ARMY SOLDIER MONITORING USING IOT

Submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in Electronics and Communication Engineering

by

ADABALA HARI VAMSI (37130004)

ALIKEPALLI SRINIVASA REDDY(37130016)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SCHOOL OF ELECTRICAL AND 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

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY (DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC 1 12B Status by UGC I Approved by AICTE

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 Adabala Hari Vamsi(37130004) A.Srinivasa Reddy(37130016) who carried out the project entitled **"ARMY SOLDIER MONITORING USING IOT"** under my supervision from November 2020 to March 2021.

Internal Guide& Head of the Department

Dr.S.LALITHA KUMARI, M.E., Ph.D.

Submitted for Viva voce Examination held on_____

Internal Examiner **External Examiner**

DECLARATION

We, Adabala Hari Vamsi (Reg. No.37130004) and A.Srinivasa Reddy (Reg.No.37130016) hereby declare that the Project Report entitled **"Analysis of XOR-MUX Full adder based computational block for low power architecture"** done by us under the guidance of **Dr.S.Lalitha Kumari, M.E. Ph.D.,** at Sathyabama Institute of Science and Technology, Chennai is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Electronics And Communications Engineering

1)

2)

DATE:

PLACE:

SIGNATURE OF THE CANDIDATES

ACKNOWLEDGEMENT

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

We convey our thanks to **Dr N.M. NANDHITHA, M.E., Ph.D., Dean, School of Electrical and Electronics** and **Dr T. RAVI, M.E., Ph.D., Head of the Department, Department of Electronics and Communication Engineering** for providing us necessary support and details at the right time during the progressive reviews.

We would like to express our sincere and deep sense of gratitude to our Project Guide **Dr.S.Lalitha Kumari, M.E., Ph.D., Department of Electronics and instrumentation Engineering** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of the project work.

We 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**.**

We express our gratitude to our parents for their constant encouragement and support for the completion of the project.

ABSTRACT

In current world scenario the security of a nation is the uttermost important factor and hence enemy warfare plays an important role. The security of any nation depends on the military, army, air-force and navy of the country and the backbone of all these forces are our soldiers.

Without the soldier it would be nearly impossible to protect a nation. But there are many concerns revolving around the security of these soldiers, especially the army soldiers. Even today when the world is at its prime for technology development, the army is still using rudimentary techniques especially when navigation technology is taken into consideration.

When the soldier enters into the war zone, it is essential for the base station to determine the exact location and the health status of the soldier and hence more emphasis should be given to navigation and health monitoring technology for the soldiers in the war zone.

In the country border the army soldiers are not monitored and they don't know what is happening for the soldier. In this project we are going to monitor the army soldier using some kinds of sensors and transfer the information to the chief kernel using IOT and the information are stored in cloud for future verification. The GPS is used in this project in order to find out the soldier location when any unwanted things happen.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

In current world scenario the security of a nation is the uttermost important factor and hence enemy warfare plays an important role. The security of any nation depends on the military, army, air-force and navy of the country and the backbone of all these forces are our soldiers. Without the soldier it would be nearly impossible to protect a nation. But there are many concerns revolving around the security of these soldiers, especially the army soldiers. Even today when the world is at its prime for technology development, the army is still using rudimentary techniques especially when navigation technology is taken into consideration. When the soldier enters into the war zone, it is essential for the base station to determine the exact location and the health status of the soldier and hence more emphasis should be given to navigation and health monitoring technology for the soldiers in the war zone. In this project the exact location and the health status parameters of the soldier can be sent to the base station in real time so that the appropriate actions can be taken in case of crisis. This technology helps to minimize the rescue, time and search operation effort of army rescue control unit. This system uses GPS module and wireless body area sensor network to record all parameters in real time and send it to the base station. The different types of sensors used in this system are the humidity sensor, temperature sensor and pulse sensor which help in deciding the health status of that particular army official. This is a wearable technology which is the most important factor of this project

The combined unit of Hardware and software constitute an “Embedded System” which is also integrated together to build a system which helps in design goals like speed and efficiency. The main advantage of embedded systems is the flexibility to

choose desired hardware and software components to design the desired system which performs the desired task. This project is based on the above mentioned merits of the embedded system. There is a necessity to develop a wearable technology which isn't bulky and dissipates very little power in the defence sector so that the location and vital health parameters of the soldiers can be tracked in real time when he is on the battlefield. Using this Soldier

Navigation system the base station can guide the soldier to reach the desired destination. The main essence of this project is that it is an Internet of Things (IOT) based project. IOT systems are systems that consist of interrelated machines (mechanical or digital), computing devices, animals, peoples and other objects which have unique functionalities and using the IOT their data can be transferred from one place to another over the network without the computer to computer and human to computer intervention. The relevance of IOT in Soldier Navigation and Health Monitoring system is that the real time location and health parameters of the soldier on the battlefield are instantaneously sent to the base station without the soldier having to input anything. The IOT makes the entire monitoring process fast, efficient

CHAPTER 2

LITERATURE SURVEY AND OBJECTIVES

2.1 LITERATURE SURVEY:

Recent Information from P. Kumar, G. Rasika, V.Patil, and S. Bobade, "Health Monitoring and Tracking of Soldier Using GPS," International Journal of Research in Advent Technology, vol.2, no.4, pp. 291-294, Apr. 2014.

The paper reports an Internet of Thing (IoT) based health monitoring and tracking system for soldiers. The proposed system can be mounted on the soldier's body to track their health status and current location using GPS. These information will be transmitted to the control room through IoT. The proposed system comprise of tiny wearable physiological equipment's, sensors, transmission modules. Hence, with the use of the proposed equipment, it is possible to implement a low cost mechanism to protect the valuable human life on the battlefield

2.2 TRACKING AND LOCKING SYSTEM FOR SHOOTER WITH SENSORY NOISE CANCELLATION

Fabian hoflinger,Zuibzhang and Leaonhard, " Wireless micro inertial measurement," IEEE Conference , June 200**7**

In the present global scenario, the dimensions of warfare has changed to such an extent that the soldiers are exposed to multiple threats, the risk of collateral damage

to soldiers are now even higher. Since the government wants the loss of life to be minimized, this work is to ease the soldiers work nature in urban warfare and close combat especially. The system minimizes the risk of soldier life by tracking and following the intruder movement till the gun is triggered. The system is purely an attachable accessory to a primary assault rifle, that a soldier usually has the system mounted on the top of assault rifle which is fixed on the rail of the gun and the course moment of the gun is synced with the real time response of sensor unit system attached to the helmet of the soldier and map the movement of soldiers head. The sensor unit noise plays an important role on the accuracy of the target locking and firing system. The proposed method has the Kalman filter estimation to remove the noise. The target missing rate has been calculated for various conventional schemes and compared with proposed system. The proposed method performs well on the parameter of success rate on target.

2.3 IMPACT OF POSITION AND ORIENTATION ACCURACY ON TARGETING IN SEE THROUGH HEAD-MOUNTED DISPLAYS FOR SOLDIER INFORMATION SYSTEMS

Q. Ladetto, J. van Seeters, S. Sokolowski, Z. Sagan, and B. Merminod, "Digital Magnetic Compass and Gyroscope for Dismounted Soldier Position & Navigation," Military Capabilities enabled by Advances in Navigation Sensors, Sensors & Electronics Technology Panel, NATO-RTO Meetings, Istanbul, Turkey, 2002.

A first-order statistical model was developed to estimate the impact of position and orientation error (e.g., due to inaccurate GPS/compass information) on the ability to accurately place markers on objects in see through headmounted displays for soldier information systems. In addition, the impact of such errors on the exchange of marker information between soldier nodes was also studied. A closed-form analytical solution was derived and compared to numerical (Monte Carlo) solutions. To compensate for the identified limitations of current systems, dynamically sized target markers and proximity warnings are proposed

2.4 Digital Command and Control System Soldier-Machine Interface for Ground Combat Systems

Brendle, B. E., Cross, M., Forest, C., and Scott, B., "Crewman's Associate: Crew Task Automation Summary Document", Project Documentation, VETRONICS Technology Center, TARDEC, 1994.

A solider-machine interface to a digital Command and Control (C2) system for a ground combat system is described in this paper. This interface is part of a larger effort to develop a crew station optimized for the digitized battlefield. This crew station was developed as part of the Crewman's Associate program. Crewman's Associate is one of the U.S. Army's Advanced Technology Demonstrations (ATD). The paper is organized as follows: Immediately following this introduction, a Background section explains why new combat system crew stations are required. The Command and Control System Description. describes the Force XXI Battle Command to which the crew station must provide a soldier-machine interface. The following section, Crew Station Objectives, lists the operational objectives of the crew station as related to the Command and Control system. The process used to develop the crew station is detailed in the Crew Station Design Process section. The Crew Station Design section provides a top-level overview of the crew station components related to the Command and Control system. The next section, the Digital Command and Control System, provides a description of the soldier-machine interface to this subsystem. The next section summarizes the BeneJits provided by the crew station. How the crew station will be tested is described in the Testing section. Finally, a Conclusion is offered to summarize the paper.

2.5 EXISTING SYSTEM:

- In the existing system they won't monitor the soldier' when they are in border. If they injured by something means, it cannot be identified and cannot give any treatment to the soldier.

- In that case some peoples also die due to loss of treatment.
- In an existing system they send the data through Zigbee
- The transmits the data around 3.1 kms only

2.6 PROPOSED SYSTEM:

- In the proposed project we are going to monitor the soldier using iot.
- The body temperature sensor is used to measure the temperature of the soldier.
- The heart beat sensor is used to measure the heartbeat. When it is go high, it automatically send message to the authenticated person.
- Pressure sensor is used to identify the pressure of the place
- Gas sensor is also used to identify the poisonous gas.
- The gps is used to identify the person when they are injured
- The data is saved in cloud in real time

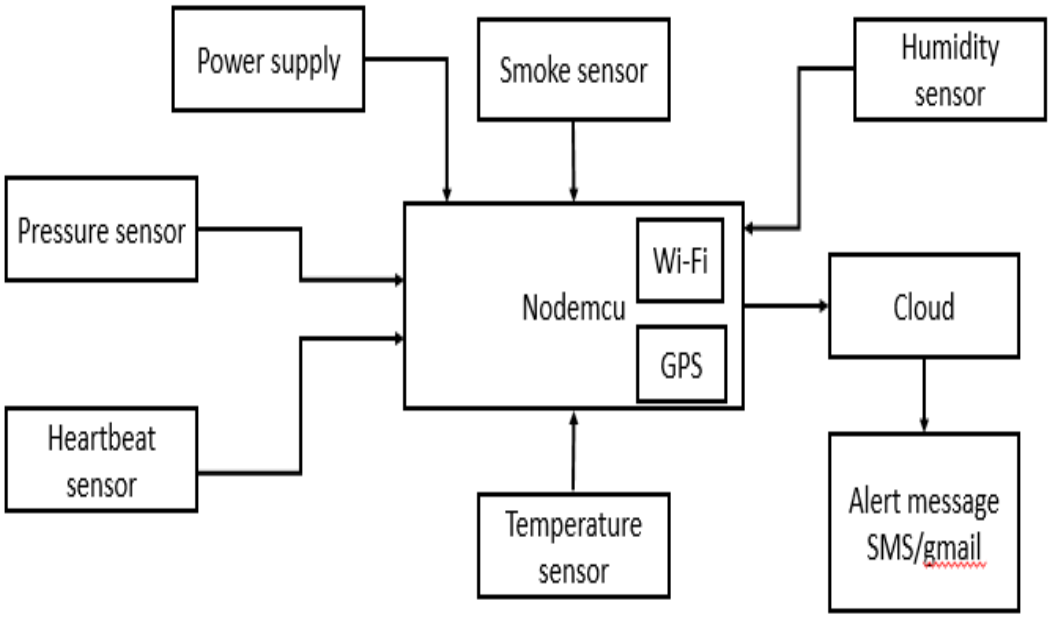

FIG : 2.1 : BLOCK DIAGRAM

2.7 HARDWARE COMPONENTS:

- Heartbeat sensor
- Temperature sensor
- Smoke sensor
- Pressure sensor
- GPS module
- Nodemcu

2.8 SOFTWARE COMPONENTS:

- Arduino c

CHAPTER 3

AIM AND SCOPE OF PRESENT INVESTIGATION

3.1 EMBEDDED SYSTEMS

An embedded system is a special-purpose computer system designed to perform one or a few dedicated functions, often with real-time computing constraints. It is usually embedded as part of a complete device including hardware and mechanical parts. In contrast, a general-purpose computer, such as a personal computer, can do many different tasks depending on programming. Embedded systems have become very important today as they control many of the common devices we use.

Since the embedded system is dedicated to specific tasks, design engineers can optimize it, reducing the size and cost of the product, or increasing the reliability and performance. Some embedded systems are mass-produced, benefiting from economies of scale.

Physically, embedded systems range from portable devices such as digital watches and MP3 players, to large stationary installations like traffic lights, factory controllers, or the systems controlling nuclear power plants Complexity varies from low, with a single microcontroller chip, to very high with multiple units, peripherals and networks mounted inside a large chassis or enclosure.

In general, "embedded system" is not an exactly defined term, as many systems have some element of programmability. For example, Handheld computers share some elements with embedded systems — such as the operating systems and microprocessors which power them — but are not truly embedded systems, because they allow different applications to be loaded and peripherals to be connected.

3.1.1 Embedded systems provide several functions

Monitor the environment; embedded systems read data from input sensors. This data is then processed and the results displayed in some format to a user or users

Control the environment; embedded systems generate and transmit commands for actuators.

Transform the information; embedded systems transform the data collected in some meaningful way, such as data compression/decompression

Although interaction with the external world via sensors and actuators is an important aspect of embedded systems, these systems also provide functionality specific to their applications. Embedded systems typically execute applications such as control laws, finite state machines, and signal processing algorithms. These systems must also detect and react to faults in both the internal computing environment as well as the surrounding electromechanical systems.

There are many categories of embedded systems, from communication devices to home appliances to control systems. Examples include;

Communication devices

e.g.: modems, cellular phones

Home Appliances

e.g.: CD player, VCR, microwave oven

Control Systems

e.g.: Automobile anti-lock braking systems, robotics, and satellite control

An embedded system usually contains an embedded processor. Many appliances that have a digital interface -- microwaves, VCRs, cars -- utilize embedded systems. Some embedded systems include an operating system. Others are very specialized resulting in the entire logic being implemented as a single program. These systems are embedded into some device for some specific purpose other than to provide general purpose computing .

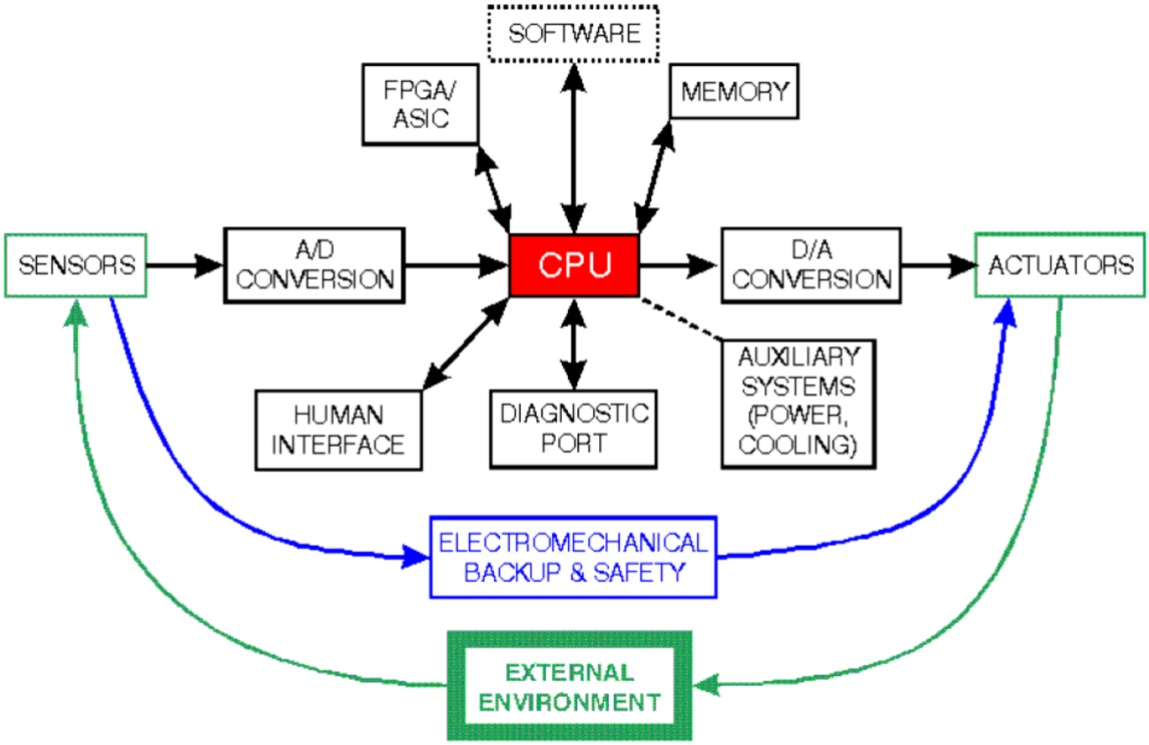

Fig : 3.1 : Block diagram of a typical embedded system

3.1.2 Characteristics of embedded systems

Embedded systems are characterized by a unique set of characteristics. Each of these characteristics imposed a specific set of design constraints on embedded systems designers. The challenge to designing embedded systems is to conform to the specific set of constraints for the application.

3.1.2.1 Application Specific Systems:

Embedded systems are not general-purpose computers. Embedded system designs are optimized for a specific application. Many of the job characteristics are known before the hardware is designed. This allows the designer to focus on the specific design constraints of a well-defined application. As such, there is limited user reprogrammability. Some embedded systems, however, require the flexibility of reprogrammability. Programmable DSPs are common for such applications.

3.1.2.2 Reactive Systems

As mentioned earlier, a typical embedded systems model responds to the environment via sensors and control the environment using actuators. This requires embedded systems to run at the speed of the environment. This characteristic of embedded system is called “reactive”. Reactive computation means that the system (primarily the software component) executes in response to external events. External events can be either periodic or aperiodic. Periodic events make it easier to schedule processing to guarantee performance. Aperiodic events are harder to schedule. The maximum event arrival rate must be estimated in order to accommodate worst case situations. Most embedded systems have a significant reactive component. One of the biggest challenges for embedded system designers is performing an accurate worst case design analysis on systems with statistical performance characteristics (e.g., cache memory on a DSP or

other embedded processor). Real time system operation means that the correctness of a computation depends, in part, on the time at which it is delivered. Systems with this requirement must often design to worst case performance. But accurately predicting the worst case may be difficult on complicated architectures. This often leads to overly pessimistic estimates erring on the side of caution. Many embedded systems have a significant requirement for real time operation in order to meet external I/O and control stability requirements. Many real-time systems are also reactive systems.

3.1.2.3 Distributed Systems

A common characteristic of an embedded system is one that consists of communicating processes executing on several CPUs or ASICs which are connected by communication links. The reason for this is economy. Economical 4 8-bit microcontrollers may be cheaper than a 32-bit processors. Even after adding the cost of the communication links, this approach may be preferable. In this approach, multiple processors are usually required to handle multiple time-critical tasks. Devices under control of embedded systems may also be physically distributed.

3.1.2.4 Heterogeneous Architectures

Embedded systems often are composed of heterogeneous architectures . They may contain different processors in the same system solution. They may also be mixed signal systems. The combination of I/O interfaces, local and remote memories, and sensors and actuators makes embedded system design truly unique. Embedded systems also have tight design constraints, and heterogeneity provides better design flexibility.

3.2 POWER SUPPLY

All electronic circuits works only in low DC voltage, so we need a power supply unit to provide the appropriate voltage supply for their proper functioning .This unit consists of transformer, rectifier, filter & regulator. AC voltage of typically 230volts rms is connected to a transformer voltage down to the level to the desired ac voltage. A diode rectifier that provides the full wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation . A regulator circuit can use this dc input to provide dc voltage that not only has much less ripple voltage but also

remains the same dc value even the dc voltage varies somewhat, or the load connected to the output dc voltages changes.

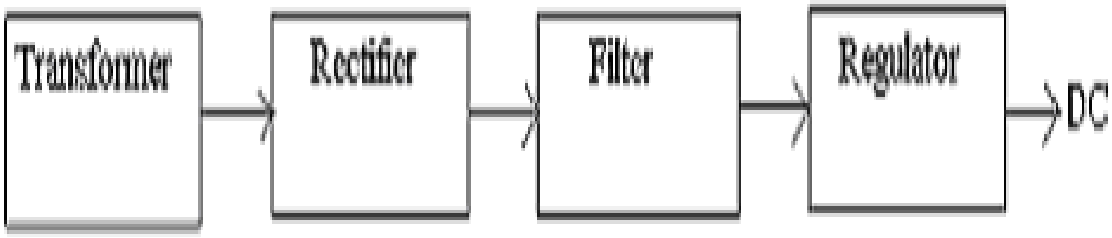

Fig:3.2: General Block of Power Supply Unit

3.3 TRANSFORMER:

A transformer is a static piece of which electric power in one circuit is transformed into electric power of same frequency in another circuit. It can raise or lower the voltage in the circuit, but with a corresponding decrease or increase in current. It works with the principle of mutual induction. In our project we are using a stepdown transformer to providing a necessary supply for the electronic circuits. Here we step down a 230volts ac into 12volts ac.

3.4 RECTIFIER:

A dc level obtained from a sinusoidal input can be improved 100% using a process called full wave rectification. Here in our project for full wave rectification we use bridge rectifier. From the basic bridge configuration we see that two diodes (say D2 & D3) are conducting while the other two diodes (D1 & D4) are in off state during the period t = 0 to T/2.Accordingly for the negative cycle of the input the conducting diodes are D1 & D4 thus the polarity across the load is the same.

In the bridge rectifier the diodes may be of variable types like 1N4001, 1N4003, 1N4004, 1N4005, IN4007 etc… can be used. But here we use 1N4007, because it can withstand up to 1000v.

3.5 FILTERS:

In order to obtain a dc voltage of 0 Hz, we have to use a low pass filter. So that a capacitive filter circuit is used where a capacitor is connected at the rectifier output& a dc is obtained across it. The filtered waveform is essentially a dc voltage with negligible ripples & it is ultimately fed to the load.

3.6 REGULATORS:

The output voltage from the capacitor is more filtered & finally regulated. The voltage regulator is a device, which maintains the output voltage constant irrespective of the change in supply variations, load variations & temperature changes. Here we use fixed voltage regulator namely LM7805.The IC LM7805 is a +5v regulator which is used for microcontroller.

3.7 FEATURES AND DESCRIPTION OF REGULATORS

- Output Current up to 1A
- Output Voltages of 5, 6, 8, 9, 10, 12, 15, 18, 24V
- Thermal Overload Protection
- Short Circuit Protection
- Output Transistor Safe Operating Area Protection

3.8 ARDUINO NODE MCU

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

NodeMCU was created shortly after the ESP8266 came out. On December 30, 2013, Espressif Systems began production of the ESP8266. The ESP8266 is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IOT applications. Node MCU started on 13 Oct 2014, when Hong committed the first file of node MCU firmware to GitHub. Two months later, the project expanded to include an open-

hardware platform when developer Huang R committed the gerber file of an ESP8266 board, named devkit v0.9. Later that month, Tuan PM ported MQTT client library from Contiki to the ESP8266 SoC platform, and committed to Node MCU project, then Node MCU was able to support the MQTT IoT protocol, using Lua to access the MQTT broker. Another important update was made on 30 Jan 2015, when Devsaurus ported the u8glib to Node MCU project, enabling Node MCU to easily drive LCD, Screen, OLED, even VGA displays.

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

3.8.1 ESP8266 Arduino Core

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

3.9 PULSE SENSOR

FIG : 3.3 : PULSE SENSOR

Pulse oximetry is a noninvasive method for monitoring a person's oxygen saturation (SO_2). Though its reading of SpO_2 (peripheral oxygen saturation) is not always identical to the more desirable reading of SaO_2 (arterial oxygen saturation) from arterial blood gas analysis, the two are correlated well enough that the safe, convenient, non-invasive, inexpensive pulse oximetry method is valuable for measuring oxygen saturation in clinical use.

In its most common (transmissive) application mode, a sensor device is placed on a thin part of the patient's body, usually a fingertip or earlobe, or in the case of an infant, across a foot. The device passes two wavelengths of light through the body part to a photodetector. It measures the changing absorbance at each of the wavelengths, allowing it to determine the absorbances due to the pulsing arterial blood alone, excluding venous blood, skin, bone, muscle, fat, and (in most cases) nail polish.

Less commonly, reflectance pulse oximetry is used as an alternative to transmissive pulse oximeter described above. This method does not require a thin section of the person's body and is therefore well suited to a universal application such as the feet, forehead, and chest, but it also has some limitations. Vasodilation and pooling of venous blood in the head due to compromised venous return to the heart can cause a combination of arterial and venous pulsations in the forehead region and lead to spurious SpO_2 results. Such conditions occur while undergoing anesthesia with endotracheal intubation and mechanical ventilation or in patients in the Trendelenburg position.

In 1935, Karl Matthes (German physician 1905–1962) developed the first 2-wavelength ear O_2 saturation meter with red and green filters (later switched to red and infrared filters). His meter was the first device to measure O_2 saturation.

The original oximeter was made by Glenn Allan Millikan in the 1940s. In 1949 Wood added a pressure capsule to squeeze blood out of the ear so as to obtain an absolute O_2 saturation value when blood was readmitted. The concept is similar to today's conventional pulse oximetry, but was difficult to implement because of unstable photocells and light sources; the method is not now used clinically. In 1964 Shaw assembled the first absolute reading ear oximeter by using eight wavelengths of light.

Pulse oximetry was developed in 1972, by Takuo Aoyagi and Michio Kishi, bioengineers, at Nihon Kohden using the ratio of red to infrared light absorption of pulsating components at the measuring site. Susumu Nakajima, a surgeon, and his associates first tested the device in patients, reporting it in 1975. It was commercialized by Biox in 1980.

By 1987, the standard of care for the administration of a general anesthetic in the U.S. included pulse oximetry. From the operating room, the use of pulse oximetry rapidly spread throughout the hospital, first to the recovery room, and then into the various intensive care units. Pulse oximetry was of particular value in the neonatal unit where the patients do not thrive with inadequate oxygenation, but too much oxygen and fluctuations in oxygen concentration can lead to vision impairment or blindness from retinopathy of prematurity (ROP). Furthermore, obtaining an arterial blood gas from a neonatal patient is painful to the patient and a major cause of neonatal anemia.Motion artifact can be a significant limitation to pulse oximetry monitoring resulting in frequent false alarms and loss of data. The reason for this is that during motion and low peripheral perfusion, many pulse oximeters cannot distinguish between pulsating arterial blood and moving venous blood, leading to underestimation of oxygen saturation. Early studies of pulse oximetry performance during subject motion made clear the vulnerabilities of conventional pulse oximetry technologies to motion artifact.

In 1995, Masimo introduced Signal Extraction Technology (SET) that could measure accurately during patient motion and low perfusion by separating the arterial signal from the venous and other signals. Since then, pulse oximetry manufacturers have developed new algorithms to reduce some false alarms during motion such as extending averaging times or freezing values on the screen, but they do not claim to measure changing conditions during motion and low perfusion. So, there are still important differences in performance of pulse oximeters during challenging conditions.

Published papers have compared signal extraction technology to other pulse oximetry technologies and have demonstrated consistently favorable results for signal extraction technology.Signal extraction technology pulse oximetry performance has also been shown to translate into helping clinicians improve patient outcomes. In one study, retinopathy of prematurity (eye damage) was reduced by 58% in very low birth weight neonates at a center using signal extraction technology, while there was no decrease in retinopathy of prematurity at another center with the same clinicians using the same protocol but with non-signal extraction technology. Other studies have shown that signal extraction technology pulse oximetry results in fewer arterial blood gas measurements, faster oxygen weaning time, lower sensor utilization, and lower length of stay. The measure-through motion and low perfusion capabilities it has also allow it to be used in previously unmonitored areas such as the general floor, where false alarms have plagued conventional pulse oximetry. As evidence of this, a landmark study was published in 2010 showing clinicians using signal extraction technology pulse oximetry on the general floor were able to decrease rapid response team activations, ICU transfers, and ICU days.

In 2011, an expert workgroup recommended newborn screening with pulse oximetry to increase the detection of critical congenital heart disease (CCHD). The CCHD workgroup cited the results of two large, prospective studies of 59,876 subjects that exclusively used signal extraction technology to increase the identification of CCHD with minimal false positives. The CCHD workgroup recommended newborn screening be performed with motion tolerant pulse oximetry that has also been validated in low perfusion conditions. In 2011, the US Secretary of Health and Human Services added pulse oximetry to the recommended uniform screening panel. Before the evidence for screening using signal extraction technology, less than 1% of

newborns in the United States were screened. Today, The Newborn Foundation has documented near universal screening in the United States and international screening is rapidly expanding. In 2014, a third large study of 122, 738 newborns that also exclusively used signal extraction technology showed similar, positive results as the first two large studies.

High-resolution pulse oximetry (HRPO) has been developed for in-home sleep apnea screening and testing in patients for whom it is impractical to perform polysomnography. It stores and records both pulse rate and SpO2 in 1 second intervals and has been shown in one study to help to detect sleep disordered breathing in surgical patients.

In 1995 Masimo introduced perfusion index, quantifying the amplitude of the peripheral plethysmograph waveform. Perfusion index has been shown to help clinicians predict illness severity and early adverse respiratory outcomes in neonates, predict low superior vena cava flow in very low birth weight infants,provide an early indicator of sympathectomy after epidural anesthesia, and improve detection of critical congenital heart disease in newborns.

In 2007, Masimo introduced the first measurement of the pleth variability index (PVI), which multiple clinical studies have shown provides a new method for automatic, noninvasive assessment of a patient's ability to respond to fluid administration. Appropriate fluid levels are vital to reducing postoperative risks and improving patient outcomes: fluid volumes that are too low (under-hydration) or too high (over-hydration) have been shown to decrease wound healing and increase the risk of infection or cardiac complications.Recently, the National Health Service in the United Kingdom and the French Anesthesia and Critical Care Society listed PVI monitoring as part of their suggested strategies for intra-operative fluid management

A blood-oxygen monitor displays the percentage of blood that is loaded with oxygen. More specifically, it measures what percentage of hemoglobin, the protein in blood that carries oxygen, is loaded. Acceptable normal ranges for patients without pulmonary pathology are from 95 to 99 percent. For a patient breathing room air at or near sea level, an estimate of arterial pO_2 can be made from the blood-oxygen monitor "saturation of peripheral oxygen" (SpO_2) reading.

A typical pulse oximeter uses an electronic processor and a pair of small light-emitting diodes (LEDs) facing a photodiode through a translucent part of the patient's body, usually a fingertip or an earlobe. One LED is red, with wavelength of 660 nm, and the other is infrared with a wavelength of 940 nm. Absorption of light at these wavelengths differs significantly between blood loaded with oxygen and blood lacking oxygen. Oxygenated hemoglobin absorbs more infrared light and allows more red light to pass through. Deoxygenated hemoglobin allows more infrared light to pass through and absorbs more red light. The LEDs sequence through their cycle of one on, then the other, then both off about thirty times per second which allows the photodiode to respond to the red and infrared light separately and also adjust for the ambient light baseline. The amount of light that is transmitted (in other words, that is not absorbed) is measured, and separate normalized signals are produced for each wavelength. These signals fluctuate in time because the amount of arterial blood that is present increases (literally pulses) with each heartbeat. By subtracting the minimum transmitted light from the peak transmitted light in each wavelength, the effects of other tissues are corrected for the ratio of the red light measurement to the infrared light measurement is then calculated by the processor (which represents the ratio of oxygenated hemoglobin to deoxygenated hemoglobin), and this ratio is then converted to SpO_2 by the processor via a lookup table based on the Beer–Lambert law.

A pulse oximeter is a medical device that indirectly monitors the oxygen saturation of a patient's blood (as opposed to measuring oxygen saturation directly through a blood sample) and changes in blood volume in the skin, producing a photoplethysmogram. The pulse oximeter may be incorporated into a multiparameter patient monitor. Most monitors also display the pulse rate. Portable, battery-operated pulse oximeters are also available for transport or home blood-oxygen monitoring

Pulse oximetry is particularly convenient for non-invasive continuous measurement of blood oxygen saturation. In contrast, blood gas levels must otherwise be determined in a laboratory on a drawn blood sample. Pulse oximetry is useful in any setting where a patient's oxygenation is unstable, including intensive care, operating, recovery, emergency and hospital ward settings, pilots in unpressurized aircraft, for assessment of any patient's oxygenation, and determining the effectiveness of or need for supplemental oxygen. Although a pulse oximeter is used

to monitor oxygenation, it cannot determine the metabolism of oxygen, or the amount of oxygen being used by a patient. For this purpose, it is necessary to also measure carbon dioxide (CO_2) levels. It is possible that it can also be used to detect abnormalities in ventilation. However, the use of a pulse oximeter to detect hypoventilation is impaired with the use of supplemental oxygen, as it is only when patients breathe room air that abnormalities in respiratory function can be detected reliably with its use. Therefore, the routine administration of supplemental oxygen may be unwarranted if the patient is able to maintain adequate oxygenation in room air, since it can result in hypoventilation going undetected.

Because of their simplicity of use and the ability to provide continuous and immediate oxygen saturation values, pulse oximeters are of critical importance in emergency medicine and are also very useful for patients with respiratory or cardiac problems, especially COPD, or for diagnosis of some sleep disorders such as apnea and hypopnea. Portable battery-operated pulse oximeters are useful for pilots operating in a non-pressurized aircraft above 10,000 feet (3,000 m) or 12,500 feet (3,800 m) in the U.S.where supplemental oxygen is required. Portable pulse oximeters are also useful for mountain climbers and athletes whose oxygen levels may decrease at high altitudes or with exercise. Some portable pulse oximeters employ software that charts a patient's blood oxygen and pulse, serving as a reminder to check blood oxygen levels.

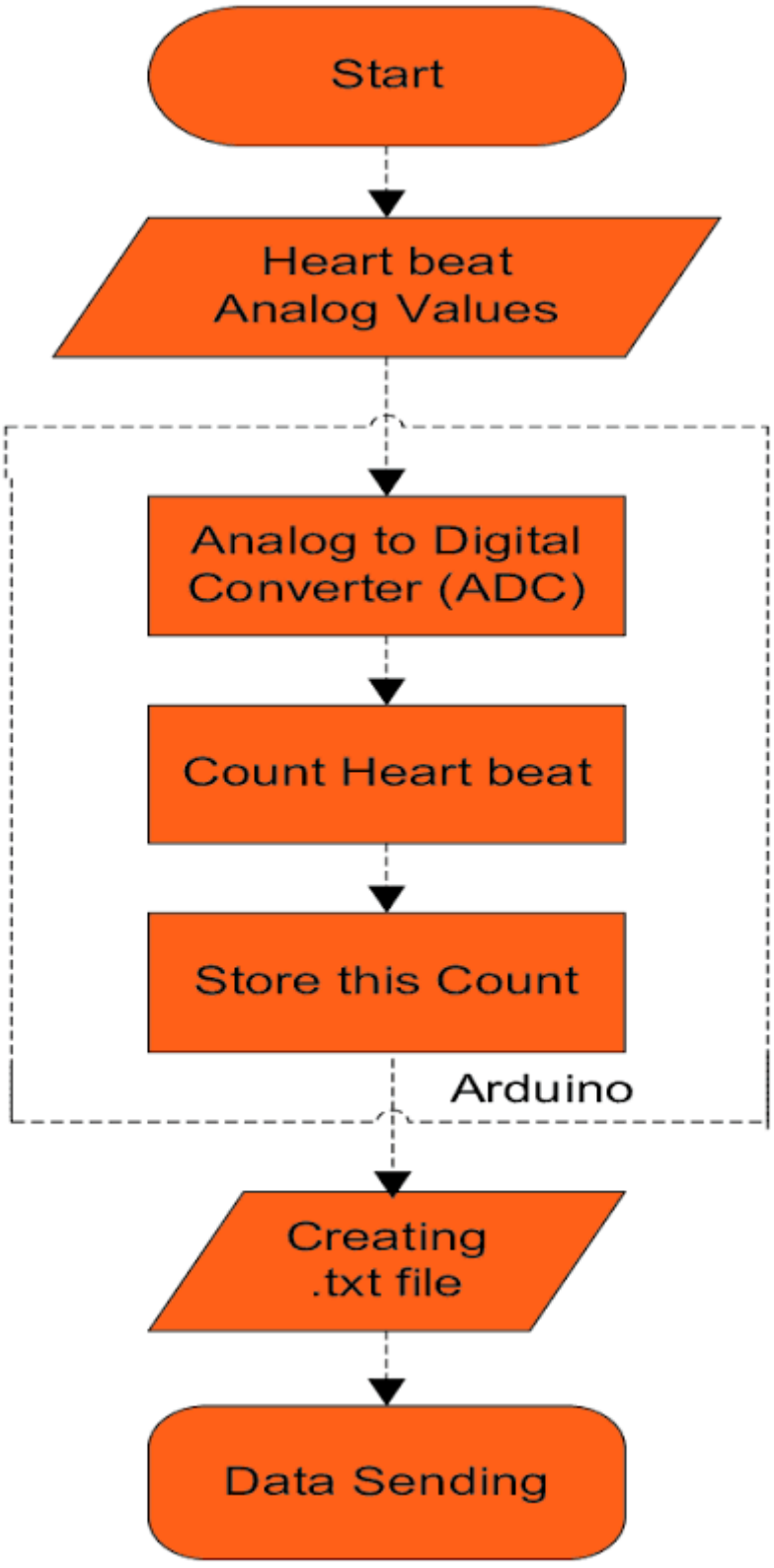

FIG : 3.4 : FLOW CHART OF PULSE SENSOR

3.1O GAS SENSOR:

FIG : 3.5 : GAS SENSOR

A gas detector is a device that detects the presence of gases in an area, often as part of a safety system. This type of equipment is used to detect a gas leak or other emissions and can interface with a control system so a process can be automatically shut down. A gas detector can sound an alarm to operators in the area where the leak is occurring, giving them the opportunity to leave. This type of device is important because there are many gases that can be harmful to organic life, such as humans or animals.

Gas detectors can be used to detect combustible, flammable and toxic gases, and oxygen depletion. This type of device is used widely in industry and can be found in locations, such as on oil rigs, to monitor manufacture processes and emerging technologies such as photovoltaic. They may be used in firefighting.

Gas leak detection is the process of identifying potentially hazardous gas leaks by sensors. These sensors usually employ an audible alarm to alert people when a dangerous gas has been detected. Exposure to toxic gases can also occur in operations such as painting, fumigation, fuel filling, construction, excavation of contaminated soils, landfill operations, entering confined spaces, etc. Common sensors include combustible gas sensors, photoionization detectors, infrared point sensors, ultrasonic sensors, electrochemical gas sensors, and semiconductor sensors. More recently, infrared imaging sensors have come into use. All of these sensors are used for a wide range of applications and can be found in industrial plants, refineries, pharmaceutical manufacturing, fumigation facilities, paper pulp mills,

aircraft and shipbuilding facilities, hazmat operations, waste-water treatment facilities, vehicles, indoor air quality testing and homes.

Gas leak detection methods became a concern after the effects of harmful gases on human health were discovered. Before modern electronic sensors, early detection methods relied on less precise detectors. Through the 19th and early 20th centuries, coal miners would bring canaries down to the tunnels with them as an early detection system against life-threatening gases such as carbon dioxide, carbon monoxide and methane. The canary, normally a very songful bird, would stop singing and eventually die if not removed from these gases, signaling the miners to exit the mine quickly.

The first gas detector in the industrial age was the *flame safety lamp* (or Davy lamp) was invented by Sir Humphry Davy (of England) in 1815 to detect the presence of methane (firedamp) in underground coal mines. The flame safety lamp consisted of an oil flame adjusted to specific height in fresh air. To prevent ignition with the lamps flame was contained within a glass sleeve with a mesh flame arrestor. The flames height varied depending on the presence of methane (higher) or the lack of oxygen (lower). To this day, in certain parts of the world flame safety lamps are still in service.

The modern era of gas detection started in 1926-1927 with the development of the catalytic combustion (LEL) sensor by Dr.Oliver Johnson. Dr Johnson was an employee of Standard Oil Company in California (now Chevron), he begun research and development on a method to detect combustible mixtures in air to help prevent explosions in fuel storage tanks. A demonstration model was developed in 1926 and denoted as the Model A. The first practical "electric vapor indicator" meter begun production in 1927 with the release of the Model B.

The worlds first gas detection company, Johnson-Williams Instruments (or J-W Instruments) was formed in 1928 in Palo Alto, CA by Dr Oliver Johnston and Phil Williams. J-W Instruments is recognized as the first electronics company in Silicon Valley. Over the next 40 years J-W Instruments pioneered many "firsts" in the modern age of gas detection, including making instruments smaller and more portable, development of a portable oxygen detector as well as the first combination instrument that could detect both combustible gases/vapors as well as oxygen.

Before the development of electronic household carbon monoxide detectors in the 1980s and 1990s, carbon monoxide presence was detected with a chemically infused paper that turned brown when exposed to the gas. Since then, many electronic technologies and devices have been developed to detect, monitor, and alert the leak of a wide array of gases.

As the cost and performance of electronic gas sensors improved, they have been incorporated into a wider range of systems. Their use in automobiles was initially for engine emissions control, but now gas sensors may also be used to ensure passenger comfort and safety. Carbon dioxide sensors are being installed into buildings as part of demand-controlled ventilation systems. Sophisticated gas sensor systems are being researched for use in medical diagnostic, monitoring, and treatment systems, well beyond their initial use in operating rooms. Gas monitors and alarms for carbon monoxide and other harmful gases are increasingly available for office and domestic use, and are becoming legally required in some jurisdictions.

Originally, detectors were produced to detect a single gas. Modern units may detect several toxic or combustible gases, or even a combination. Newer gas analyzers can break up the component signals from a complex aroma to identify several gases simultaneously.

Gas detectors can be classified according to the operation mechanism (semiconductors, oxidation, catalytic, photoionization, infrared, etc.). Gas detectors come packaged into two main form factors: portable devices and fixed gas detectors.

Portable detectors are used to monitor the atmosphere around personnel and are either hand-held or worn on clothing or on a belt/harness. These gas detectors are usually battery operated. They transmit warnings via audible and visible signals, such as alarms and flashing lights, when dangerous levels of gas vapors are detected.

Fixed type gas detectors may be used for detection of one or more gas types. Fixed type detectors are generally mounted near the process area of a plant or control room, or an area to be protected, such as a residential bedroom. Generally, industrial sensors are installed on fixed type mild steel structures and a cable connects the

detectors to a SCADA system for continuous monitoring. A tripping interlock can be activated for an emergency situation.

Electrochemical gas detectors work by allowing gases to diffuse through a porous membrane to an electrode where it is either chemically oxidized or reduced. The amount of current produced is determined by how much of the gas is oxidized at the electrode,indicating the concentration of the gas. Manufactures can customize electrochemical gas detectors by changing the porous barrier to allow for the detection of a certain gas concentration range. Also, since the diffusion barrier is a physical/mechanical barrier, the detector tended to be more stable and reliable over the sensor's duration and thus required less maintenance than other early detector technologies.

However, the sensors are subject to corrosive elements or chemical contamination and may last only 1–2 years before a replacement is required. Electrochemical gas detectors are used in a wide variety of environments such as refineries, gas turbines, chemical plants, underground gas storage facilities, and more.

Catalytic bead sensors are commonly used to measure combustible gases that present an explosion hazard when concentrations are between the lower explosion limit (LEL) and upper explosion limit (UEL). Active and reference beads containing platinum wire coils are situated on opposite arms of a Wheatstone bridge circuit and electrically heated, up to a few hundred degrees C. The active bead contains a catalyst that allows combustible compounds to oxidize, thereby heating the bead even further and changing its electrical resistance. The resulting voltage difference between the active and passive beads is proportional to the concentration of all combustible gases and vapors present. The sampled gas enters the sensor through a sintered metal frit, which provides a barrier to prevent an explosion when the instrument is carried into an atmosphere containing combustible gases. Pellistors measure essentially all combustible gases, but they are more sensitive to smaller molecules that diffuse through the sinter more quickly. The measureable concentration ranges are typically from a few hundred ppm to a few volume percent. Such sensors are inexpensive and robust, but require a minimum of a few percent oxygen in the atmosphere to be tested

and they can be poisoned or inhibited by compounds such as silicones, mineral acids, chlorinated organic compounds, and sulfur compounds.

Photoionization detectors (PIDs) use a high-photon-energy UV lamp to ionize chemicals in the sampled gas. If the compound has an ionization energy below that of the lamp photons, an electron will be ejected, and the resulting current is proportional to the concentration of the compound. Common lamp photon energies include 10.0 eV, 10.6 eV and 11.7 eV; the standard 10.6 eV lamp lasts for years, while the 11.7 eV lamp typically last only a few months and is used only when no other option is available. A broad range of compounds can be detected at levels ranging from a few ppb to several thousand ppm. Detectable compound classes in order of decreasing sensitivity include: aromatics and alkyl iodides; olefins, sulfur compounds, amines, ketones, ethers, alkyl bromides and silicate esters; organic esters, alcohols, aldehydes and alkanes; H2S, NH3, PH3 and organic acids. There is no response to standard components of air or to mineral acids. Major advantages of PIDs are their excellent sensitivity and simplicity of use; the main limitation is that measurements are not compound-specific. Recently PIDs with pre-filter tubes have been introduced that enhance the specificity for such compounds as benzene or butadiene. Fixed, hand-held and miniature clothing-clipped PIDs are widely used for industrial hygiene, hazmat, and environmental monitoring.

Infrared (IR) point sensors use radiation passing through a known volume of gas; energy from the sensor beam is absorbed at certain wavelengths, depending on the properties of the specific gas. For example, carbon monoxide absorbs wavelengths of about 4.2-4.5 μm.The energy in this wavelength is compared to a wavelength outside of the absorption range; the difference in energy between these two wavelengths is proportional to the concentration of gas present.

This type of sensor is advantageous because it does not have to be placed into the gas to detect it and can be used for remote sensing. Infrared point sensors can be used to detect hydrocarbons and other infrared active gases such as water vapor and carbon dioxide. IR sensors are commonly found in waste-water treatment facilities, refineries, gas turbines, chemical plants, and other facilities where flammable gases are present and the possibility of an explosion exists. The remote sensing capability allows large volumes of space to be monitored.

Engine emissions are another area where IR sensors are being researched. The sensor would detect high levels of carbon monoxide or other abnormal gases in vehicle exhaust and even be integrated with vehicle electronic systems to notify drivers.

Infrared image sensors include active and passive systems. For active sensing, IR imaging sensors typically scan a laser across the field of view of a scene and look for backscattered light at the absorption line wavelength of a specific target gas. Passive IR imaging sensors measure spectral changes at each pixel in an image and look for specific spectral signatures that indicate the presence of target gases.The types of compounds that can be imaged are the same as those that can be detected with infrared point detectors, but the images may be helpful in identifying the source of a gas.

Semiconductor sensors detect gases by a chemical reaction that takes place when the gas comes in direct contact with the sensor. Tin dioxide is the most common material used in semiconductor sensors,and the electrical resistance in the sensor is decreased when it comes in contact with the monitored gas. The resistance of the tin dioxide is typically around 50 kΩ in air but can drop to around 3.5 kΩ in the presence of 1% methane. This change in resistance is used to calculate the gas concentration. Semiconductor sensors are commonly used to detect hydrogen, oxygen, alcohol vapor, and harmful gases such as carbon monoxide. One of the most common uses for semiconductor sensors is in carbon monoxide sensors. They are also used in breathalyzers. Because the sensor must come in contact with the gas to detect it, semiconductor sensors work over a smaller distance than infrared point or ultrasonic detectors.

Ultrasonic gas leak detectors are not gas detectors per se. They detect the acoustic emission created when a pressured gas expands in a low pressure area through a small orifice (the leak). They use acoustic sensors to detect changes in the background noise of its environment. Since most high-pressure gas leaks generate sound in the ultrasonic range of 25 kHz to 10 MHz, the sensors are able to easily distinguish these frequencies from background acoustic noise which occurs in the audible range of 20 Hz to 20 kHz.The ultrasonic gas leak detector then produces an alarm when there is an ultrasonic deviation from the normal condition of background

noise. Ultrasonic gas leak detectors cannot measure gas concentration, but the device is able to determine the leak rate of an escaping gas because the ultrasonic sound level depends on the gas pressure and size of the leak.

Ultrasonic gas detectors are mainly used for remote sensing in outdoor environments where weather conditions can easily dissipate escaping gas before allowing it to reach leak detectors that require contact with the gas to detect it and sound an alarm. These detectors are commonly found on offshore and onshore oil/gas platforms, gas compressor and metering stations, gas turbine power plants, and other facilities that house a lot of outdoor pipeline.

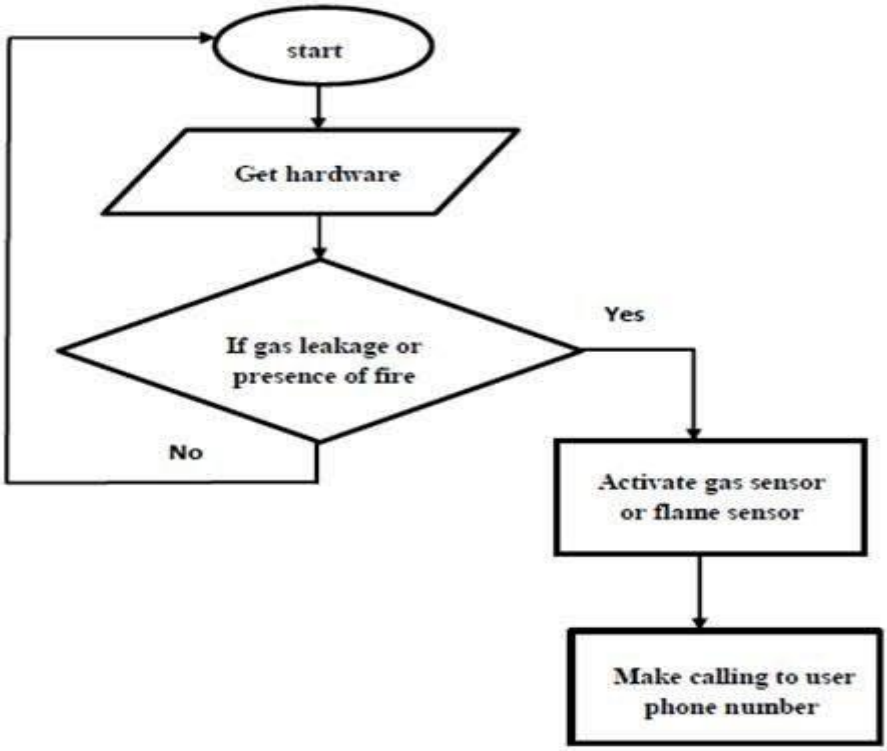

FIG : 3.6 : FLOW CHART OF GAS SENSER

3.11 TEMPERATURE SENSOR:

FIG : 3.7 : TEMPERATURE SENSER

The LM35 series are precision integrated-circuit temperature devices with an output voltage linearly-proportional to the Centigrade temperature. The LM35 device has an advantage over linear temperature sensors calibrated in Kelvin, as the user is not required to subtract a large constant voltage from the output to obtain convenient Centigrade scaling. The LM35 device does not require any external calibration or trimming to provide typical accuracies of ±¼°C at room temperature and ±¾°C over a full −55°C to 150°C temperature range. Lower cost is assured by trimming and calibration at the wafer level. The low-output impedance, linear output, and precise inherent calibration of the LM35 device makes interfacing to readout or control circuitry especially easy. The device is used with single power supplies, or with plus and minus supplies. As the LM35 device draws only 60 µA from the supply, it has very low self-heating of less than 0.1°C in still air. The LM35 device is rated to operate over a −55°C to 150°C temperature range, while the LM35C device is rated for a −40°C to 110°C range (−10° with improved accuracy). The LM35-series devices are available packaged in hermetic TO transistor packages, while the LM35C, LM35CA, and LM35D devices are available in the plastic TO-92 transistor package. The LM35D device is available in an 8-lead surface-mount small-outline package and a plastic TO-220 package.

3.11 .1 FEATURE:

- Calibrated Directly in Celsius (Centigrade)
- Linear + 10-mV/°C Scale Factor
- 0.5°C Ensured Accuracy (at 25°C)
- Rated for Full −55°C to 150°C Range
- Suitable for Remote Applications
- Low-Cost Due to Wafer-Level Trimming

- Operates From 4 V to 30 V
- Less Than 60-µA Current Drain
- Low Self-Heating, 0.08°C in Still Air
- Non-Linearity Only ±¼°C Typical
- Low-Impedance Output, 0.1 Ω for 1-mA Load

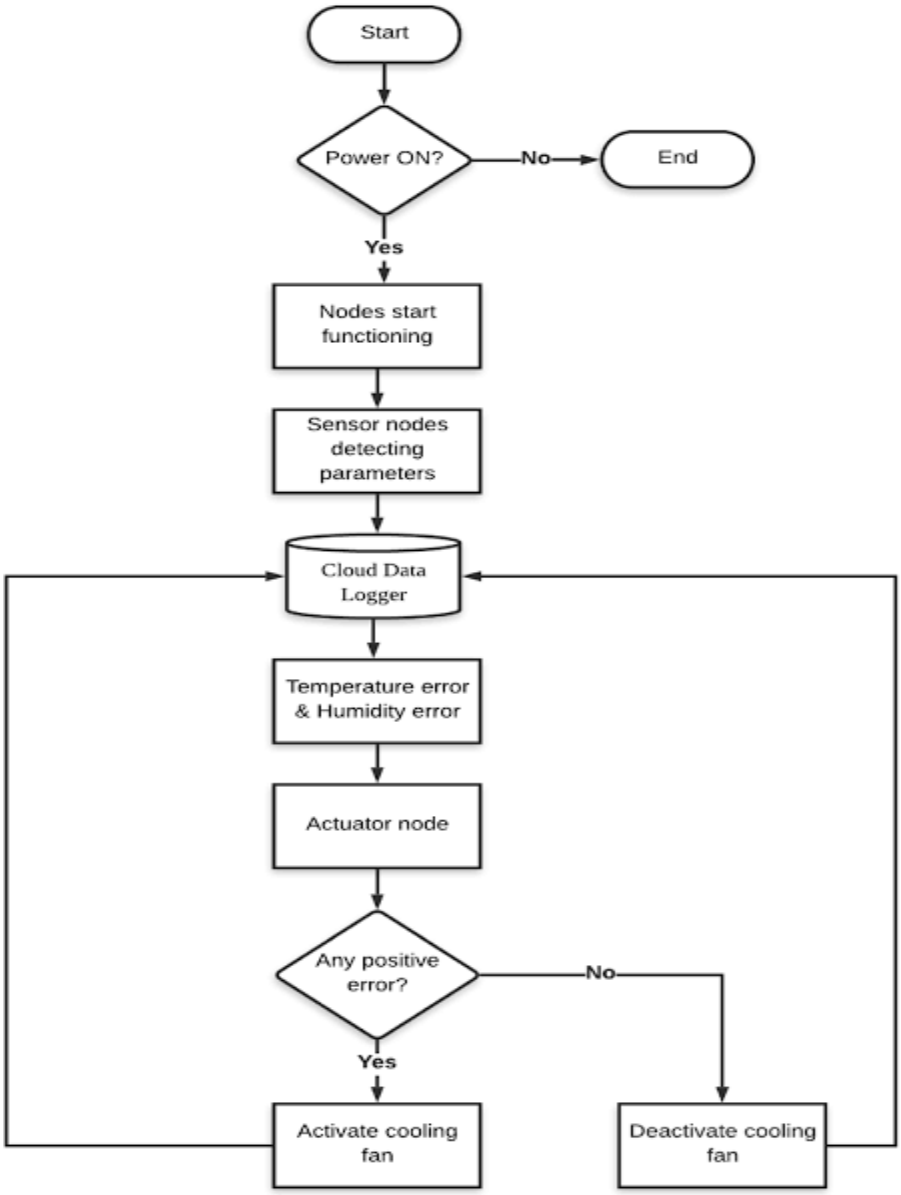

FIG : 3.8 :FLOW CHART OF TEMPERATURE SENSOR

3.12 PRESSURE SENSOR:

FIG : 3.9 : PRESSURE SENSOR

This pressure sensor is a BMP-180 based digital barometric pressure sensor module and is functional compatible with older BMP-085 digital pressure sensor with less power consumption smaller in size and more accurate. BMP180 combines barometric pressure, temperature and altitude. The I2C allows easy interface with any microcontroller. On board 3.3V LDO regulator makes this board fully 5V supply compatible. BMP-180 can measure pressure range from 300 to 1100hPa (+9000m to -500m relating to sea level) with an accuracy down to 0.02hPa (0.17m) in advance resolution mode. BMP-180 is an improved replacement for BMP-085 sensor. BMP-180 uses piezo-resistive technology for high accuracy, linearity, EMC robustness and stability for a longer period of time

- Supply Voltage:**1.8V to 3.6V**
- Low power consumption:**0.5uA at 1Hz**
- **I2C** interface
- Max I2C Speed: **3.5Mhz**
- Very low noise:**up to 0.02hPa (17cm)**
- Pressure Range: **300hPa to 1100hPa (+9000m to -500m)**

The BMP180 consists of a piezo-resistive sensor, an analog to digital converter and a control unit with E2PROM and a serial I2C interface. The BMP180 delivers the uncompensated value of pressure and temperature.The microcontroller sends a start sequence to start a pressure or temperature measurement. After converting time, the result value (pressure or temperature respectively) can be read via the I2C interface. For calculating temperature in °C and pressure in hPa, the calibration data has to be

used. These constants can be read out from the BMP180 E2PROM via the I2C interface at software initialization.The sampling rate can be increased up to 128 samples per second (standard mode) for dynamic measurement. In this case, it is sufficient to measure the temperature only once per second and to use this value for all pressure measurements during the same period.

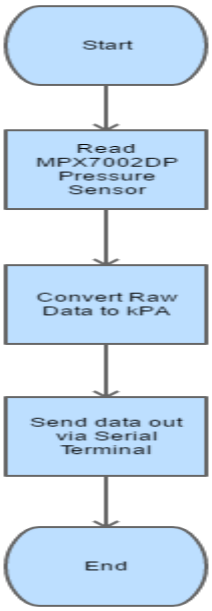

FIG : 3.10 : FLOW SHART OF PRESSURE SENSOR

3.13 INTERNET OF THINGS:

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

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

3.13.1 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. 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.

CHAPTER 4

EXPERIMENTAL OR MATERIALS AND METHODS;ALGORITHMS

4.1 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.

4.2 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.

4.3 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.

4.4 Manufacturing Network

Control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well. The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together. Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT. But it also extends itself to asset management via predictive maintenance, statistical evaluation, and

measurements to maximize reliability. Smart industrial management systems can also be integrated with the Smart Grid, thereby enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors. The National Science Foundation established an Industry/University Cooperative Research Center on intelligent maintenance systems (IMS) in 2001 with a research focus to use IoT-based predictive analytics technologies to monitor connected machines and to predict machine degradation, and further to prevent potential failures. The vision to achieve near-zero breakdown using IoT-based predictive analytics led the future development of e-manufacturing and maintenance activities. The term IIoT (Industrial Internet of Things) is often encountered in the manufacturing industries, referring to the industrial subset of the IoT. IIoT in manufacturing could generate so much business value that it will eventually lead to the fourth industrial revolution, so the so-called Industry 4.0. It is estimated that in the future, successful companies will be able to increase their revenue through Internet of things by creating new business models and improve productivity, exploit analytics for innovation, and transform workforce. The potential of growth by implementing IIoT will generate $12 trillion of global GDP by 2030 while connectivity and data acquisition are imperative for IIoT, they should not be the purpose, rather the foundation and path to something bigger. Among all the technologies, predictive maintenance is probably a relatively "easier win" since it is applicable to existing assets and management systems. The objective of intelligent maintenance systems is to reduce unexpected downtime and increase productivity. And to realize that alone would generate around up to 30% over total maintenance costs. Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. Cyber-physical systems can be designed by following the 5C (connection, conversion, cyber, cognition, configuration) architecture, and it will transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes. An IoT-enabled intelligent system of such cases has been demonstrated by the NSF Industry/University Collaborative Research Center for Intelligent Maintenance Systems (IMS) at University of Cincinnati on a band saw machine in IMTS 2014 in Chicago. Band saw machines are not necessarily

expensive, but the band saw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics, it can be only determined by experience when the band saw belt will actually break. The developed prognostics system will be able to recognize and monitor the degradation of band saw belts even if the condition is changing, so that users will know in near real time when is the best time to replace band saw. This will significantly improve user experience and operator safety, and save costs on replacing band saw belts before they actually break. The developed analytical algorithms were realized on a cloud server, and was made accessible via the Internet and on mobile devices.

4.5 Energy Management

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

4.6 Medical And Healthcare

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure

and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. Other consumer devices to encourage healthy living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT. More and more end-to-end health monitoring IoT platforms are coming up for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

4.7 Building and Home Automation

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

4.8 Transportation

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

4.8.1 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, Song do, 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, digital city agenda among others. City context information is used in this deployment so as to benefit merchants through a spark deals mechanism based on city behavior that aims at maximizing the impact of each notification. Other examples of large-scale deployments underway include the Sino-Singapore Guangzhou Knowledge City; work on improving air and water quality, reducing noise pollution, and increasing transportation efficiency in San Jose, California; and smart traffic management in western Singapore. French company, Sigfox, commenced building an ultra-narrowband wireless data network in the San Francisco Bay Area in 2014, the first business to achieve such a deployment in the U.S. It subsequently announced it would set up a total of 4000 base stations to cover a total of 30 cities in the U.S. by the end of 2016, making it the largest IoT network coverage provider in the country thus far. Another example of a large deployment is the one completed by New York Waterways in New York City to connect all the city's vessels and be able to monitor them live 24/7. The network was designed and engineered by Fluid mesh 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.

4.8.2 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.

4.9 Unique Addressability Of Things

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

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

4.10 Trends And Characteristics

4.10.1 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 behavior through the collection and reasoning of context information as well as the objects ability to detect changes in the environment, faults affecting sensors and introduce suitable mitigation measures constitute a major research trend, clearly needed to provide credibility to the IoT technology. Modern IoT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation but more sophisticated forms of intelligence are requested to permit sensor units to be deployed in real environments.

4.10.2 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.

4.10.3 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, ZeroMQ, and MQTT would provide lightweight data transport. "MQ" in "MQTT" came from IBM's MQ Series message queuing product line. Fog computing is a viable alternative to prevent such large burst of data flow through Internet. The edge devices' computation power can be used to analyse and process data, thus providing easy real time scalability.

4.11 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.

4.11.1 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.

4.11.2 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.

4.12 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.

4.12.1 A Solution To "Basket Of Remotes"

According to the CEO of Cisco, the commercial opportunity for "connected products ranging from cars to household goods" is expected to be a $USD 19 trillion. Many IoT devices have a potential to take a piece of this market. Jean-Louis Gassée (Apple initial alumni team, and BeOS co-founder) has addressed this topic in an article on Monday Note, where he predicts that the most likely problem will be what he calls the "basket of remotes" problem, where we'll have hundreds of applications to

interface with hundreds of devices that don't share protocols for speaking with one another. There are multiple approaches to solve this problem, one of them called the "predictive interaction", where cloud or fog based decision makers will predict the user's next action and trigger some reaction. For user interaction, new technology leaders are joining forces to create standards for communication between devices. While AllJoyn alliance is composed of the top 20 World technology leaders, there are also big companies that promote their own protocol like CCF from Intel. Manufacturers are becoming more conscious of this problem, and many companies have begun releasing their devices with open APIs. Many of these APIs are used by smaller companies looking to take advantage of quick integration.

4.12.2 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.

4.13 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 fulfil:

4.14 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.

4.14.1 Medium-Range Wireless

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

4.14.2 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.

4.15 Wired

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

4.16 Simulation

IoT modeling and simulation (and emulation) is typically carried out at the design stage before deployment of the network. Network simulators like OPNET, NetSim 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.

4.16.1 Politics and civic engagement

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

4.17 Criticism and controversies

4.17.1 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's 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.

4.18 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 behavior, citing an instance of billboards with hidden cameras that tracked the demographics of passers-by who stopped to read the advertisement. The Internet of Things Council compared the increased prevalence of digital surveillance due to the Internet of things to the conceptual panopticon described by Jeremy Bentham in the 18th Century. The assertion was defended by the works of French philosophers Michel Foucault and Gilles Deleuze. In Discipline and Punish: The Birth of the Prison Foucault asserts that the panopticon was a central element of the discipline society developed during the Industrial Era. Foucault also argued that the discipline systems established in factories and school reflected Bentham's vision of panopticism. In his 1992 paper "Postscripts on the Societies of Control," Deleuze wrote that the discipline society had transitioned

into a control society, with the computer replacing the panopticon as an instrument of discipline and control while still maintaining the qualities similar to that of panopticism.

4.18.1 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.

4.18.2 Security:

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

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

4.19 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."

4.19.1 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.

4.19.2 Intentional obsolescence of devices:

The Electronic Frontier Foundation has raised concerns that companies can use the technologies necessary to support connected devices to intentionally disable

or "brick" their customers' devices via a remote software update or by disabling a service necessary to the operation of the device. In one example, home automation devices sold with the promise of a "Lifetime Subscription" were rendered useless after Nest Labs acquired Revolv and made the decision to shut down the central servers the Revolv devices had used to operate. As Nest is a company owned by Alphabet (Google's parent company), the EFF argues this sets a "terrible precedent for a company with ambitions to sell self-driving cars, medical devices, and other high-end gadgets that may be essential to a person's livelihood or physical safety." Owners should be free to point their devices to a different server or collaborate on improved software. But such action violates the United States DMCA section 1201, which only has an exemption for "local use". This forces tinkerers who want to keep using their own equipment into a legal grey area. EFF thinks buyers should refuse electronics and software that prioritize the manufacturer's wishes above their own. Examples of post-sale manipulations include Google Nest Revolv, disabled privacy settings on Android, Sony disabling Linux on PlayStation 3, and enforced EULA on Wii U.

4.20 IoT Adoption Barriers

4.20.1 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.

.

CHAPTER 5

RESULS AND DISCUSSION PERFORMANCE ANALYSIS

5.1 Arduino c:

- Open-source hardware shares much of the principles and approach of free and open-source software.
- In particular, we believe that people should be able to study our hardware to understand how it works, make changes to it, and share those changes. To facilitate this, we release all of the original design files (Eagle CAD) for the Arduino hardware.
- These files are licensed under a Creative Commons Attribution Share-Alike license, which allows for both personal and commercial derivative works, as long as they credit Arduino and release their designs under the same license.
- The Arduino software is also open-source. The source code for the Java environment is released under the GPL and the C/C++ microcontroller libraries are are under the LGPL.

5.1.1 Arduino IDE

Get the latest version from the download page. You can choose between the Installer (.exe) and the Zip packages. We suggest you use the first one that installs directly everything you need to use the Arduino Software (IDE), including the drivers. With the Zip package you need to install the drivers manually. The Zip file is also useful if you want to create aportable installation.

When the download finishes, proceed with the installation and please allow the driver installation process when you get a warning from the operating system.

Arduino is a tool for making computers that can sense and control more of the physical world than your desktop computer. It's an open-source physical computing platform based on a simple microcontroller board, and a development environment for writing software for the board.

Arduino can be used to develop interactive objects, taking inputs from a variety of switches or sensors, and controlling a variety of lights, motors, and other physical

outputs. Arduino projects can be stand-alone, or they can be communicate with software running on your computer (e.g. Flash, Processing, MaxMSP.) The boards can be assembled by hand or purchased preassembled; the open-source IDE can be downloaded for free.

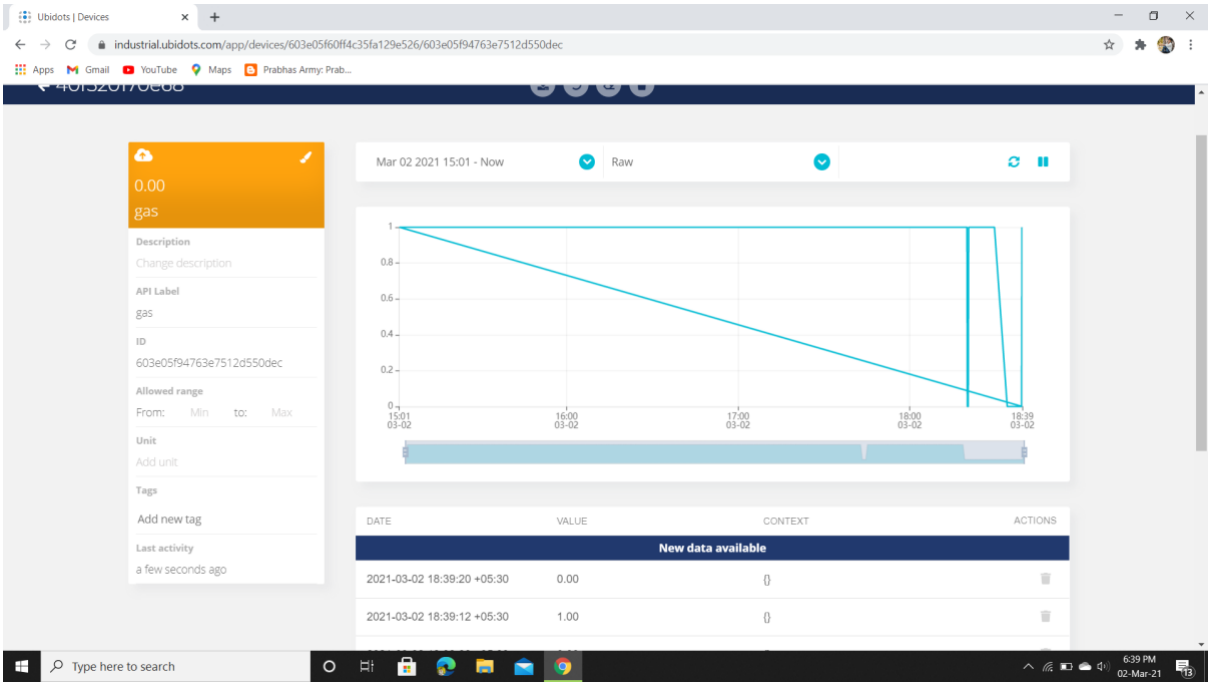

FIG : 5.1 : Graphical Representation Of Gas

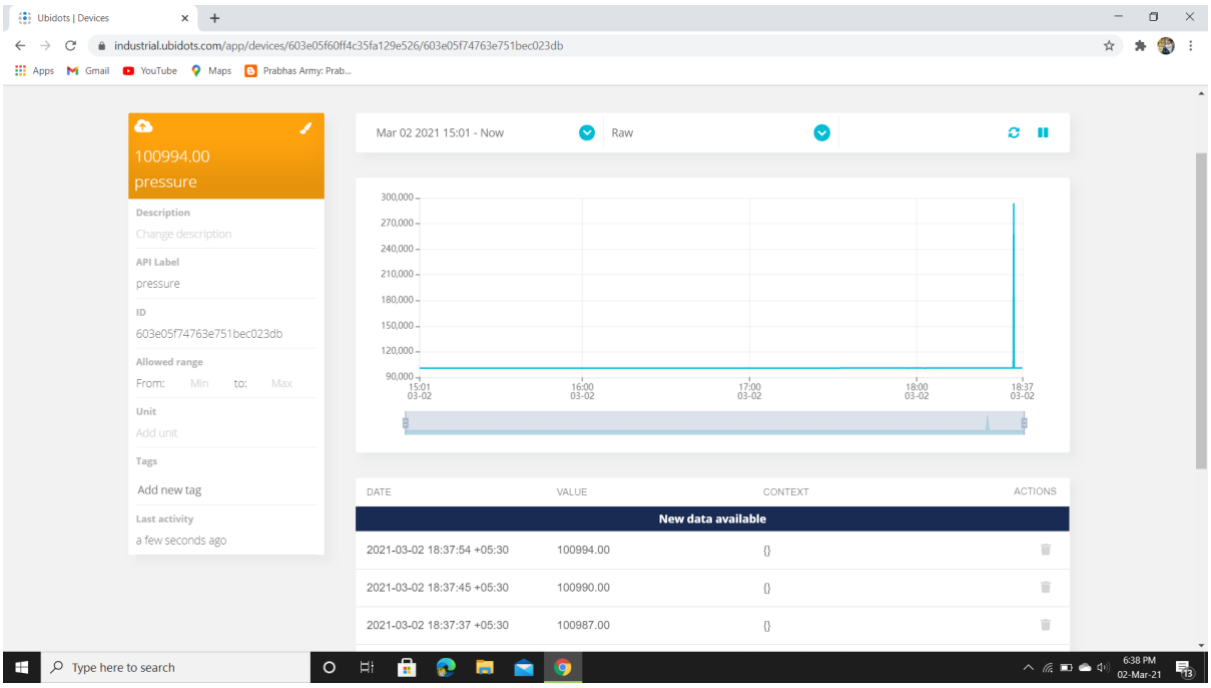

FIG : 5.2 : Graphical Representation Of Pressure

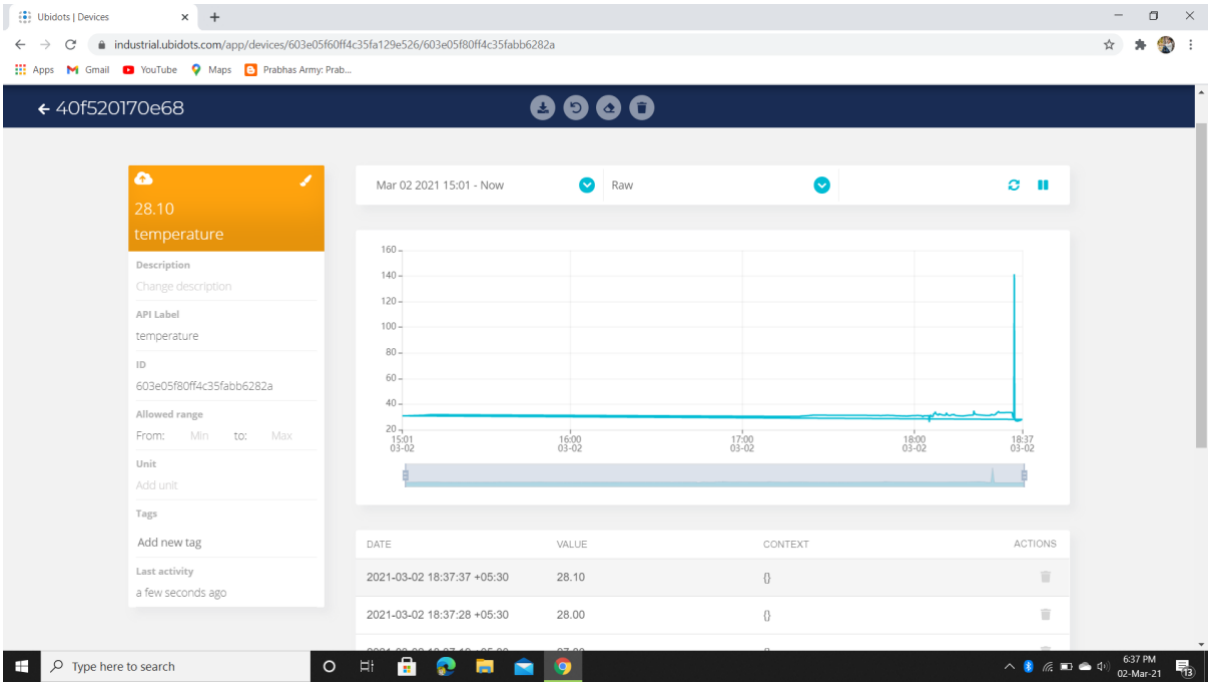

FIG : 5.3 : Graphical Representation Of Temperature

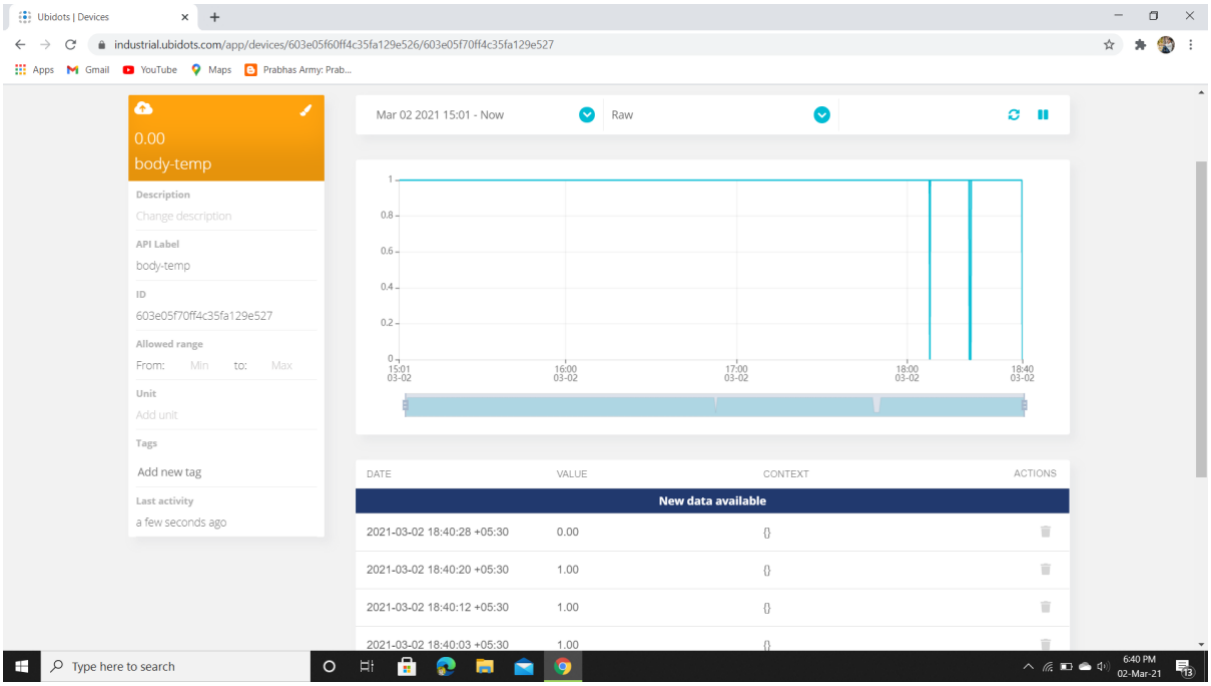

FIG : 5.4 : Graphical Representation Of Body-Temp

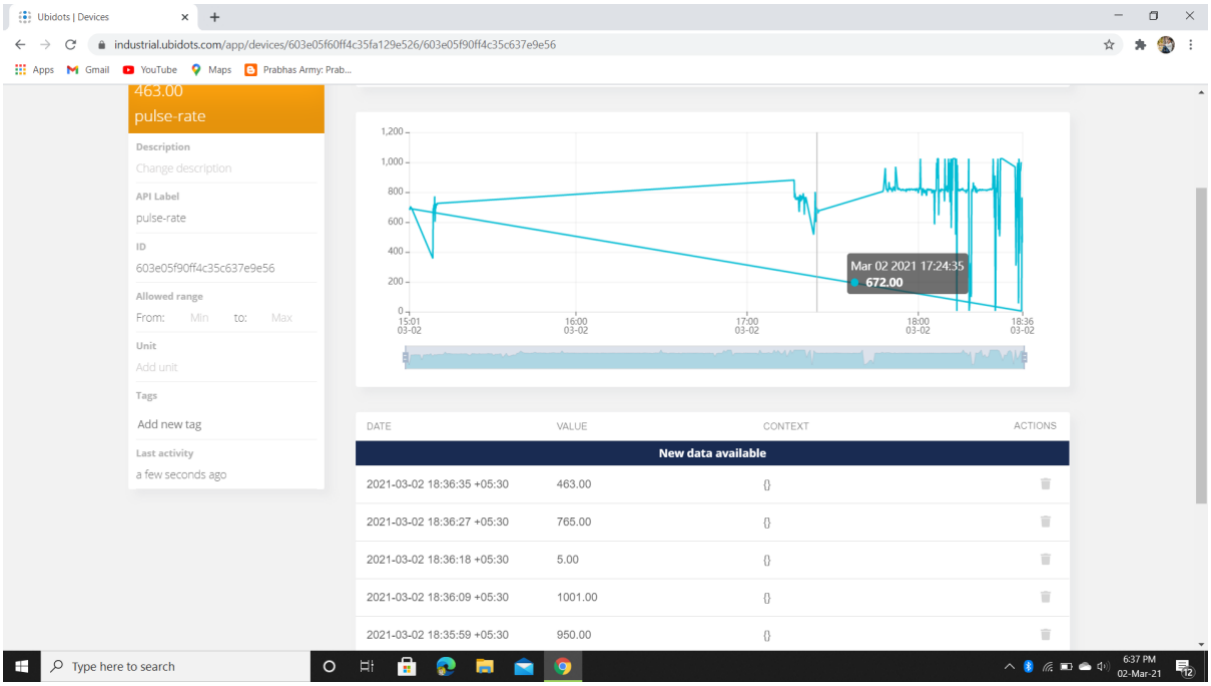

FIG : 5.5 : Graphical Representation Of Pulse Rate

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Proceed with board specific instructions

When the Arduino Software (IDE) is properly installed you can go back to the Getting Started Home and choose your board from the list on the right of the page.

6.2 CONCLUSION

Monitor army solider using biological sensors and transfer the information to the chief kernel using IOT

REFERENCE:

[1] Matthew J. Zieniewicz, Douglas C. Johnson, Douglas C. Wong, and John D. Flat —The Evolution of Army Wearable Computers‖ Research,Development and engineering center,US Armu communication October–December 2002.

[2] Wayne Soehren &Wes Hawkinson —Prototype Personal NavigatioNavigationn system‖,IEEE A&E system magazine April-2008.

[3] Simon L. Cotton and William G. Scanlon —Millimeter - wave Soldier –to-soldier communications for covert battlefield operation‖ Defence science and Tecnlogy laboratory, IEEE communication Magzin October 2009.

[4] Alexandrous Plantelopoulous and Nikolaos ,G. Bourbakis‖A Survey on Wearable sensor based system for health monitoring and prognosis‖ IEEE Transaction on system,Man and Cybernetics ,Vol.40,No.1, January 2010.

[5] A uderey Giremus,Jean-yves Tourneret,Senior member,IEEE &Arnaud Doucet—A fixed-Lag particle filter for the joint Detection/Compensation of interference effects in GPS Navigation—December-2011.

[6] Hock Beng Lim “A Soldier Health Monitoring System for Military Applications‖ 2010 International Conference on Body Sensor Networks (BSN).

[7] Jouni Rantakoko,Joakim Rydell and peter Stromback,‖Accurate and Realiable soldier and first responder Poasitioning :Multisensor System and co-operative localization‖April-2011

[8] Ravidra B.Sathe ,A.S.Bhide.‖Gps-based soldier tracking and health monitoring system‖ conference on Advances in communication and computing April 2011-12.

[9] Vincent Pereira,Audrey Giremus,anderic grivel —Modeling of multipath environment using copulas For particle filtering based GPS navigation‖ June-2012

[10] Warwick A. Smith; —ARM Microcontroller Interfacing ardware and Software‖.