting Smart Grids from CMPv6 Vulnerabilities Manali Chakraborty • Nabendu Chaki • Agostino Cortesi Smart Grid is an integrated power grid with a. reliable, communication network running in parallel towards providing two ways communications in the grid. It's trivial to mention that a network like this would connect a huge number of IPenabled devices. IPv6 that offers 128-bit address space becomes an obvious choice in this context. In a smart grid, functionalities like neighbourhood discovery, autonomic address configuration of a node or its router identification may often be invoked whenever newer equipment's are introduced for capacity enhancement at some level of hierarchy. In IPv6, these basic functionalities like neighbourhood discovery, autonomic address configuration of networking require to use Internet Control Message Protocol version 6 (ICMPv6). Such usage may lead to security breaches in the grid as a result of possible abuses of ICMPv6 protocol. In this paper, some potential newer attacks on Smart Grid have been discussed. Subsequently, intrusion prevention mechanisms for these attacks are proposed to plug- in the threats.

Smart Grid — The New and Improved Power Grid: A Survey

Xi Fang • Satyajayant Misra • Guoliang Xue • Dejun Yang The Smart Grid, regarded as the next generation power grid, uses two-way flows of electricity and information to create a widely distributed automated energy delivery network. In this article, we survey the literature till 2011 on the enabling technologies for the Smart Grid. We explore three major systems, namely the smart infrastructure system, the smart management system, and the smart protection system. We also propose possible future directions in each system. Specifically, for the smart infrastructure system, we explore the smart energy subsystem, the smart information subsystem, and the smart communication subsystem. For the smart management system, we explore various management objectives, such as improving energy efficiency, profiling demand, maximizing utility, reducing cost, and controlling emission. We also explore various management methods to achieve these objective.

Defending mechanisms against false-data injection attacks in the power system state estimation:

Suzhi Bi Accurate state estimation is of critical importance to maintain normal operating conditions of smart power grids. To ensure the integrity of state estimation, the current power grid systems use bad data detection (BDD) system to filter faulty measurements caused by device malfunctions or malicious attacks, etc. However, recent research shows that carefully synthesized false-data injection attacks can bypass the BDD system and thus introduce arbitrary errors to state estimates. In this paper, we investigate defending mechanisms against false-data injection attacks. We first derive a necessary and sufficient condition to select the protection measurements and analyze the properties of the optimal solution which protects the state estimates with minimum number of measurements.

Based on the arguments, both optimal and reduced-complexity suboptimal algorithms are proposed. In particular, the suboptimal algorithm allows the system operator to protect the state estimates in arbitrary sequence according to their relative importance. Analysis and experiments show that it significantly reduces computational complexity, while yielding negligible performance degradation compared with the optimal algorithm.

CHAPTER – 3

EXISTING SYSTEM AND PROPOSED SYSTEM

3.1 EXISTING SYSTEM

- The already existing system is having lot of complexities in before that they are all using to measure the ac current using current transformer.
- A current transformer can only sense current down to some minimum frequency below which gain falls off rapidly. A current transformer can't sense a fixed current.
- If you are measuring current of something that is inherently AC, like the power line, then a current transformer can be appropriate. If you really need to sense DC current, then you can't use a current transformer. Controlling the home appliance through Bluetooth, GSM is already existing system.
- Bluetooth is having the distance parameter and there is no more monitoring.
- By using GSM module it just send the units consumption to the mobile but not to store any kind of data. Today the world is facing such an environment that offers challenges.
- Energy crisis is the main problem faced by our society. A relevant system to control and monitor the power usage is one of the solutions for this problem. One approach through which today's energy crisis can be addressed is through the reduction of power usage in households.
- The consumers are increasing rapidly and also burden on electricity offering divisions is sharply increasing.

3.2 PROPOSED SYSTEM

- The smart grid involves the application of advanced communications and control technologies and practices to improve reliability, efficiency, and security which are key ingredients in the on-going modernization of the electricity delivery infrastructure.
- Advanced metering infrastructure (AMI), which comprises smart meters, communication networks, and information management systems, is enhancing the operational efficiency of utilities and providing electricity customers with information to more effectively manage their energy use.
- Smart grid applications enable utilities to automatically locate and isolate faults to reduce outages, dynamically optimize voltage and reactive power levels for more efficient power use, and monitor asset health to guide maintenance.
- We are proposed the project to give the notification to the consumer side how much power they consumed depend upon the units once the units is reach above 50 automatically give the notification to the consumer side and depend upon the consumption LED indication is also present below 50 means GREEN LED is On, above 50 to 90 units means YELLOW LED IS ON, and once reach above 90 units means RED LED is ON
- To placing the current sensor in the transmitter side and receiver side if any one theft the power in-between the lines receiver side is get analyse power consumption automatically gives the indication through the LCD screen
- To automatically control the electrical appliance through internet because it does not having any kind of distance parameter and the continuously monitoring the data and stored in cloud

The smart EB involves the application of advanced communications and control technologies and practices to improve reliability, efficiency, and security which are key ingredients in the on-going modernization of the electricity delivery infrastructure. Advanced metering infrastructure (AMI), which comprises smart meters, communication networks, and information management systems, is enhancing the

operational efficiency of utilities and providing electricity customers with information to more

effectively manage their energy use. Smart grid applications enable utilities to automatically locate and isolate faults to reduce outages, dynamically optimize voltage and reactive power levels for more efficient power use, and monitor asset health to guide maintenance. By using button to manually restart the function.

3.2.1 OPERATION OF THE PROPOSED SYSTEM

Smart grid applications enable utilities to automatically locate and isolate faults to reduce out ages, dynamically optimize voltage and reactive power levels for more efficient power use, and monitor as set health to guide maintenance.

NEED OF THE SYSTEM

1. To design a smart grid using various sensors this can be controlled and monitored by the Raspberry Pi via the Internet of Things (IOT)
2. To provide a low cost platform for interconnecting electrical/electronic devices and various sensors in a home via the internet network.

3.2.2 ADVANTAGES:

- No manpower automated.
- More security than existing system.
- Less maintenance.
- More comfortable.
- Continuously monitoring.
- Current sensor sense the AC and DC current.
- Control the appliance at anywhere in the world.

3.3 BLOCK DIAGRAM:

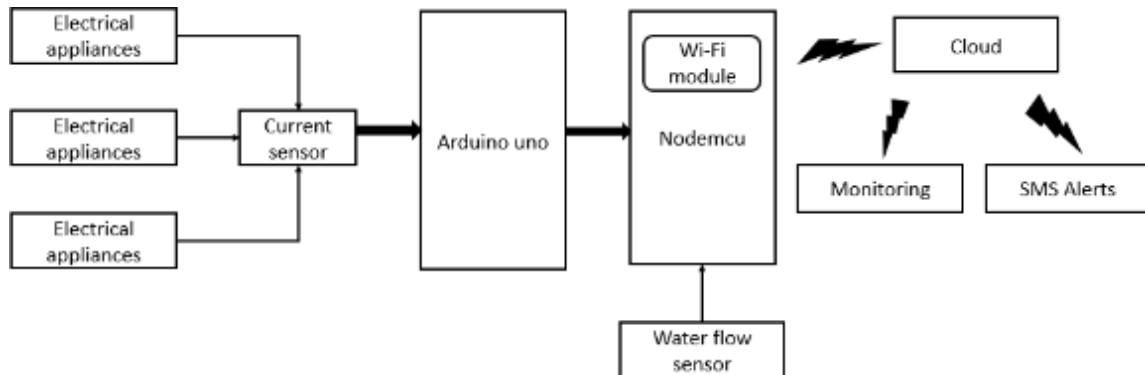


Fig. 3.1. Block diagram

POWER THEFT IDENTIFICATION

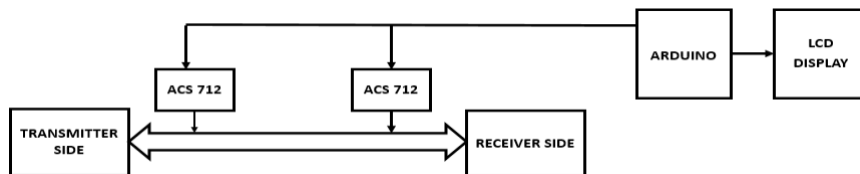


Fig. 3.2. power theft identification

3.4 REQUIREMENTS:

3.4.1 HARDWARE REQUIREMENTS:

- Arduino Uno
- NodeMcu
- Current sensor
- Electrical appliances (loads)
- Water flow sensor

3.4.2 SOFTWARE REQUIREMENTS:

- Arduino ide
- Embedded c
- Ubidots explorer

CHAPTER-4

IOT-INTERNET OF THINGS

4.1 INTRODUCTION:

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

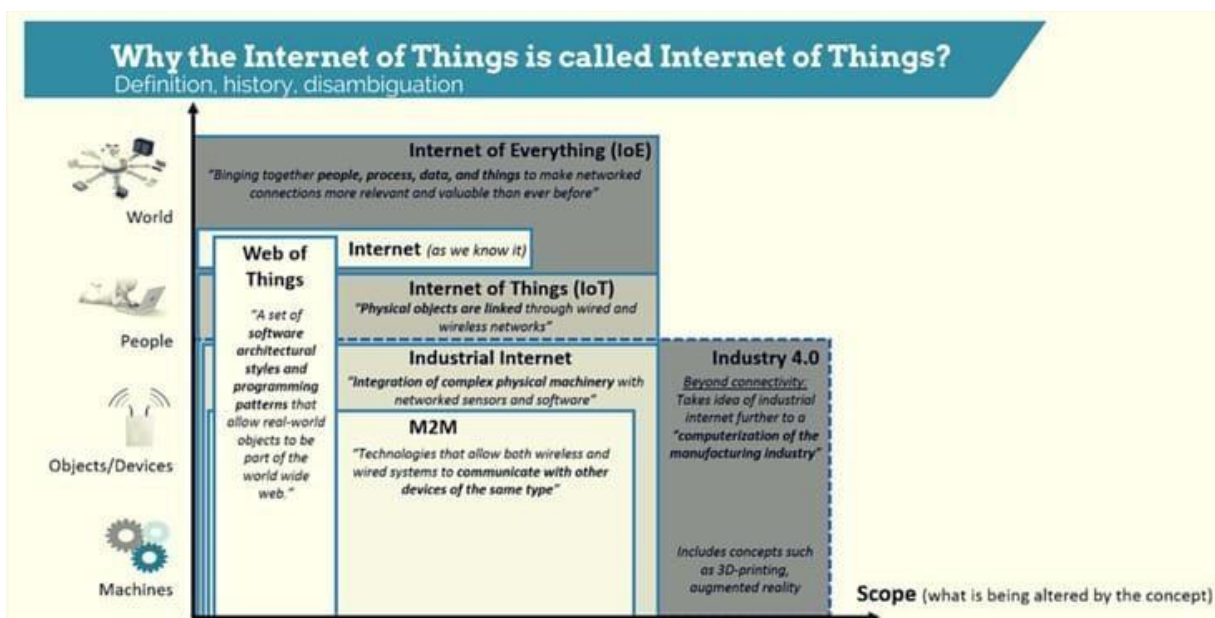


Fig.4.1. Introduction

4.2 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.

4.3 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.

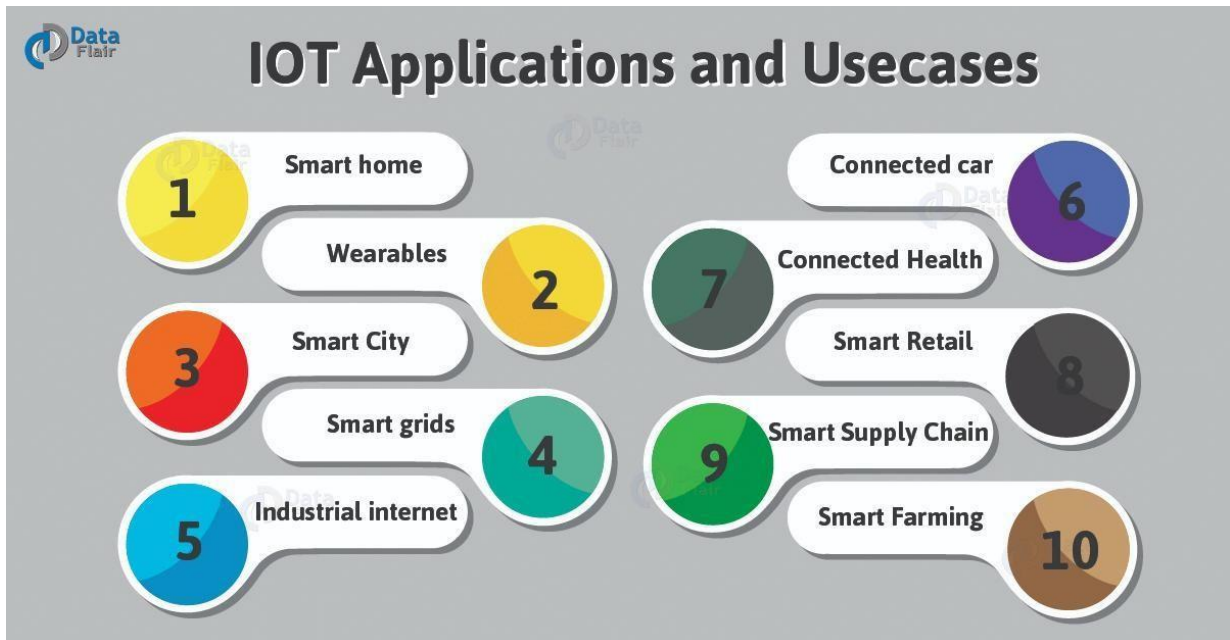


Fig.4.2 IoT Application

4.4 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 mind set. 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.

4.5 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.

4.6 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.

4.7 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. 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.

4.8 ENERGY MANAGEMENT:

Integration of sensing and actuation systems, connected to the Internet, is likely to optimize energy consumption as 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.

4.9 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.

4.10 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 Behavior. The integration of smart devices in the built environment and how they might be used in future applications.

4.11 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. 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.

4.12 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.

4.13 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.

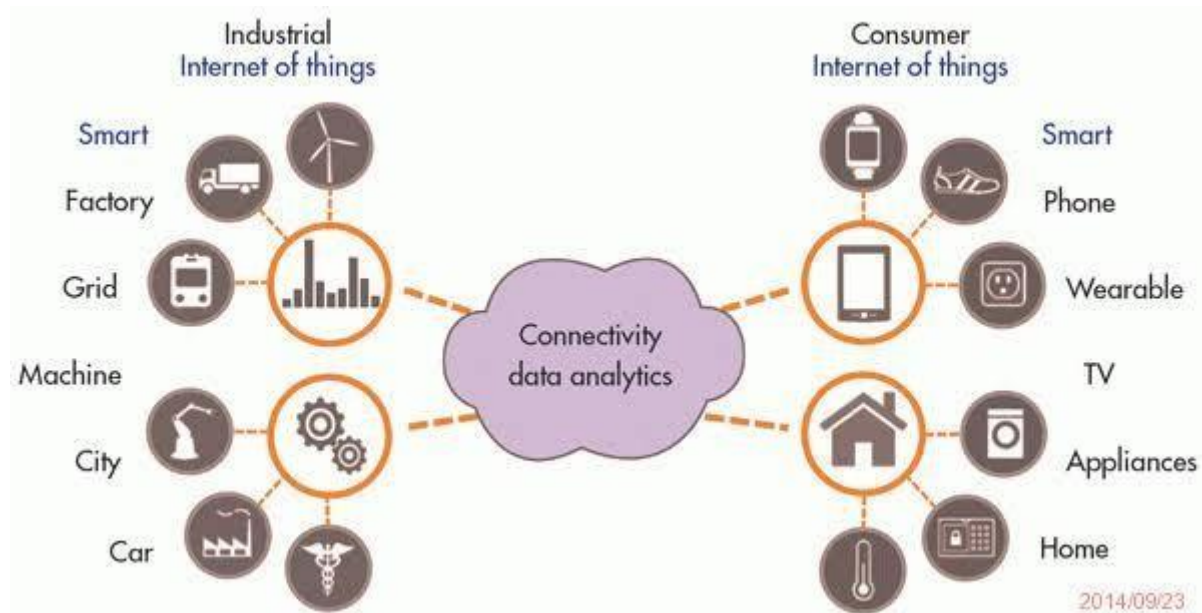


Fig.4.3. Consumer Application

4.14 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.

4.15 TRENDS AND CHARACTERISTICS

4.15.1 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.

4.15.2 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.

4.15.3 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.

4.16 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.

4.16.1 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.

4.16.2 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.

4.16.3 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.

4.16.4 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.

4.17 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

4.17.1 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 full fill:

4.17.2 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.

4.17.3 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.

4.17.4 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.

4.17.5 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.

4.18 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.

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.

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.

4.19 CRITICISM AND CONTROVERSIES

4.19.1 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.

4.19.2 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 panoptic on 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. 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.

4.19.3 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.

4.19.4 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 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. 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.

4.20 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."

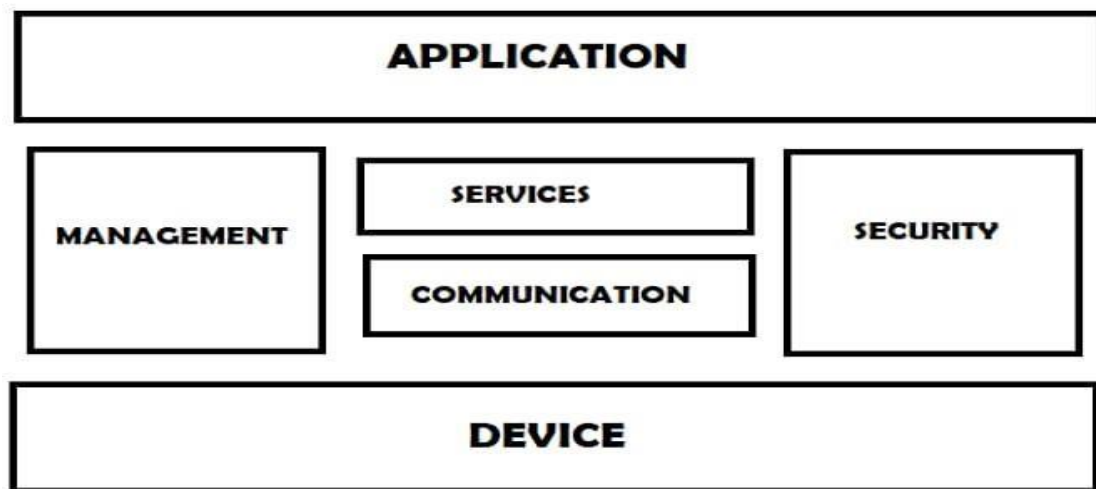


Fig.4.4. Design

4.21 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.

4.22 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 , disabled privacy settings on Android, Sony disabling Linux on PlayStation 3, and enforced EULA on Wii U.

4.23 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.

4.24 IOT ADOPTION BARRIERS

4.24.1 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.

4.24.2 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.

4.25 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 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.

4.26 Arduino Introduction:

Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board. The Arduino platform has become quite popular with people just starting out with electronics, and for good reason. Unlike most previous programmable circuit boards, the Arduino does not need a separate piece of hardware (called a programmer) in order to load new code onto the board – you can simply use a USB cable. Additionally, the Arduino IDE uses a simplified version of C++, making it easier to learn to program. Finally, Arduino provides a standard form factor that breaks out the functions of the micro-controller into a more accessible package.

4.26.1 What Does it Do?

The Arduino hardware and software was designed for artists, designers, hobbyists, hackers, newbies, and anyone interested in creating interactive objects or environments. Arduino can interact with buttons, LEDs, motors, speakers, GPS units, cameras, the internet, and even your smart-phone or your TV! This flexibility combined with the fact that the Arduino software is free, the hardware boards are pretty cheap, and both the software and hardware are easy to learn has led to a large community of users who have contributed code and released instructions for a **huge** variety of Arduino-based projects. For everything from robots and a heating pad hand warming blanket to honest fortune-telling machines, and even a Dungeons and Dragons dice-throwing gauntlet, the Arduino can be used as the brains behind almost any electronics project.

4.26.2 What's on the board?

There are many varieties of Arduino boards (explained on the next page) that can be used for different purposes. Some boards look a bit different from the one below, but most Arduinos have the majority of these components in common

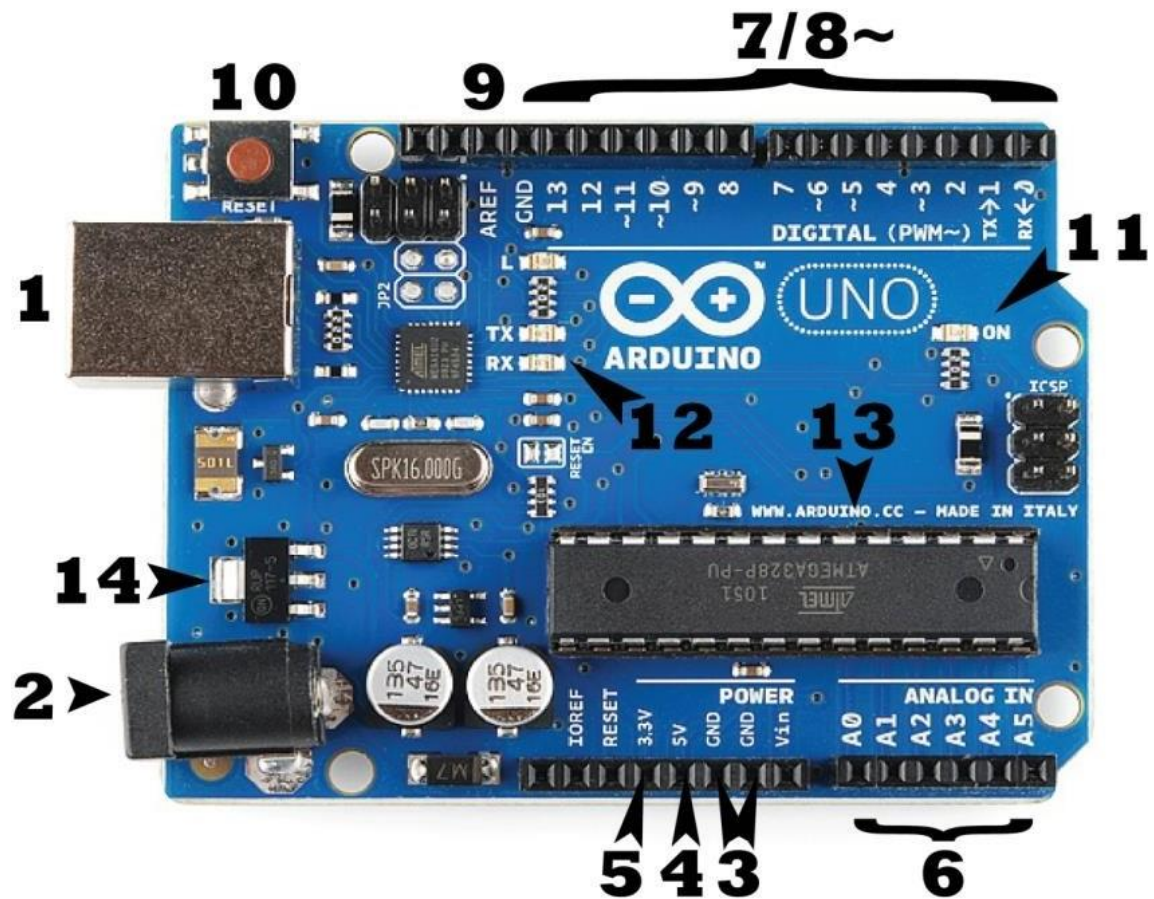


Fig.4.5. What on the Arduino Board

4.26.2.1 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 labeled **(1)** and the barrel jack is labeled **(2)**.

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.

4.26.2.2 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 labeled 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.

4.26.2.3 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.

4.26.2.4 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!

4.26.2.5 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).

4.26.2.6 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 ATmega 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.

4.26.2.7 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:

4.26.2.8 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 a AC-to-DC adapter or battery to get started.

ARDUINO IDE

The Arduino project provides the Arduino integrated development environment (IDE), which is across-platform application written in the programming language Java. It

originated hierarchy of operation menus. from the IDE for the languages Processing and Wiring. It includes a code editor with features such as text cutting and pasting, searching and replacing text, automatic indenting, brace matching, and syntax highlighting, and provides simple one-click mechanisms to compile and upload programs to an Arduino board. It also contains a message area, a text console, a toolbar with buttons for common functions.

A program written with the IDE for Arduino is called as sketch. Sketches are saved on the development computer as text files with the file extension `.ino`. Arduino Software (IDE) pre-1.0 saved sketches with the extension `.sketch`. The Arduino IDE supports the languages C and C++ using special rules of code structuring. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures. User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub `main ()` into an executable cyclic executive program with the GNU tool chain, also included with the IDE distribution.

The Arduino IDE employs the program `avrdude` to convert the executable code into a text file in hexadecimal encoding that is loaded into the Arduino board by a loader program in the board's firmware.

4.26.3 WHY ARDUINO?

Thanks to its simple and accessible user experience, Arduino has been used in thousands of different projects and applications. The Arduino software is easy to-use for beginners, yet flexible enough for advanced users. It runs on Mac, Windows, and Linux. Teachers and students use it to build low cost scientific instruments, to prove chemistry and physics principles, or to get started with programming and robotics. Designers and architects build interactive prototypes, musicians and artists use it for installations and to experiment with new musical instruments. Makers, of course, use it to build many of the projects exhibited at the Maker Faire, for example. Arduino is a key tool to learn new things. Anyone - children, hobbyists, artists, programmers - can start tinkering just following the step by step instructions of a kit, or sharing ideas online with other members of the Arduino community. There are many other microcontrollers and

microcontroller platforms available for physical computing. Parallax Basic Stamp, Net media's BX-24, Phidgets, MIT's Handy board, and many others offer similar functionality. All of these tools take the messy details of microcontroller programming and wrap it up in an easy-to-use package. Arduino also simplifies the process of working with microcontrollers, but it offers some advantage for teachers, students, and interested amateurs over other systems

ARDUINO:

The Arduino microcontroller is an easy to use yet powerful single board computer that has gained considerable traction in the hobby and professional market. The Arduino is open source, which means hardware is reasonably priced and development software is free. This guide is for students in ME 2011, or students anywhere who are confronting the Arduino for the first time. For advanced Arduino users, prowl the web; there are lots of resources. This guide covers the Arduino Uno board (Sparkfun DEV-09950, \$29.95), a good choice for students and educators. With the Arduino board, you can write programs and create interface circuits to read switches and other sensors, and to control motors and lights with very little effort. Many of the pictures and drawings in this guide were taken from the documentation on the Arduino site, the place to turn if you need more information. The Arduino section on the ME 2011 covers more on interfacing the Arduino to the real world. This is what the Arduino board looks like.



Fig.4.6.Arduino board

The Duemilanove board features an Atmel ATmega328 microcontroller operating at 5 V with 2 Kb of RAM, 32 Kb of flash memory for storing programs and 1 Kb of EEPROM for storing parameters. The clock speed is 16 MHz, which translates to about executing about 300,000 lines of C source code per second. The board has 14 digital I/O pins and 6 analog input pins. There is a USB connector for talking to the host computer and a DC power jack for connecting an external 6-20 V power source, for example a 9 V battery, when running a program while not connected to the host computer. Headers are provided for interfacing to the I/O pins using 22 g solid wire or header connectors. The Arduino programming language is a simplified version of C/C++. If you know C, programming the Arduino will be familiar. If you do not know C, no need to worry as only a few commands are needed to perform useful functions. An important feature of the Arduino is that you can create a control program on the host PC, download it to the Arduino and it will run automatically. Remove the USB cable connection to the PC, and the program will still run from the top each time you push the reset button. Remove the battery and put the Arduino board in a closet for six months. When you reconnect the battery, the last program you stored will run. This means that you connect the board to

the host PC to develop and debug your program, but once that is done, you no longer need the PC to run the program.

What You Need for a Working System

1. Arduino Duemilanove board
2. USB programming cable (A to B)
3. 9V battery or external power supply (for stand-alone operation)
4. Solderless breadboard for external circuits, and 22 g solid wire for connections
5. Host PC running the Arduino development environment. Versions exist for Windows, Mac and Linux

Installing the Software

Follow the instructions on the Getting Started section of the Arduino web site, <http://arduino.cc/en/Guide/HomePage>. Go all the way through the steps to where you see the pin 13 LED blinking. This is the indication that you have all software and drivers successfully installed and can start exploring with your own programs.

Connecting a Battery

For stand-alone operation, the board is powered by a battery rather than through the USB connection to the computer. While the external power can be anywhere in the range of 6 to 24 V (for example, you could use a car battery), a standard 9 V battery is convenient. While you could jam the leads of a battery snap into the Vin and Gnd connections on the board, it is better to solder the battery snap leads to a DC power plug and connect to the power jack on the board. A suitable plug is part number 28760 from www.jameco.com. Here is what this looks like.



Fig.4.7. Connecting a Battery

Warning: Watch the polarity as you connect your battery to the snap as reverse orientation could blow out your board.

Disconnect your Arduino from the computer. Connect a 9 V battery to the Arduino power jack using the battery snap adapter. Confirm that the blinking program runs. This shows that you can power the Arduino from a battery and that the program you download runs without needing a connection to the host PC .

Moving On

Connect your Arduino to the computer with the USB cable. You do not need the battery for now. The green PWR LED will light. If there was already a program burned into the Arduino, it will run.

Warning: Do not put your board down on a conductive surface; you will short out the pins on the back!

Start the Arduino development environment. In Arduino-speak, programs are called “sketches”, but here we will just call them programs. In the editing window that comes up, enter the following program, paying attention to where semi-colons appear at the end of command lines.

4.26.4 Using Arduino IDE:

The most basic way to use the ESP8266 module is to use serial commands, as the chip is basically a WiFi/Serial transceiver. However, this is not convenient. What we recommend is using the very cool Arduino ESP8266 project, which is a modified version of the Arduino IDE that you need to install on your computer. This makes it very convenient to use the ESP8266 chip as we will be using the well-known Arduino IDE. Following the below step to install ESP8266 library to work in Arduino IDE environment.

Install the ESP8266 Board Package

Enter http://arduino.esp8266.com/stable/package_esp8266com_index.json into Additional Board Manager URLs field in the Arduino v1.6.4+ preferences.

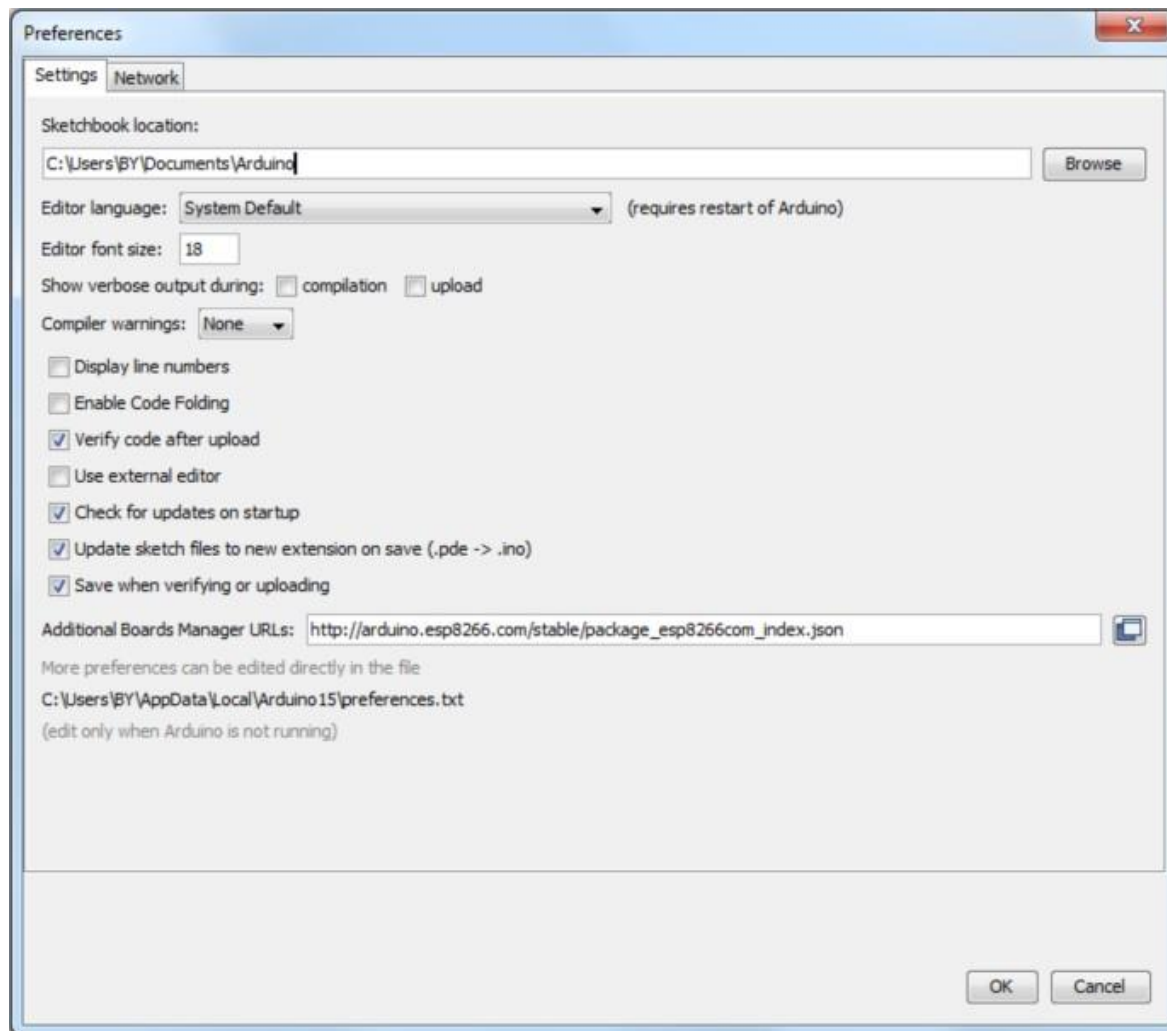


Fig.4.8. preference

Click 'File' -> 'Preferences' to access this panel. Next, use the Board manager to install the ESP8266 package.

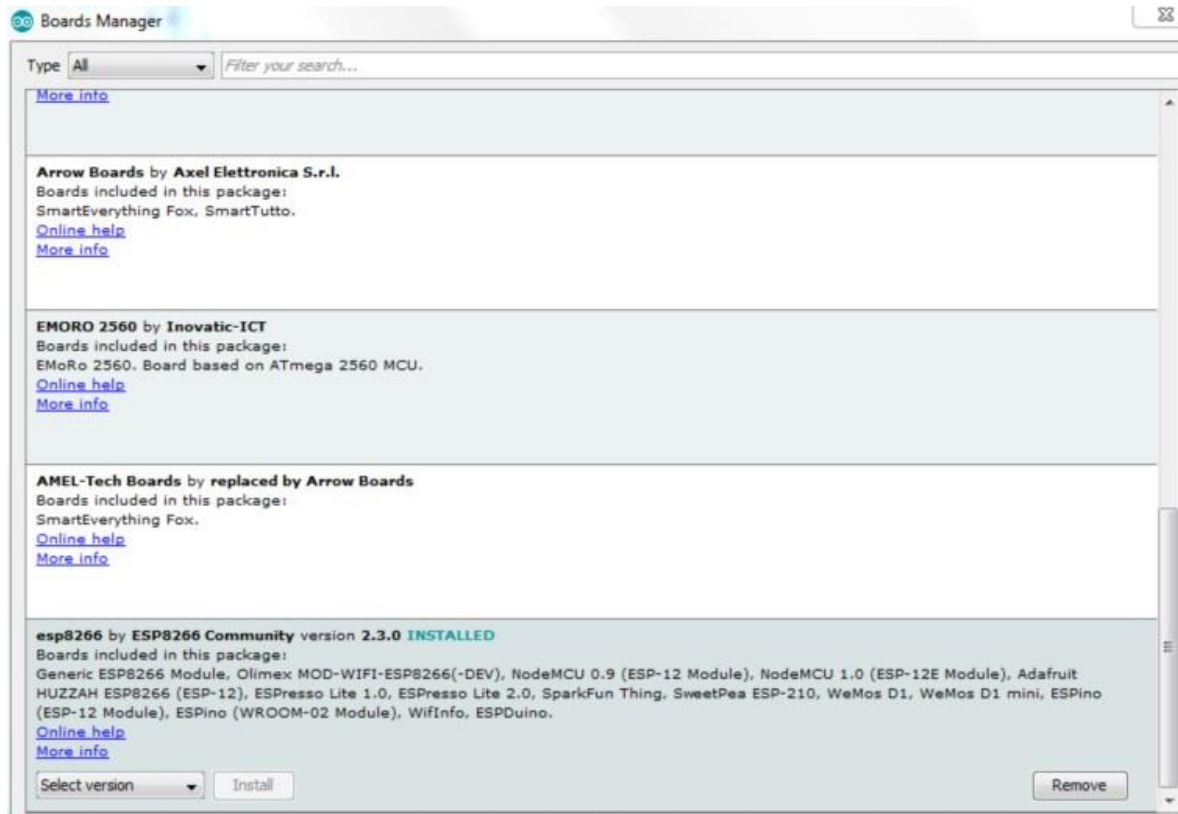


Fig.4.9. Boards Manger

Click 'Tools' -> 'Board:' -> 'Board Manager...' to access this panel. Scroll down to 'esp8266 by ESP8266 Community' and click "Install" button to install the ESP8266 library package. Once installation completed, close and re-open Arduino IDE for ESP8266 library to take effect.

Setup ESP8266 Support

When you've restarted Arduino IDE, select 'Generic ESP8266 Module' from the 'Tools' -> 'Board:' dropdown menu.

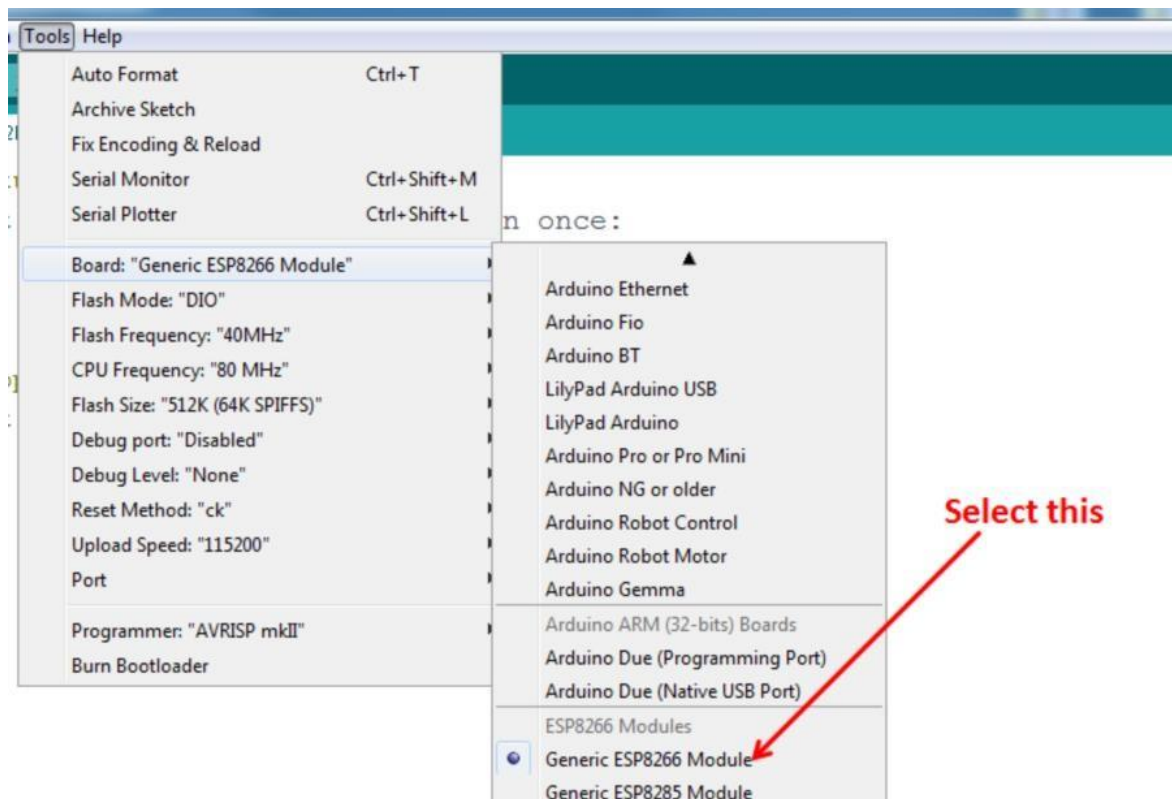


Fig.4.10.1. setup

Select 80 MHz as the CPU frequency (you can try 160 MHz overclock later)

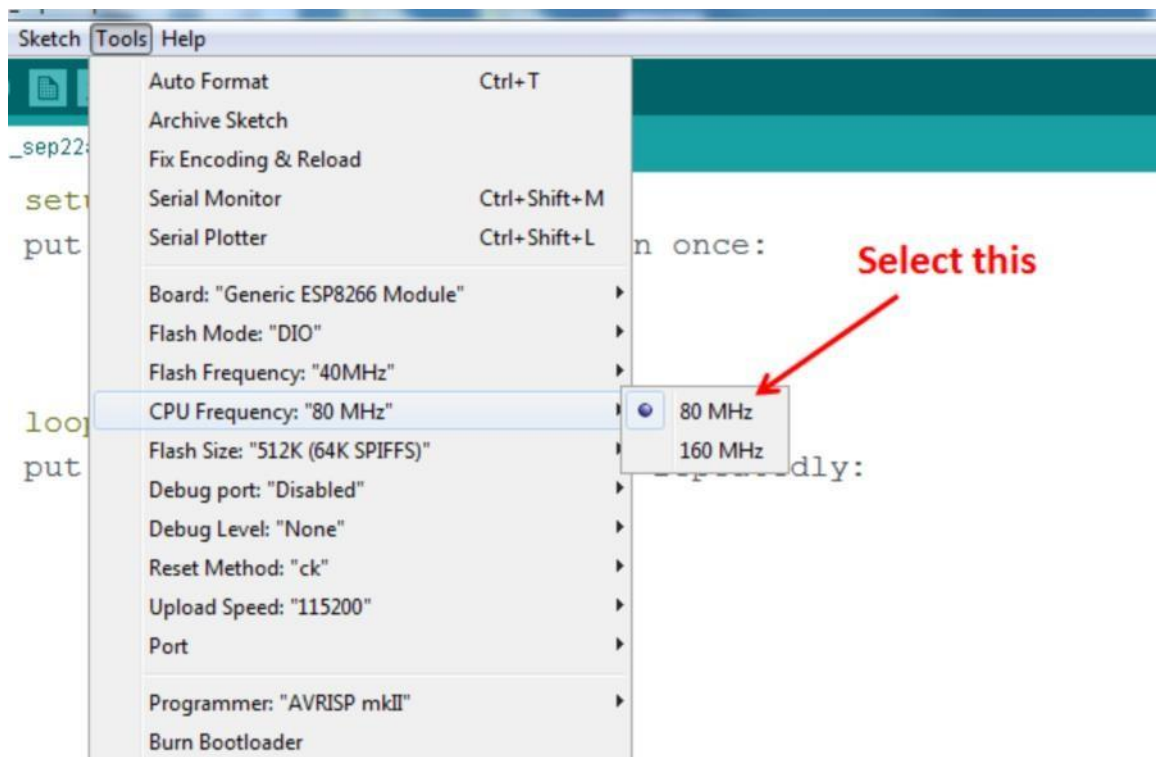


Fig.4.10.2. Setup

Select '115200' baud upload speed is a good place to start - later on you can try higher speeds but 115200 is a good safe place to start.

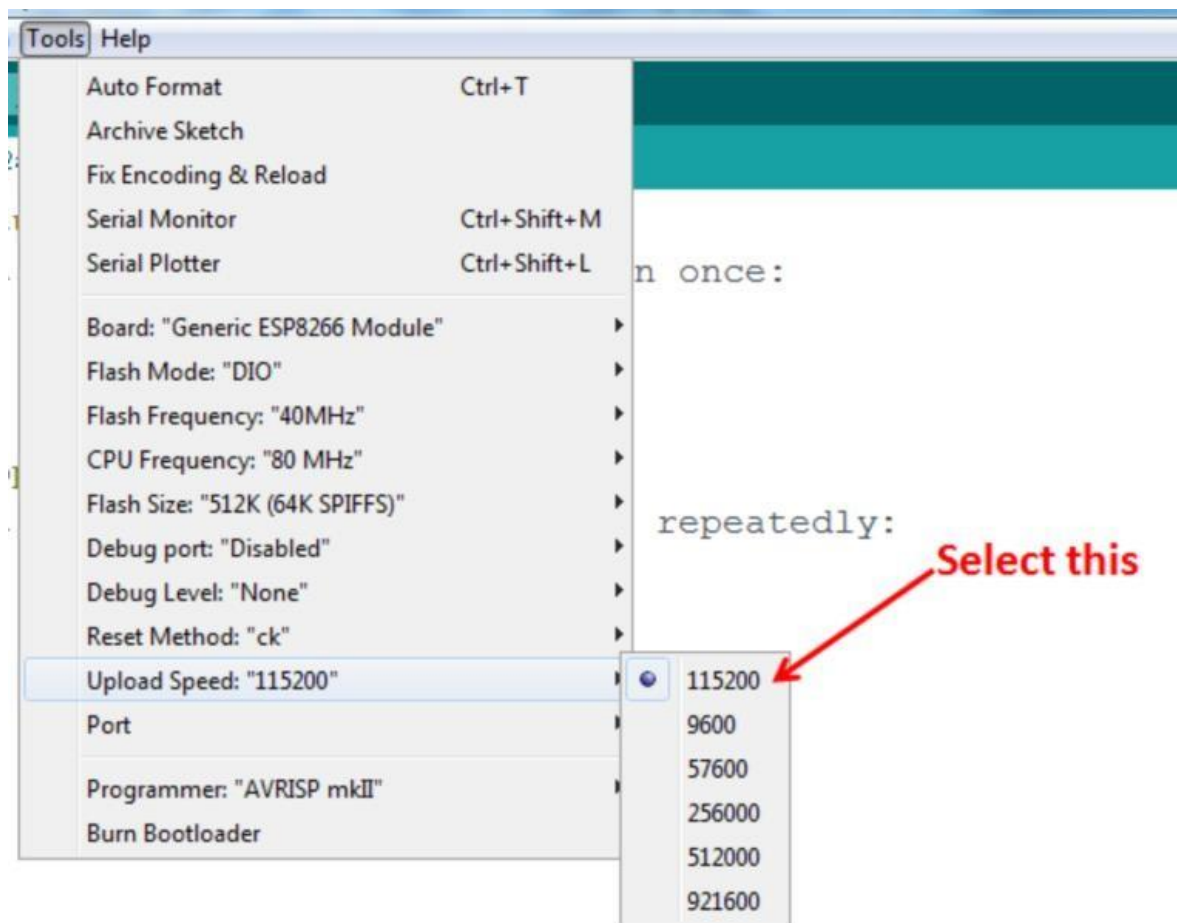


Fig.4.10.3.Setup

Go to your Windows 'Device Manager' to find out which Com Port 'USB-Serial CH340' is assigned to. Select the matching COM/serial port for your CH340 USB-Serial interface.

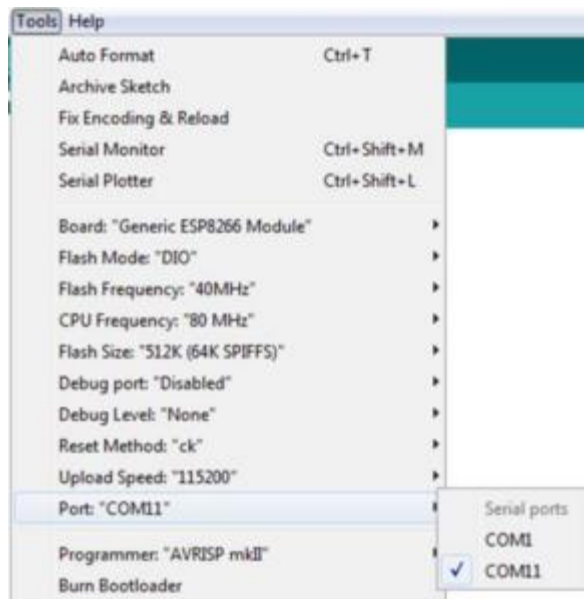
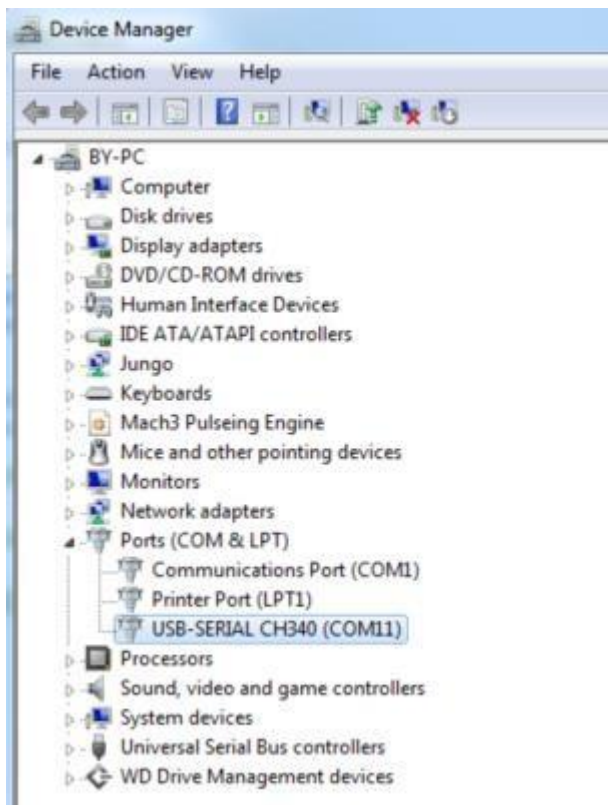


Fig.4.10.4.Setup

Blink Test

We'll begin with the simple blink test. Enter this into the sketch window (and save since you'll have to). Connect a LED as shown in Figure3-1.

Now you'll need to put the board into bootload mode. You'll have to do this before

each upload. There is no timeout for bootloader mode, so you don't have to rush!

- Hold down the 'Flash' button.
- While holding down 'Flash', press the 'RST' button.
- Release 'RST', then release 'Flash'.

Once the ESP board is in bootloader mode, upload the sketch via the IDE.

Flashing NodeMCU Firmware on the ESP8266 using Windows

NodeMCU is a firmware that allows you to program the ESP8266 modules with LUA script. And you'll find it very similar to the way you program your Arduino. With just a few lines of code you can establish a WiFi connection, control the ESP8266 GPIOs, turning your ESP8266 into a web server and a lot more. In this tutorial we are going to use another ESP8266 module with pin header adapter board which is breadboard friendly.



ESP8266 Module Breadboard Friendly with Header Connector

Pin Assignment:

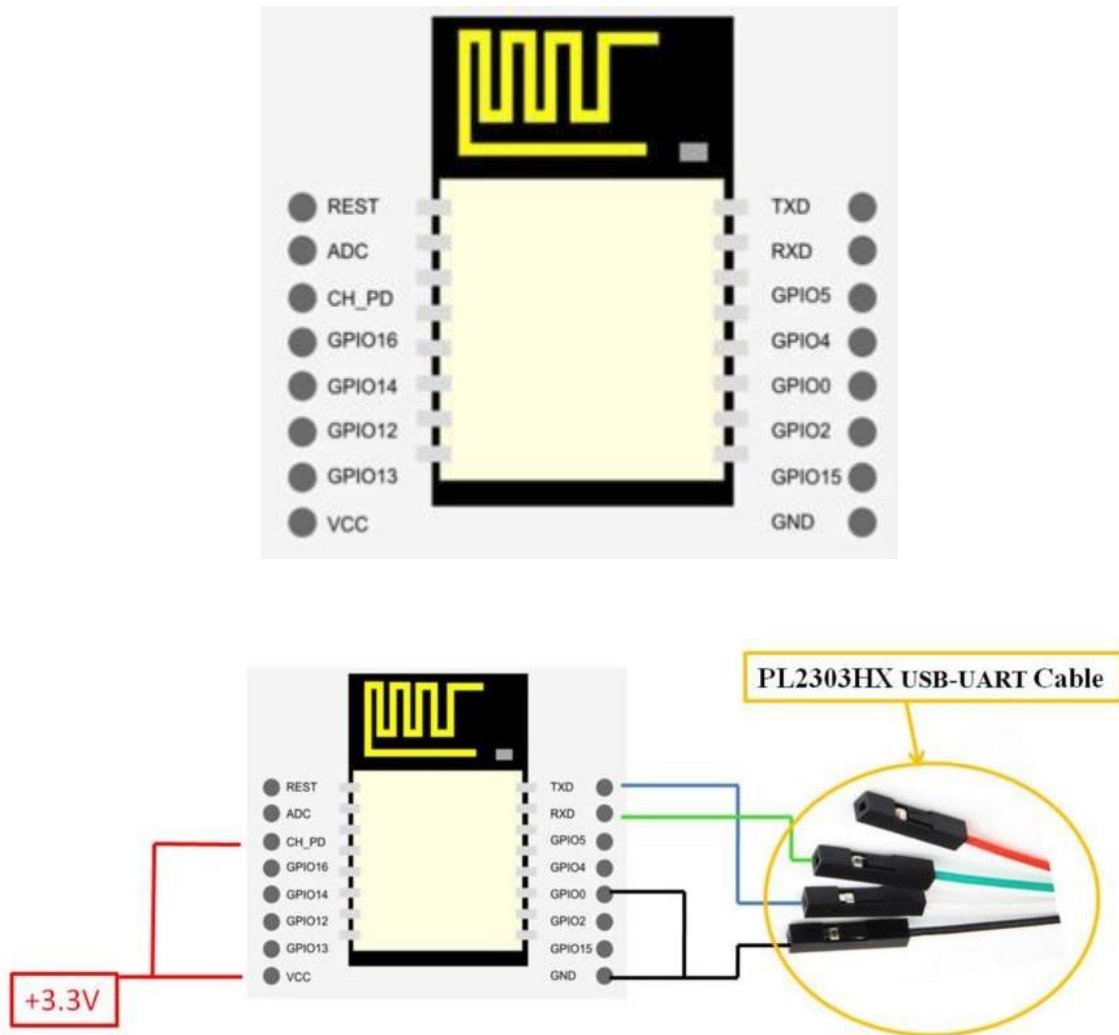


Fig.4.11 .HEARTBEAT SENSOR

4.27 ESP8266 NodeMCU Wi-Fi Devkit:

The **ESP8266** is a low-cost **Wi-Fi** microchip, with a full TCP/IP stack and microcontroller capability, produced by Espressif Systems in Shanghai, China..... This small **module** allows microcontrollers to connect to a **Wi-Fi** network and make simple TCP/IP connections using Hayes-style commands.

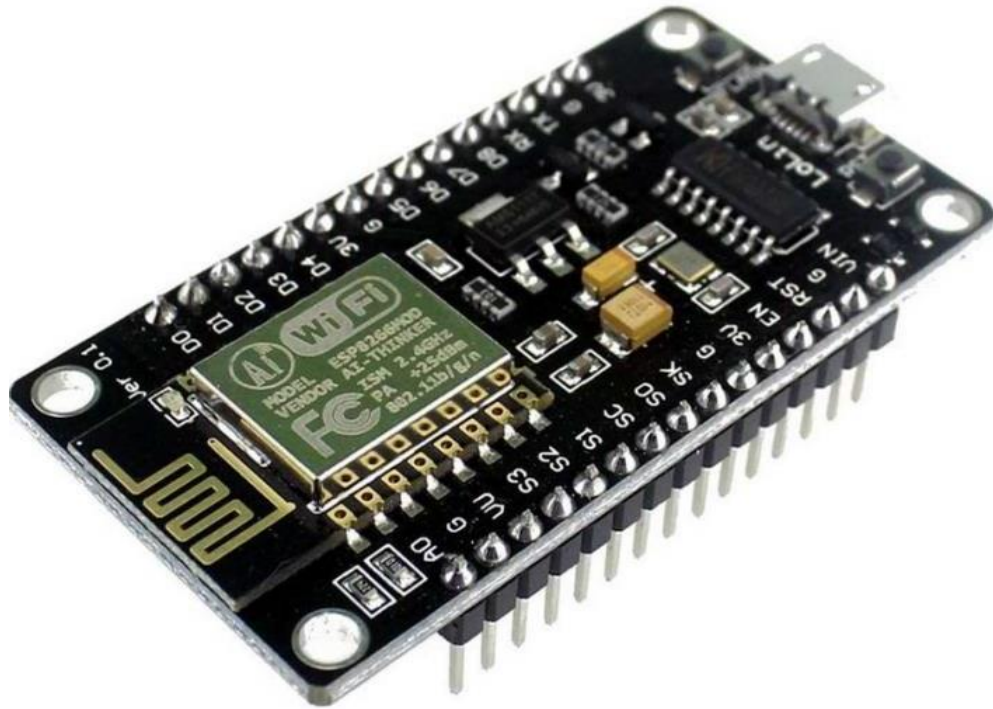


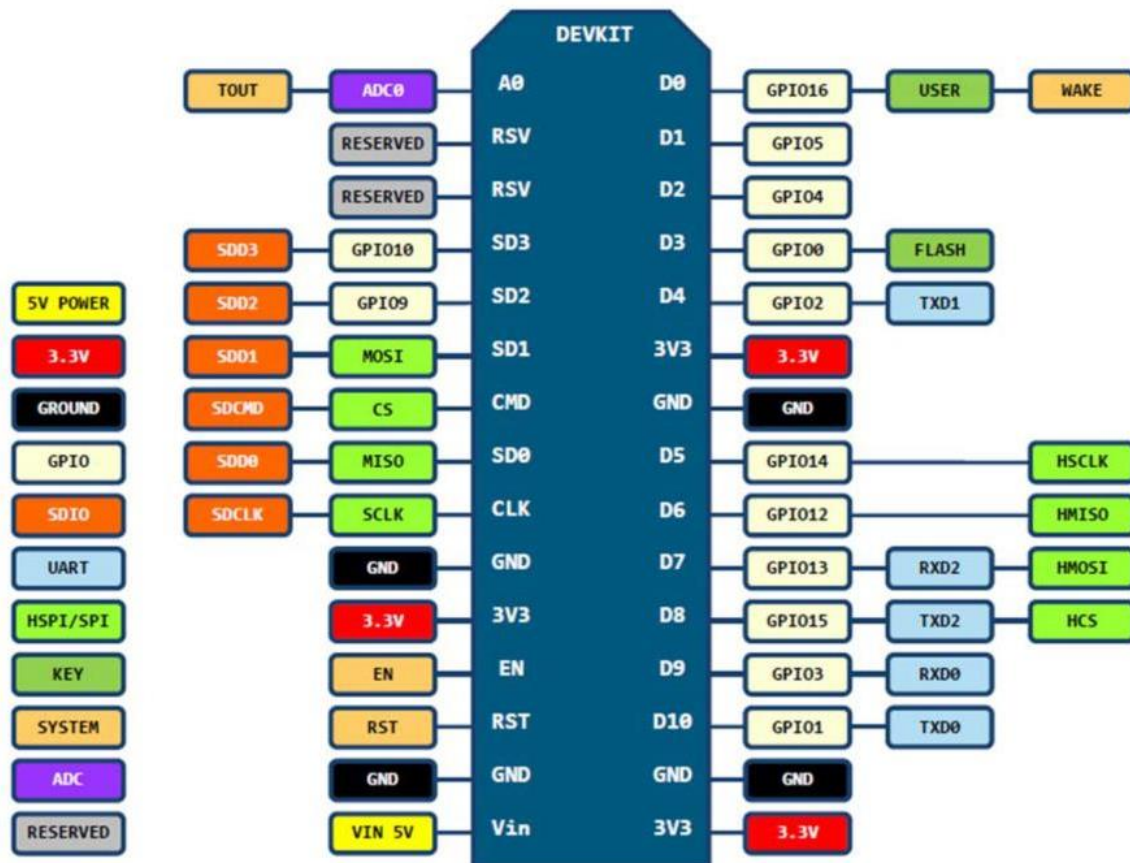
Fig.4.12. NodeMUC wifi kit

4.27.1 Specification:

- Voltage: 3.3V.
- Wi-Fi Direct (P2P), soft-AP.
- Current consumption: 10uA~170mA.
- Flash memory attachable: 16MB max (512K normal).
- Integrated TCP/IP protocol stack.
- Processor: Tensilica L106 32-bit.
- Processor speed: 80~160MHz.
- RAM: 32K + 80K.
- GPIOs: 17 (multiplexed with other functions).
- Analog to Digital: 1 input with 1024 step resolution. • +19.5dBm output power in 802.11b mode
- 802.11 support: b/g/n.

Maximum concurrent TCP connections: 5.

Pin Definition:



D0(GPI016) can only be used as gpio read/write, no interrupt supported, no pwm/i2c/ow supported.

Fig.4.13.Pin Definition

4.28 RELAYS

A relay is an electro-magnetic switch which can be used in case of using a low voltage circuit to switch on and off a light bulb (or anything else) connected to the 220v mains supply, i.e., it 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 most have doubled left row (change over). Relay allow one circuit to switch a second circuit which is completely separated from the first. For example a low voltage battery circuit can use a relay to switch a 230VAC mains circuit. There is no electrical connection inside the relay between the two circuits the link is magnetic and mechanical

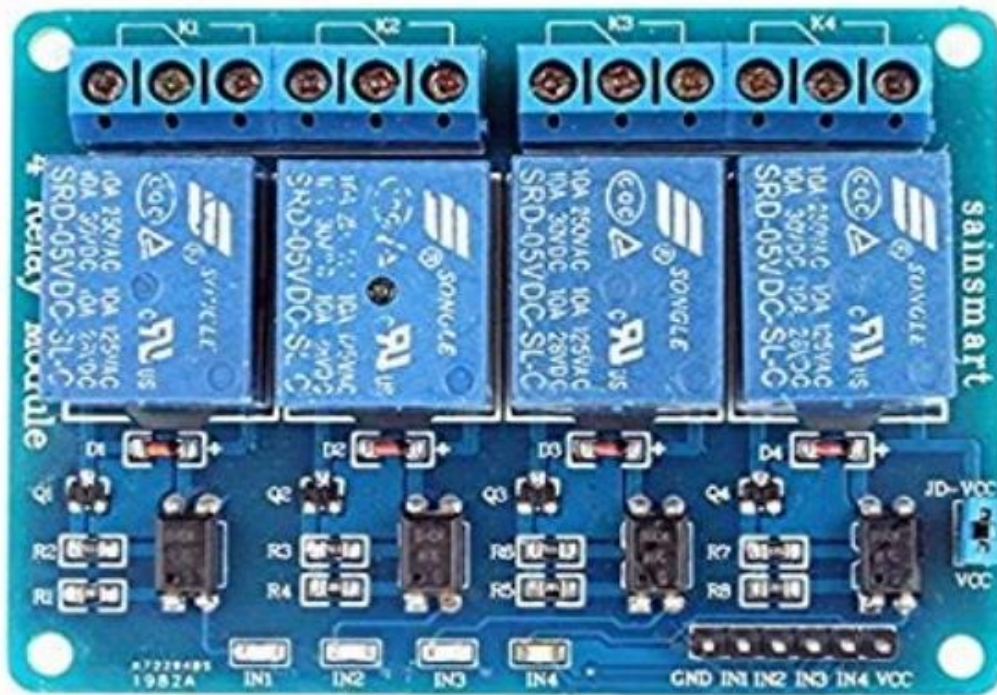


Fig .4.14.Relays

4.29 WATER FLOW SYSTEM

4.29.1 Water Flow Sensor:

Sensors play a very crucial role in today's automatic systems. Being a small, low cost and reliable device, sensors are easy to embed with larger electronics. Today we can find various types of sensors in the market. With the advance in technology, sensors are also evolved in their functioning and size. From the early size of cm units, size of sensors has shrunk to the scale of nm. Sensors have also solved many challenges of electronic and electrical engineering such as finding the intensity of ambient light, determining the temperature in the furnace, calculating humidity of surrounding, etc.... Water flow sensor gives an amazing solution for measuring the flow rate of liquids.

What is Water Flow Sensor?

Huge industrial plants, commercial and residential buildings require a large amount of water supply. The public water supply system is used to meet this requirement. To monitor the amount of water being supplied and used, the rate of flow of water has to be measured. Water flow sensors are used for this purpose.



Fig.4.15. Water Flow Sensor

Water Flow Sensor

Water flow sensors are installed at the water source or pipes to measure the rate of flow of water and calculate the amount of water flowed through the pipe. Rate of flow of water is measured as liters per hour or cubic meters.

4.29.2 Working Principle

Water flow sensor consists of a plastic valve from which water can pass. A water rotor along with a Hall Effect sensor is present to sense and measure the water flow.

When water flows through the valve it rotates the rotor. By this, the change can be observed in the speed of the motor. This change is calculated as output as a pulse signal by the Hall effect sensor. Thus, the rate of flow of water can be measured.

The main working principle behind the working of this sensor is the Hall Effect. According to this principle, in this sensor, a voltage difference is induced in the conductor due to the rotation of the rotor. This induced voltage difference is transverse to the electric current.

When the moving fan is rotated due to the flow of water, it rotates the rotor which induces the voltage. This induced voltage is measured by the Hall Effect sensor and displayed on the LCD display.

The water flow sensor can be used with hot waters, cold waters, warm waters, clean water, and dirty water also. These sensors are available in different diameters, with different flow rate ranges.

These sensors can be easily interfaced with microcontrollers like Arduino. For this, an Arduino microcontroller board for processing, a Hall Effect water flow sensor, a 16×2 LCD display, and Breadboard connecting wires are required. The sensor is placed at the water source inlet or at the opening of the pipe.

The sensor contains three wires. Red wire to connect with supply voltage. Black wire to connect to ground and a yellow wire to collect output from Hall Effect sensor. For

supply voltage 5V to 18V of DC is required.

4.29.3 Applications of Water Flow Sensor:

Water flow sensors can measure the rate of flow of water either by measuring velocity or displacement. These sensors can also measure the flow of water like fluids such as measuring milk in a dairy industry etc. There are various types of water flow sensors available based on their diameter and method of measuring. A cost-effective and most commonly used water flow sensor is Paddlewheel sensor. It can be used with water-like fluids. For the type of applications where a straight pipe is not available for inlet, Positive displacement flow meter is used. This type of water flow sensor can be used for viscous liquids also. For working with dirty water and wastewater which may be conductive, Magnetic flow meter is used. For applications such as sewage water, slurries, and other dirty liquids Ultrasonic flow meters are used. The LCD display is used to display the measurements. The magnetic Hall Effect water flow sensor outputs a pulse of every revolution of the rotor. The Hall Effect sensor present in the device is sealed from water to keep it safe and dry.

Example of Water Flow Sensor

YFS201 Hall effect sensor is an example of this sensor. These sensors also require a display to display the measurements. This sensor outputs 4-5 pulses for every liter of liquid flowing through it per minute. It has a working flow rate of 1-30liters per minute. Easy to use and cost-effectiveness are the important characteristics of this sensor. Which of the water flow sensor have you

CHAPTER-5

RESULTS

OUTPUT 1:

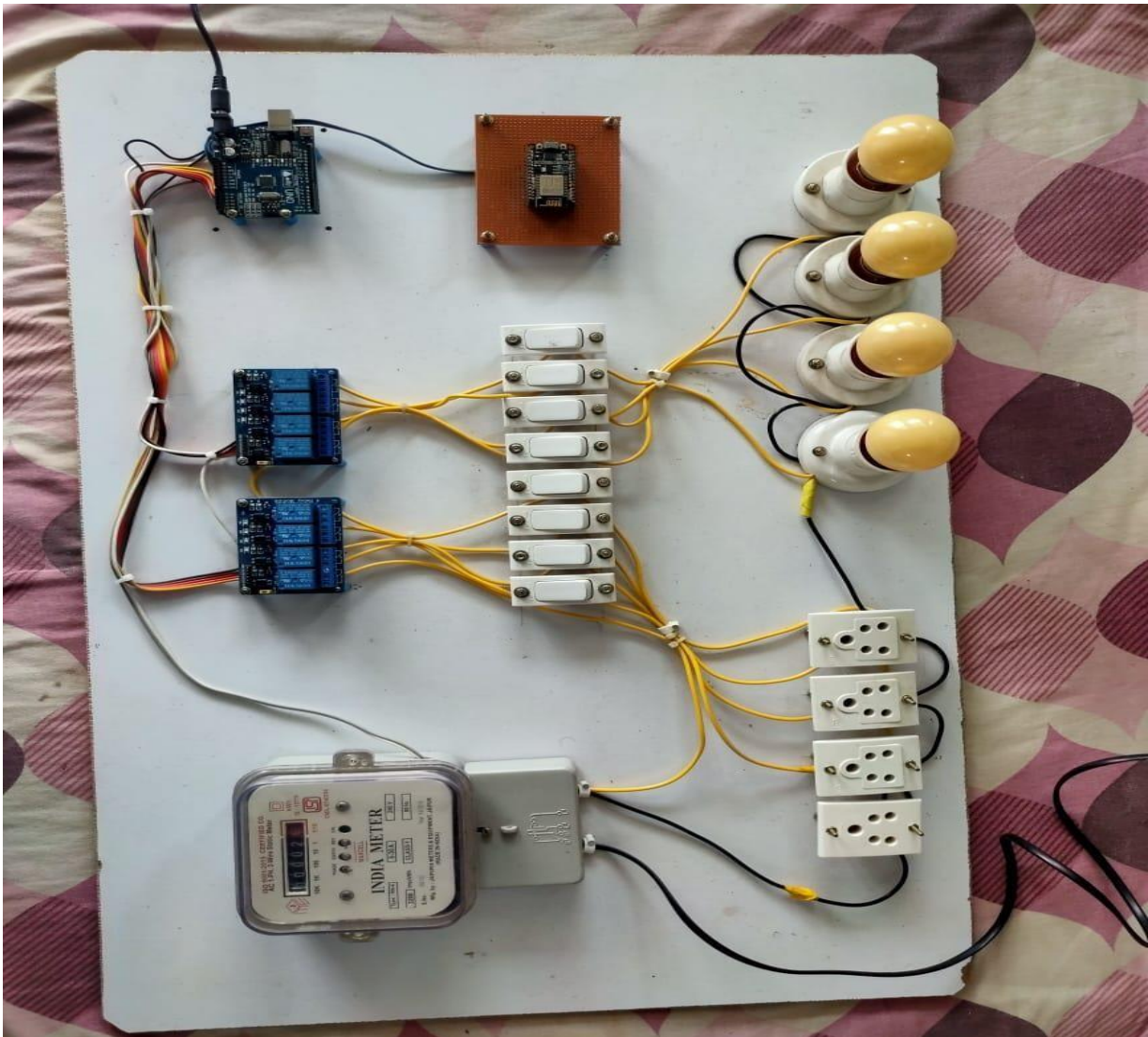


Fig.5.1.output 1

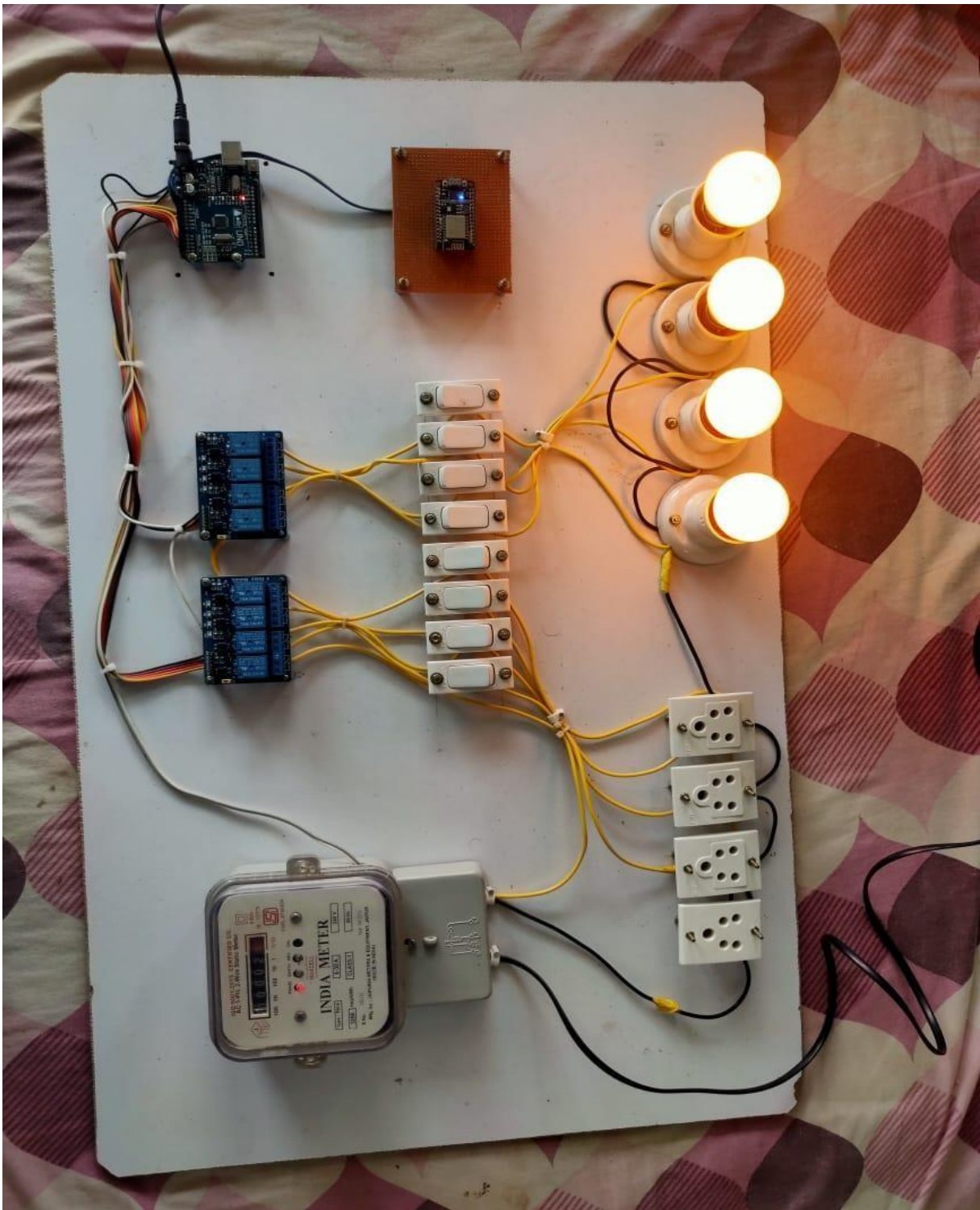


Fig.5.2. output 2

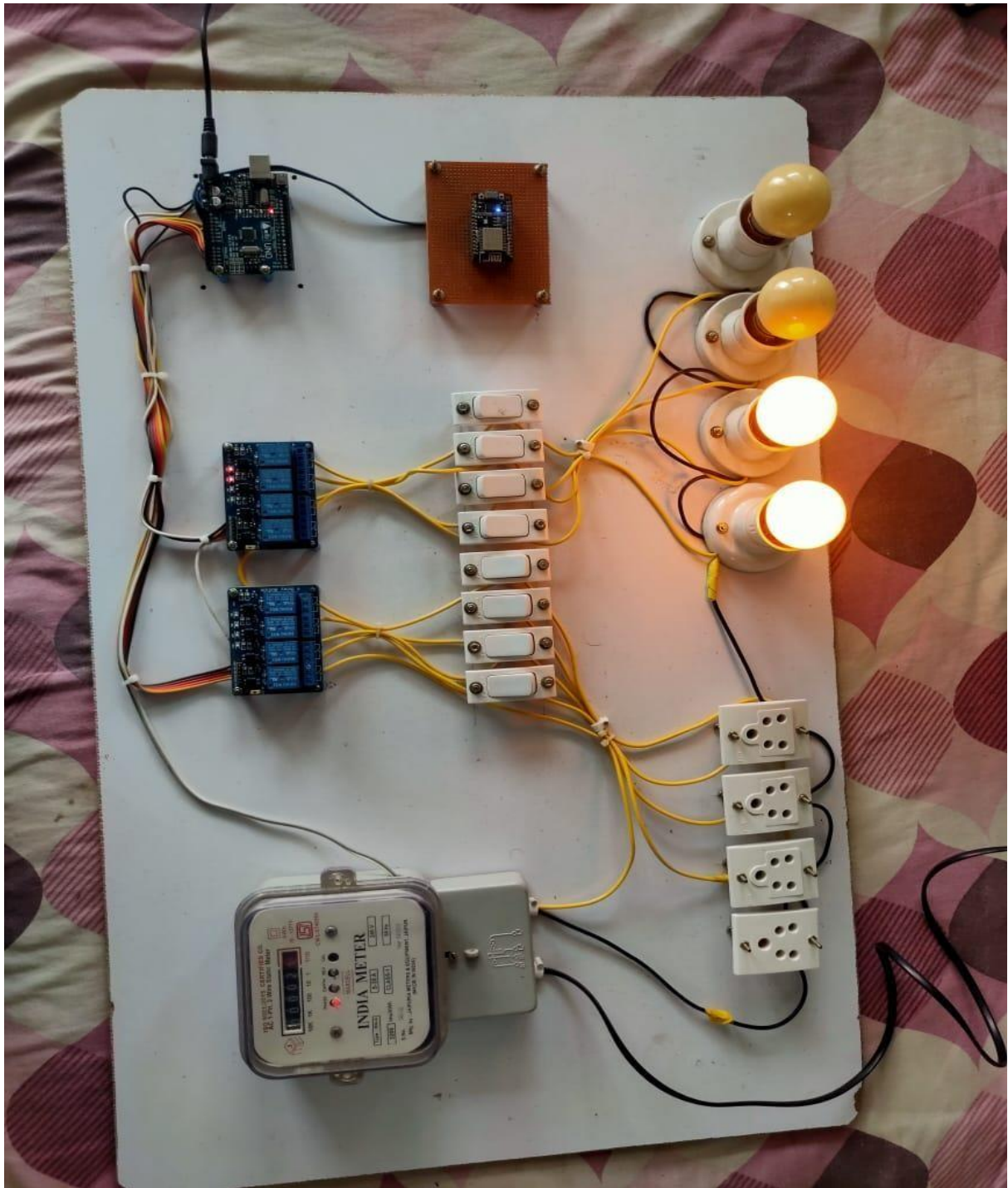


Fig.5.3. output 3

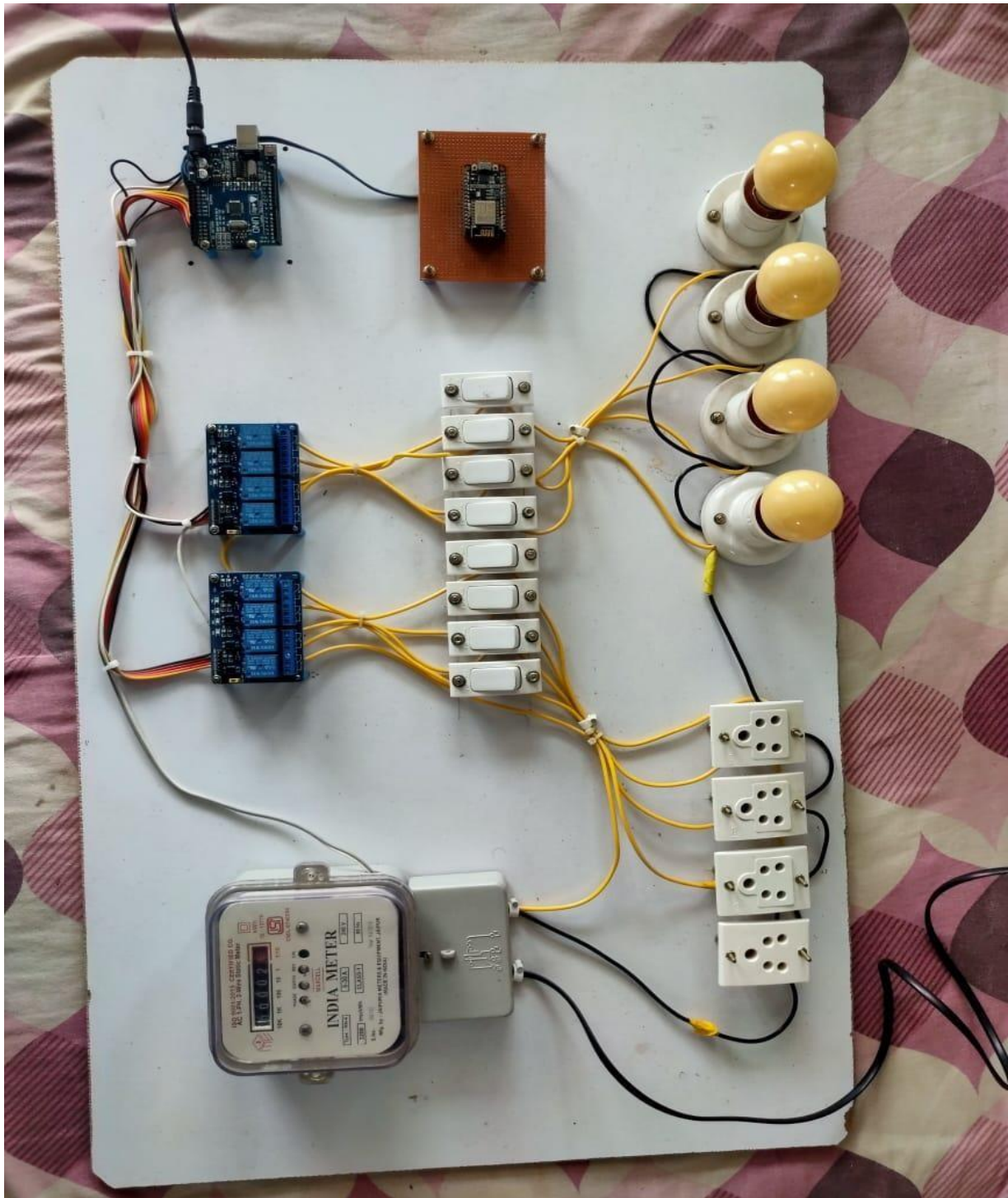


Fig.5.4. output 4

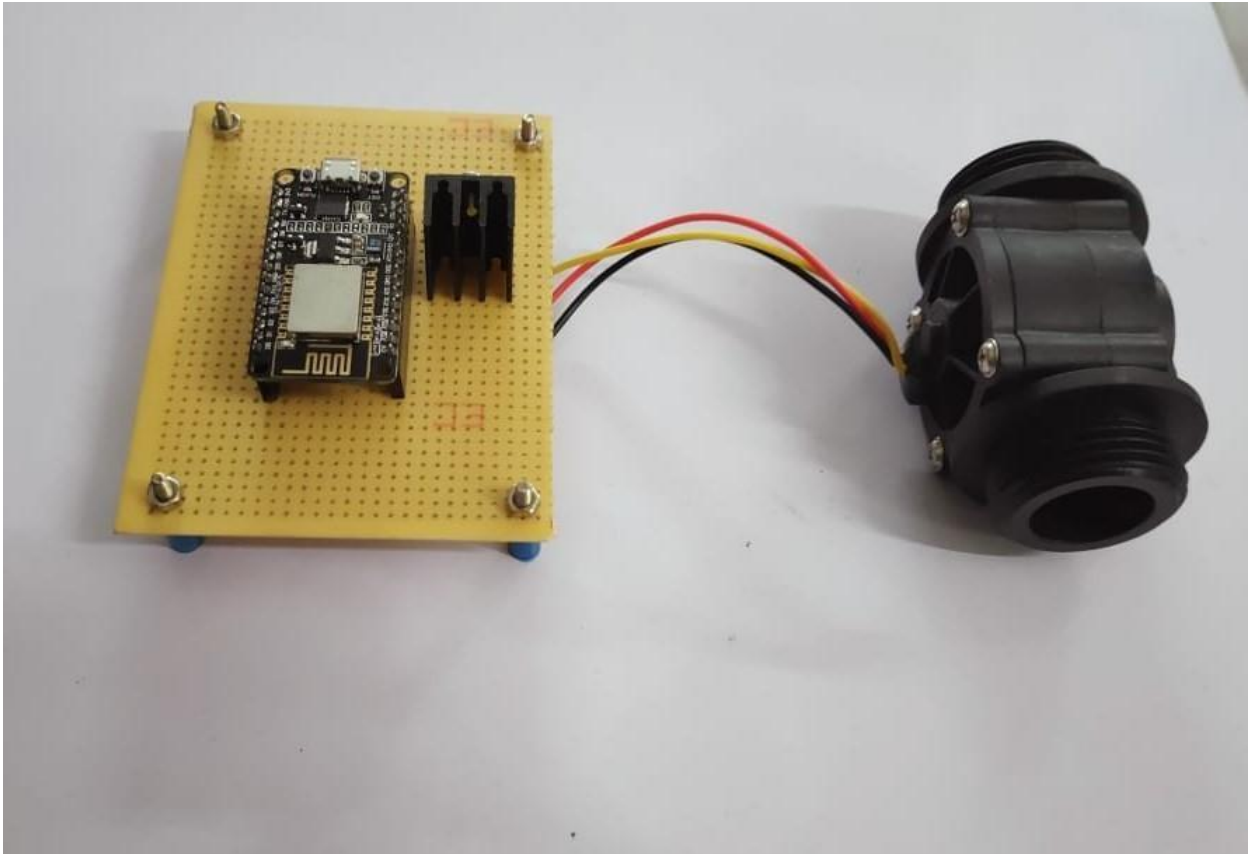


Fig.5.5 output 5

5.2 CONCLUSION:

In the era of smart city advancement, this project is concentrated on the connectivity and networking factor of the IOT. In this system, an energy consumption calculation based on the counting of calibration pulses is designed and implemented using ATMEGA328P Microcontroller unit in embedded system domain. In the proposed work, IOT and MMC based meter reading system is designed to continuously monitor the meter reading and service provider can Disconnect the power source whenever the customer does not pay the monthly bill and also it eliminates the human Involvement, delivers effective meter reading, prevent the billing mistake. The Project has achieved following objectives: Ease of accessing information for consumer from energy meter through IOT.

CHAPTER-6

6.0 REFERENCE:

- [1] Landi, C.; Dipt. Di Ing. dell'Inf., Seconda Univ. di Napoli, Aversa, Italy Merola, P. Ianniello, G, "ARM-based energy management system using smart meter and Web server", IEEE Instrumentation and Measurement Technology Conference Binjiang pp. 1 – 5, May 2011.
- [2] Garrab, A.; Bouallegue, A.; Ben Abdallah, "A new AMR approach for energy saving in Smart Grids using Smart Meter and partial Power Line Communication", IEEE First International Conference on Renewable Energies and Vehicular Technology (REVET), pp.263 – 269 march 2012.
- [3] B. S. Koay, S. S. Cheah, Y. H. Sng, P. H. Chong, P. Shum, Y. C. Tong, X. Y. Wang, Y. X. Zuo and H. W. Kuek, "Design and implementation of Bluetooth energy meter", IEEE Proceedings of the 4th International Joint Conference of the ICICS, vol. 3, pp. 1474-1477, Dec,2003.
- [4] K. Li, J. Liu, C. Yue and M. Zhang, "Remote power management and meter-reading system based on ARM microprocessor", IEEE Precision Electromagnetic Measurements Digest CPEM, pp. 216-217, June, 2008.
- [5] Steven Lanzisera, Member, IEEE, Andrew R. Weber, Anna Liao, Dominic Pajak, and Alan K. Meier, "Communicating Power Supplies: Bringing the Internet to the Ubiquitous Energy Gateways of Electronic Devices", IEEE Internet of Things Journal, vol. 1, no. 2, pp.153-160, march 2014.
- [6] Andrea Zanella, Senior Member, IEEE, Nicola Bui, Angelo Castellani , Lorenzo Vangelista, Senior Member, IEEE, and Michele Zorzi, Fellow, IEEE, "Internet of Things for Smart Cities", IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, February 2014.
- [7] poonam Borle, Ankitha Saswadhar, Deepali Hiwarkar, Rupali S Kali,

“Automatic Meter Reading for Electricity”,International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, no. 3,pp. 982-987, March 2013.

[8] http://wiki.iteadstudio.com/ESP8266_Serial_WIFI_Module.

[9] Microchip, “High-Performance Microcontrollers with XLP Technology PIC18 (L)F2X/4XK22”, DS41412F Data Sheet, 2010-2012.

[10] Microchip, “Microcontrollers with 10-Bit A/D and Nano Watt Technology PIC18F2420/2520/4420/4520”, DS39631E Data Sheet, 2008.

[11] K. Li, J. Liu, C. Yue and M. Zhang, "Remote power management and meter-reading system based on ARM microprocessor", IEEE Precision Electromagnetic Measurements Digest CPEM, pp. 216-217, June 2008.

[12] Steven Lanzisera, Member, IEEE, Andrew R. Weber, Anna Liao, Dominic Pajak, and Alan K. Meier, “Communicating Power Supplies: Bringing the Internet to the Ubiquitous Energy Gateways of Electronic Devices”, IEEE Internet of Things Journal, vol. 1, no. 2, pp.153-160, march 2014.

[13] Andrea Zanella, Senior Member, IEEE, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Senior Member, IEEE, and Michele Zorzi, Fellow, IEEE, “Internet of Things for Smart Cities”, IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22-32, February 2014.

[14] Poonam Borle, Ankitha Saswadhar, Deepali Hiwarkar, Rupali S Kali, “Automatic Meter Reading for Electricity”,International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, no. 3,pp. 982-987, March 2013.

[15] http://wiki.iteadstudio.com/ESP8266_Serial_WIFI_Module.