Health Care Monitoring System by Using IOT and Arduino

DIVYA LAKSHMI [1],JAYAKANTH D[2], SIMEON DANIEL S[3],SAM RUBAN S [4],SARAN B[5] ,VIJAY V[6]

[1]Assistant Professor -Department of Information Technology & Kings Engineering College-India.

[2,3,4,5,6] Department of Information Technology & Kings Engineering College-India.

---***---

Abstract - Advances in devices and systems enabled with wireless communication have a substantial impact in the field of healthcare. Monitoring patient's health status anytime and anywhere without limiting the patient's movement as a consequenceof being tied down through cables to the monitoring equipment is an important application.Through the reduction in the size of sensors and the use of wireless interface to transmit the data recorded by the sensors, health care monitoring can be stretched beyond the hospital boundaries. This is considered to be a fundamental technology for integration of universal healthcare systems in IOT application with the capacity of reducing the expenses incurred in health care.This is because the physician is able to monitor the patient's advancement or deterioration in health without having to spend on the cost of hospitalization. The incorporation of wireless communication into medical applications has immense benefits. With wireless technology, the patients can be monitored from a remote location and this is efficient to a certain extent. This would also enable smart monitoring of multiple patients simultaneously. When an alarming condition occurs in a patient, the doctor in charge could be notified to take appropriate action.

1. INTRODUCTION

1.1 GENERAL

The Internet of Things (IOT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer D

A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. IOT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS), micro services and the internet. The convergence has helped tear down the silo walls between operational technology (OT) and information technology (IT), allowing unstructured machine-generated data to be analyzed for insights that will drive improvements.

Today computers -- and, therefore, the internet are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of datą available on the internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code. The problem is, people have limited time, attention and accuracy all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things -- using data they gathered without any help from us

we would be able to track and count everything and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling and whether they were fresh or past their best.

FIGURE.1.1 Internet of Things

1.2 HISTORY

The internet isn't that old, so far as the world wide web. In 1974, the TCIP/IP structure that we know today had it's birth. It was not until ten years later that the first domain name system or DNS was introduced. The first website actually came online in 1991. The internet that he had proposed just a scant two years earlier came crashing into our mainstream world. It was a technological awakening that had been a long time coming.

In no time the internet took over. By 1995, multiple websites and systems came online. Entertainment by means of bulletin board systems began to be seen. All of it came from the imaginings of others that had taken place decades earlier.

The term "internet of things" or "IOT" is also not a new one. It's frequently used and has been so for years, but in a survey it was revealed that even those who work in it every day are not at all conversant with the history of the IOT. That history or at least the ideology goes back a great deal further than most people know The first look at the internet of things arguably came from Nicola Tesla in 1926 when he commented in Collier's "When wireless"* is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket." It was a comment that got him laughed at in some circles, but one which was remarkably accurate considering the state of computing at that time.

In 1998, Google incorporated and too, in 1998, in Touch a project that was developed at MIT was put into play by Scott Brave and Professor Hiroshi Ishii who announced "... We then present in Touch, which applies Synchronized Distributed Physical Objects to create a "tangible telephone" for long distance haptic communication. "In 1998, the real IOT was touched by Mark Weiser, who developed a water fountain that was amazing and delightful to everyone who saw it. It rose and fell respectively according to the pricing trends and the volume of stock on the NYSE.1999 saw the term Internet of Things spoken by Kevin Ashton who was the then executive director for the Auto-ID Center. "I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention.

Business Week in 1999 was the scene of the next big announcement about the term Internet of Things. 1999 Neil Gross, speaking to Business Week commented, "In the next century, planet earth will don an electronic skin. It will use the Internet as a scaffold to support and transmit its sensations. This skin is already being stitched together. It consists of millions of embedded electronic measuring devices: thermostats, pressure gauges, pollution detectors, cameras, microphones, glucose sensors, EKG's, electroencephalographs. These will probe and monitor cities and endangered species, the atmosphere, our ships, highways and fleets of trucks, our conversations, our bodies-even our dreams. "IOT has continued to grow and to evolve and projections are bright for this new methodology for using the internet. The future of IOT is now with devices coming online every day. The world is reliant upon connected cars, connected medical devices and even connected homes Companies today are scrambling to get their own IOT systems online and moving, and new recruits are being brought in every day to head up IOT systems in companies from small to large.

1.3 WHY IOT

It goes without saying that cyber security is a serious concern, especially as internet and online services become more ingrained in our lives. Since the advent of Internet of Things (IoT), the number of connected devices in our homes, office and on our person is growing at a fast pace. Connected devices already outnumber human beings, and continue to propagate at a chaotic pace across many fields, including healthcare, home appliances, industrial control systems (ICS) and vehicles.

The rise of IoT brings huge advantages to businesses, consumers, government agencies and researchers in different sectors. Energy savings, better customer service, enhanced health data, improved vehicle performance and accurate crash analysis are just some of the benefits of IOT technology.

But the benefits it brings to malicious hackers and cybercriminals are enormous as well, and the IOT security nightmare has already become a cause of serious concern. In this post, I will explain how IOT security is different from traditional cyber security we've all come to know and love (or loath, if you like), and why it should be taken more seriously.

1.4 PRIVACY ISSUES

IOT devices generate a lot of data. Some of this data, such as health-related information, is quite confidential and intimate, and is subject to laws and regulations such as HIPAA. Others, such as data generated by your connected toaster or light bulb, might not be very sensitive per se, but when combined with data from your smart lock, smart fridge, motion sensors... it can give away much about your life patterns and habits.

Moreover, the storage and distribution of the generated data is the issue of much debate. For most devices, the data is stored on cloud servers, and is later used by service providers to make assumptions about user interaction with devices and make decisions that will improve user experience (or at least that's what they say).

However, regulations that are in place pertaining to the boundaries of ownership of data are not nearly enough to address the issues we're facing with the explosion of data generation and consumption. What kind of data can vendors collect exactly (does anyone remember the connected TVs that spy on users or Hello Barbie dolls that record children's interactions)? How much authority do vendors have over the data they collect from their consumers? Whom can they share it with? How long can they store it? What are the encryption and storage protection laws that apply to IOT data? These are just some of the questions tech experts and legislators will have to deal with very soon. And the in consistencies in data privacy rules across different countries only adds dimensions to the IOT privacy Rubik's Cube.

1.5 NETWORK SECURITY ISSUES

A considerable percentage of IoT devices are lacking proper means to protect themselves against network breaches. In some cases, this can be critical, such as a smart lock that is remotely compromised and unlocked by a malicious actor, or vulnerable baby monitors that allow hackers to pick up live feed of you children. In other cases, such as smart sensors or connected kettles, it might not be a big deal, you might argue. Cyber criminals usually grab at every opportunity to exploit a vulnerability. And as far as they're concerned, IOT security issues aren't a "let me hack your light bulb and turn it on and off at my own will" situation (though I do admit 'that such an occurrence would be annoying) but rather an "I'll compromise you light bulb and gain access to your network" opportunity.
See where it's leading?
The problem is each new connected device can become a path into the network, which we call "attack vectors" in cyber security jargon.

Compromised devices can become beachheads for more serious attacks, allowing hackers to move laterally across the network and gain access to more critical information and devices. Smart kettles that give away Wi-Fi passwords and smart fridges that give away Gmail credentials are testament to the case Of special concern are smart homes, which are lacking the IT security infrastructure that organizations and tech firms are equipped with, house some of the most vulnerable devices, and can become attractive targets for malicious actors.

1.6 SAFETY ISSUES

IoT security issues go beyond the simple data theft, network manipulation hacks, and financial losses. In many cases, it has to do with the health and safety of real human beings or the functionality of critical infrastructure that affects the lives of thousands and millions of people. Smart rifles that can be hacked to designate new targets remotely, drug infusion pumps that can be compromised to harm or kill the patient through dosage change, cars that can be shut down remotely while driving at 70 mph, and entire power grids that can brought offline are just some of the cases that have surfaced in the recent year.

The IoT is now responsible for many critical functionalities in the home, office and across the entire metropolitan life. And with the forecasts made by Gartner, it will only grow larger and more prominent in the coming years. It can easily ruń out of control and pave the way for a new wave of totally different acts of terrorism and felony.

Just think about the spooky opportunities that'll arise when driverless cars become main stream. Remote abductions and car crashes are two things that comes to the mind. I don't know about you, but it gives me the shivers.

As we approach singularity, more and more of our identities are being digitized and sent into the cloud, thanks in large part to IOT. IOT is the future, and it is one of the biggest things that has happened in the history of the internet. We have to prepare ourselves for the worst if we want to take advantage of the best. Taking IOT security seriously will be an important factor in this regard.

1.7 MEDICAL USES

1. Monitor Both Machine and Patient Health-While connected patient medical devices can provide unparalleled access to individual health, with connected equipment, techs can also monitor the health of the machines of which they're in charge. This is especially helpful for those must-have machines that are imperative for patient care. Having this kind 24/7 automatic monitoring can give piece of mind to those organizations in charge of keeping vital medical equipment up and running.

2. Ensure Equipment is Spread Equally Across Machines-Keeping equipment running is the main concern for medical equipment companies, but making sure it's used effectively can also help service organizations see tremendous benefits. IOT Sensors have the ability to reveal how long, how often, and how well machines are being used.

This means that if one piece of equipment is continually overused, while is rarely used, companies can make adjustments so they receive equal wear

3. Understand Where to Implement Equipment Improvements-With an endless flow of data from device to manufacturer, companies receive insights into how equipment can be modified or upgraded. For example, if a particular device tends to use resources too quickly, the manufacturer can change the design in the next iteration of the equipment. Useful data about the efficiency or performance of the equipment can make the manufacturing process more efficient, and by relation, healtficare as well.

There are many advantages of incorporating IOT into our lives, which can help individuals, businesses, and society on a daily basis. For individuals this new concept can come in many forms including health, safety, financially, and every day planning.

1.8 IOT ADVANTAGES

The integration of IoT into the health care system could prove to be incredibly beneficial for both an individual and a society. A chip could be implemented into each individual, allowing for hospitals to monitor the vital signs of the patient.

- By tracking their vital signs, it could help indicate whether or not serious assessment is necessary
- With all of the information that is available on the Internet, it can also scare people into believing they need more care than what is really needed.
- Hospitals already struggle to assess and take care of the patients that they have. By monitoring individual's health, it will allow them to judge who needs primary attention
- The Internet of Things can also assist people with their personal safety.
- ADT, which is a home security system, allows individuals to monitor their security systems at home through their phones, with the ability to control it.
- Also, another technology that has already been released is GM OnStar.
- This is a system that is embedded in GM cars that can detect if a crash has occurred and it automatically calls 9-1-1. It can also track the movement of the car.

2PROPOSED SYSTEM

2.1 INTRODUCTION

This chapter deals with Hardware and software architecture. Components are briefly explained with pin configuration. PIC16F877A is one of the most renowned microcontrollers in the industry. This controller is very convenient to use, the coding or programming of this controller is also easier. The processed data is displayed in the LED display via the Arduino. Arduino is an open source computer hardware and software company, project, and user community that designs and manufactures single-board microcontrollers and microcontroller kits for building digital devices and interactive objects that can sense and control objects in the physical world. Power supply is given to all the components. Voltage regulator is used. The processed data is sent to ESP8266(WI-FI module), it is a self contained SOC with TCP/IP protocol.

2.2 ARDUINO

Arduino is an open source computer hardware and software company, project, and user community that designs and manufactures single-board microcontrollers and microcontroller kits for building digital devices and interactive objects that can sense and control objects in the physical world. The project's products are distributed as open-source hardware and software, which are licensed under the GNU Lesser General Public License (LGPL) or the GNU General Public License (GPL), permitting the manufacture of Arduino boards and software distribution by anyone. Arduino boards are available commercially in preassembled form, or as do-it-yourself (DIY) kits.

Arduino microcontrollers are pre-programmed with a boot loader that simplifies uploading of programs to the on-chip flash memory. The default boot loader of the arduino UNO is the optiboot bootloader. 12 月 Boards are loaded with program code via a serial connection to another computer. Some serial Arduino boards contain a level shifter circuit to convert between RS-232 logic levels and transistor-transistor logic (TTL) level signals. Current Arduino boards are programmed via Universal Serial Bus (USB), implemented using USB-to-serial adapter chips such as the FTDI FT232. Some boards, such as later-model Uno boards, substitute the FTDI chip with a separate AVR chip containing USB-to-serial firmware, which is reprogrammable via its own ICSP header.

Other variants, such as the Arduino Mini and the unofficial Boarduino, use a detachable USB-to-serial adapter board or cable, Bluetooth or other methods. When used with traditional microcontroller tools, instead of the Arduino IDE, standard AVR in-system programming (ISP) programming is used.

The Arduino project provides the Arduino integrated development environment (IDE), which is a cross-platform application written in the programming language Java. It originated from the IDE for the languages Processing and Wiring. It includes a code editor with features such as text cutting and pasting, searching and replacing text, automatic indenting. brace matching, and syntax highlighting, and provides simple one-click mechanisms to compile and upload programs to an Arduino board. It also contains a message area, a text console, a toolbar with buttons for common functions and a hierarchy of operation menus.

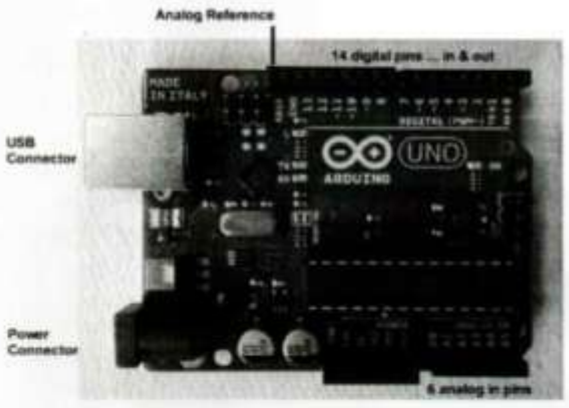

FIGURE.3.1 Arduino Board

2.3 ESP8266 WI-FI MODULE

Wi-Fi or WiFi is a technology for wireless local area networking with devices based on the IEEE 802.11 standards. Wi-Fi is a trademark of the Wi-Fi Alliance, which restricts the use of the term Wi-FiCertified to products that successfully complete interoperability certification testing

Wi-Fi most commonly uses the 2.4 gigahertz (12 cm) UHF and 5.8 gigahertz (5 cm) SHFISM radio bands. Anyone within range with a wireless modem can attempt to access the network; because of this, Wi-Fi is more vulnerable to attack (called eavesdropping) than wired networks. Wi-Fi Protected Access is a family of technologies created to protect information moving across Wi-Fi networks and includes solutions for personal and enterprise networks. Security features of Wi-Fi Protected Access constantly evolve to include stronger protections and new security practices as the security landscape changes,

2.3.1 WI-FI radio spectrum

802.11b and 802.11g use the 2.4 GHzISM band, operating in the United States under Part 15 Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones, and Bluetooth devices.

Spectrum assignments and operational limitations are not consistent worldwide: Australia and Europe allow for an additional two channels (12, 13) beyond the 11 permitted in the United States for the 2.4 GHz band, while Japan has three more (12-14). In the US and other countries, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations.

A Wi-Fi signal occupies five channels in the 2.4 GHz band. Any two channel numbers that differ by five or more, such as 2 and 7, do not overlap. The oft-repeated adage that channels 1, 6, and 11 are the only non-overlapping channels is, therefore, not accurate. Channels 1, 6, and 11 are the only group of three non-overlapping channels in North America and the United Kingdom. In Europe and Japan using Channels 1, 5, 9, and 13 for 802.11g and 802.11n is recommended

802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap.

2.3.2 RANGE

The Wi-Fi signal range depends on the frequency band, radio power output, antenna gain and antenna type as well as the modulation technique. Line-of-sight is the thumbnail guide but reflection and refraction can have a significant impact.

An access point compliant with either 802.11b or 802.11g, using the stock antenna might have a range of 100 m (0.062 mi). The same radio with an external semi parabolic antenna (15 dB gain) might have a range over 20 miles.

Higher gain rating (dBi) indicates further deviation (generally toward the horizontal) from a theoretical, perfect isotropic radiator, and therefore the further the antenna can project a usable signal, as compared to a similar output power on a more isotropic antenna. For example, an 8 dBi antenna used with a 100 MW driver will have a similar horizontal range to a 6 dBi antenna being driven at 500 MW. Note that this assumes that radiation in the vertical is lost, this may not be the case in some situations, especially in large buildings or within a waveguide. In the above example, a directional waveguide could cause the low power 6 dBi antenna to project much further in a single direction than the 8 dBi antenna which is not in a waveguide, even if they are both being driven at 100 MW.

IEEE 802.11n, however, can more than double the range. Range also varies with frequency band. Wi-Fi in the 2.4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block used by 802.11a (and optionally by 802.11n). On wireless routers with detachable antennas, it is possible to improve range by fitting upgraded antennas which have higher gain in particular directions. Outdoor ranges can be improved to many kilometers through the use of high gain directional antennas at the router and remote device(s). In general, the maximum armount of power that a Wi-Fi device can transmit is limited by local regulations, such as FCC Part 15 in the US. Equivalent isotropically radiated power (EIRP) in the European Union is limited to 20 dBm (100 MW).

To reach requirements for wireless LAN applications, Wi-Fi has fairly high power consumption compared to some other standards. Technologies such as Bluetooth (designed to support wireless personal area network (PAN) applications) provide a much shorter propagation range between 1 and 100 mand so in general have a lower power consumption.

Researchers have developed a number of "no new wires" technologies to provide alternatives to Wi-Fi for applications in which Wi-Fi's indoor range is not adequate and where installing new wires (such as CAT-6) is not possible or cost-effective. For example, the ITU-TG.hn standard for high speed local area networks uses existing home wiring (coaxial cables, phone lines and power lines). Although G.hn does not provide some of the advantages of Wi-Fi (such as mobility or outdoor use), it is designed for applications (such as IPTV distribution) where indoor range is more important than mobility. For the best performance, a number of people only recommend using wireless networking as a supplement to wired networking.Due to the complex nature of radio propagation at typical Wi-Fi frequencies, particularly the effects of signal reflection off trees and buildings, algorithms can only approximately predict Wi-Fi signal strength for any given area in relation to a transmitter. This effect does not apply equally to long-range Wi-Fi, since longer links typically operate from towers that transmit above the surrounding.The practical range of Wi-Fi essentially confines mobile use to such applications as inventory-taking machines in warehouses or in retail spaces, barcode-reading devices at check-out stands, or receiving/shipping stations. Mobile use of Wi-Fi over wider ranges is limited, for instance, to uses such as in an automobile moving from one hotspot to another. Other wireless technologies are more suitable for communicating with moving vehicles.

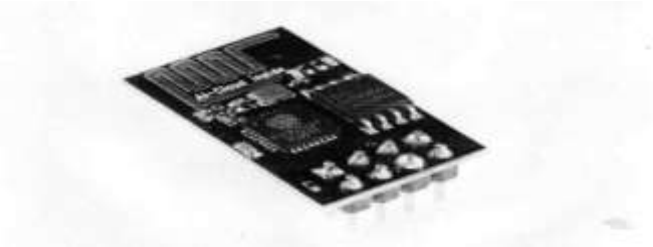

FIGURE.2.2 WI-FI module

2.4 LCD DISPLAY

LCD (liquid crystal display) is the technology used for displays in notebook and other smaller computers. Like light-emitting diode (LED)

and gas-plasma technologies, LCDs allow displays to be much thinner than cathode ray tube (CRT) technology. LCDs consume much less power than LED and gas-display displays because they work on the principle of blocking light rather than emitting it.

An LCD is made with either a passive matrix or an active matrix display display grid. The active matrix LCD is also known as a thin film transistor (TFT) display. The passive matrix LCD has a grid of conductors with pixels located at each intersection in the grid. A current is sent across two conductors on the grid to control the light for any pixel. An active matrix has a transistor located at each pixel intersection, requiring less current to control the luminance of a pixel

FIGURE.2.3 LCD Display

2.4.1 WORKING PRINCIPAL OF LCD

LCD (liquid crystal display) is the technology used for displays in notebook and other smaller computers. Like light-emitting diode (LED) and gas-plasma technologies, LCDs allow displays to be much thinner than cathode ray tube (CRT) technology. LCDs consume much less power than LED and gas-display displays because they work on the principle of blocking light rather than emitting it.

An LCD is made with either a passive matrix or an active matrix display display grid. The active matrix LCD is also known as a thin film transistor (TFT) display. The passive matrix LCD has a grid of conductors with pixels located at each intersection in the grid. A current is sent across two conductors on the grid to control the light for any pixel. An active matrix has a transistor located at each pixel intersection, requiring less current to control the luminance of a pixel.

Next comes to the second piece of glass with an electrode in the form of the rectangle on the bottom and, on top, another polarizing film. It must be considered that both the pieces are kept at right angles. When there is no current, the light passes through the front of the LCD it will be reflected by the mirror and bounced back. As the electrode is connected to a battery the current from it will cause the liquid crystals between the common-plane electrode and the electrode shaped like a rectangle to untwist. Thus the light is blocked from passing through. That particular rectangular area appears blank.

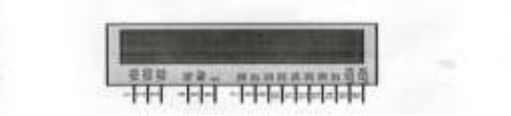

FIGURE.2.4 LCD Display

2.4.2 APPLICATION

They are used in a wide range of applications including: computer monitors, television, instrument panels, aircraft cock displays, signage, etc. They are common in consumer devices such as video players, gaming devices, clocks, watches, calculators, and telephones. LCDs have displaced cathode ray tube(CRT) displays in most applications. They are usually more compact, lightweight, portable, less expensive, more reliable, and easier on the eyes. They are available in a wider range of screen sizes than CRT and plasma displays, and since they do not use phosphors, they cannot suffer image burn-in.

2.5 Circuit diagram of proposed system

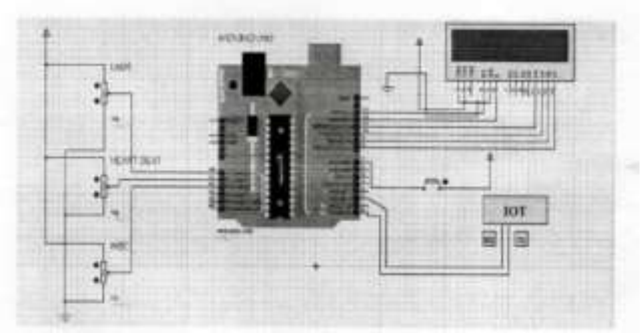

FIGURE.3.5 Circuit diagram

2.5.1 DISCRIPTION

ARDUINO

Arduino is an open source computer hardware and software company, project, and user community that designs and manufactures single-board microcontrollers and microcontroller kits for building digital devices and interactive

LCD DISPLAY

LCD (liquid crystal display) is the technology used for displays in notebook and other smaller computers. jects that can sense and control objects in the physical world.

PIR SENSOR

A passive infrared sensor (PIR sensor) is an electronic sensor that measures infrared (IR) light radiating from of view..

WET SENSOR

It is a self designed sensor it detects the patients wet condition and intimates to the nurse via the buzzer bjects in its field of view

TEMPERATURE SENSOR

Temperature with its output proportional to the temperature (in "C).

2.6 ADVANTAGE

- Improved Outcomes of Treatment
- Improved Disease Management
- Reduced Errors
- Better Patient Experience

2.7 APPLICATION

- Rural Health
- Correctional Facilities
- School-Based Health Centers
- Mobile Health Clinics

3.HARDWARE DETIALS

3.1 POWER SOURCE

There are common configurations for 78xx ICs, including 7805 (5 V), 7806 (6 V), 7808 (8 V), 7809 (9V), 7810 (10 V), 7812 (12 V), 7815 (15 V), 7818 (18 V), and 7824 (24 V) versions. The 7805 is the most common, as its regulated 5-volt supply provides a convenient power source for most TTL. components.

Less common are lower-power versions such as the LM78Mxx series (500 mA) and LM78Lxx series (100 mA) from National Semiconductor. Some devices provide slightly different voltages than usual, such as the LM781.62 (6.2 volts) and LM78L82 (8.2 volts) as well as the STMicroelectronics L78133ACZ (3.3 volts).

3.2 HARDWARE

3.2.1 Transformer:

AC-240 V to AC 12 V.RM0513 is a general purpose chassis mounting mains transformer. Transformer has 240 V primary windings and centre tapped secondary winding. The transformer has flying colored insulated connecting leads (Approx 100 mm long). The Transformer act as step down transformer reducing AC 240 V to AC-12 V.The Transformer gives two outputs of 12 V, 24 V and OV.

3.2.2 Bridge Rectifier:

A Bridge rectifier is an Alternating Current (AC) to Direct Current (DC) converter that rectifies mains AC input to DC output. Bridge Rectifiers are widely used in power supplies that provide necessary DC voltage for the electronic components or devices. They can be constructed with four or more diodes

Depending on the load current requirements, a proper bridge rectifier is selected. Components' ratings and specifications, breakdown voltage,
temperature ranges, transient current rating, forward current rating. mounting requirements and other considerations are taken

into account while selecting a rectifier power supply for an appropriate electronic circuit's application.

3.2.3 Voltage Regulator:

7805 is a voltage regulator integrated circuit. It is a member of 78xx series of fixed linear voltage regulator ICs. The voltage source in a circuit may have fluctuations and would not give the fixed voltage output. The voltage regulator IC maintains the output voltage at a constant value. The xx in 78xx indicates the fixed output voltage it is designed to provide. 7805 provides +5V regulated power supply. Capacitors of suitable values can be connected at input and output pins depending upon the respective voltage levels

3.4 TEMPERATURE SENSOR LM35

LM35 is a precision IC temperature sensor with its output proportional to the temperature (in °C). The sensor circuitry is sealed and therefore it is not subjected to oxidation and other processes. With LM35, temperature can be measured more accurately than with a thermistor. It also possess low self heating and does not cause more than 0.1°C temperature rise in still air. The operating temperature range is from -55°C to 150°C. The output voltage varies by 10mV in response to every °C rise/fall in ambient temperature, i.e., its scale factor is 0.01V/°C.

3.4.2 FEATURES

- Linear +10.0 mV/ degree celsius
- ●0.5 degreecelsius accuracy guaranteeable (at +25degree celsius)
- Rated for full-55 to +150 degree celsius range
- Suitable for remote applications
- Low cost due to wafer-level trimming
- Operates from 4 to 30 volts
- Less than 60 Micro ampere current drain
- Low self-heating, 0.08 degree celsius in still air
- Nonlinearity only +/- 1/4 degree celsius typical
- Low impedance output, 0.1 Ohm for ImA load

3.5.5 PIR SENSOR

A passive infrared sensor (PIR sensor) is an electronic sensor that measures infrared (IR) light radiating from objects in its field of view. All objects with a temperature above absolute zero emit heat energy in the form of radiation. Usually this radiation isn't visible to the human eye because it radiates at infrared wavelengths, but it can be detected by electronic devices designed for such a purpose.

The term passive in this instance refers to the fact that PIR devices do not generate or radiate energy for detection purposes. They work entirely by detecting infrared radiation emitted by or reflected from objects. They do not detect or measure "heat”

3.5.1 PIR SENSOR WORKING

Whenever, human being (even a warm body or object with some temperature) passes through the field of view of PIR sensor, then it detects the infrared radiation emitted by a hot body motion. Thus, the infrared radiation detected by the sensor generates an electrical signal 3.

3.5.2 APPLICATIONS

- All outdoor Lights
- Lift Lobby
- Multi Apartment Complexes
- Common staircases
- For Basement or Covered Parking Area
- Shopping Malls
- For garden lights

3.5.3 FEATURES

- Complete with PIR, Motion Detection.
- Dual Element Sensor with Low Noise and High Sensitivity.
- Supply Voltage-5V.
- Delay Time Adjustable.
- Standard TTL Output.

3.6 WET SENSOR

It is a self designed sensor it detects the patients wet condition and intimates to the nurse via the buzzer It display the condition of the patient via the LCD ie wet detected or not so that the patient could be helped out.

3.7 BUZZER

A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave oven, or game shows. It most commonly consists of a number of switches or sensors connected to a control unit that determines if and which button was pushed or a preset time has lapsed, and usually illuminates a light on the appropriate button or control panel, and sounds a warning in the form

of a continuous or intermittent buzzing or beeping sound. Initially this device was based on an electromechanical system which was identical to an electric bell without the metal gong (which makes the ringing noise).

Often these units were anchored to a wall or ceiling and used the ceiling or wall as a sounding board. Another implementation with some AC-connected devices was to implement a circuit to make the AC current into a noise loud enough to drive a loudspeaker and hook this circuit up to a cheap 8-ohm speaker. Nowadays, it is more popular to use a ceramicbased piezoelectric sounder like a Sonalert which makes a highpitched tone.

Usually these were hooked up to "driver" circuits which varied the pitch of the sound or pulsed the sound. The circuit is designed to control the buzzer. The buzzer ON and OFF is controlled by the pair of switching transistors (BC 547). The buzzer is connected in the Q2 transistor collector terminal. When high pulse signal is given to base of the Q1 transistors, the transistor is conducting and close the collector and emitter terminal so zero signals is given to base of the Q2 transistor. Hence Q2 transistor and buzzer is turned OFF state. When low pulse is given to base of transistor Q1 transistor, the transistor is turned OFF. Now 12v is given to base of Q2 transistor so the transistor is conducting and buzzer is energized and produces the sound signal

3.8 SOFTWARE DEVELOPMENT

A program for Arduino may be written in any programming language for a compiler that produces binary machine code for the target processor. Atmel provides a development environment for their microcontrollers, AVR Studio and the newer Atmel Studio.

The Arduino project provides the Arduino integrated development environment (IDE), which is a cross-platform application written in the programming language Java. It originated from the IDE for the language processing and wiring. It includes a code editor with features such as text cutting and pasting and replacing text, automatic indenting, brace matching, and syntax highlighting. It provides simple one-click mechanisms to compile a message area a text console.

3.8.1 PROTEUS SOFTWARE

Proteus is a simulation software design tool developed by Lab center Electronics for Electrical and Electronic circuit design. It also possess 2D CAD drawing feature. It is a software containing schematic simulation as well as PCB designing

3.8.2 FEATURES OF PROTEUS SOFTWARE

ISIS has the wide range of components in its library. It has sources, signal generators, measurements and analysis tools like oscilloscope, voltmeter, ammeter etc..

ARES offers designing upto 14 inner layers, with surface mount and through hole packages. It is embedded with the foot prints of different category of components.

3.8.3 PROGRAMMING LANGUAGE:

Embedded c is a set of a language extensions for the e programming language by the e standards committee to address commonality issues that exist between e extensions for different embedded systems. Historically. embedded c programming requires non standard extensions to the c language in order to support exotic features such as fixed-point arithmetic multiple distinct memory banks, and basic I/O operations.

3.8.3.1 ADVANTAGE

- It is fairly efficient
- It is small and simpler to learn, understand, program and debug
- C compilers are available for almost all embedded devices in use today
- There is a large pool of experienced e programs

3.9 INTERNET OF THINGS OUTPUT

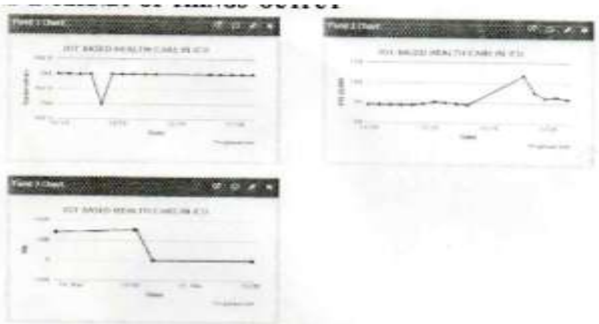

FIGURE4.9 WAVEFORMS

ACKNOWLEDGEMENT

We thank God for his blessings and also for giving as good knowledge and strength in enabling us to finish our project. Our deep gratitude goes to our founder late **Dr. D. SELVARAJ, M.A., M.Phil.,** for his patronage in the completion of our project. We like to take this opportunity to thank our honourable chairperson **Dr.S. NALINI SELVARAJ, M.COM., MPhil., Ph.D.** and honourable director, **MR.S. AMIRTHARAJ, M.Tech., M.B.A** for their support given to us to finish our project successfully. We wish to express our sincere thanks to our beloved principal. **Dr. C. Ramesh Babu Durai M.E., Ph.D** for his kind encouragement and his interest towards us. We are extremely grateful and thanks to our professor **Dr. D. C. Jullie Josephine M.Tech., PhD**, Head of Information Technology, Kings Engineering College, for his valuable suggestion, guidance and encouragement. We wish to express our sense of gratitude to our project supervisor **Mrs. DIVYA LAKSHMI M.E.,** Assistant Professor of Information Technology Department, Kings Engineering College whose idea and direction made our project a grand success. We express our sincere thanks to our parents, friends and staff members who have helped and encouraged us during the entire course of completing this project work successfully.

RESULTS

SUMMARY

The project is to recognize the movement of different part of the body of the comatose patients. Whenever the patient moves and blinks his/her eye are observed by the sensors and then send to the cloud for the doctors observance. The system monitor physically for getting the improvement of comatose patient for further treatment over them. This system, has developed a reliable, energy efficient for sending the messages to the concern person when the person is in coma.

CONCLUSION AND FUTURE WORK

CONCLUSION

In conclusion, this low cost system is designed to improve the standard living in home. The remote control function by pic16f877a provides help and assistance especially to disabled and elderly. In order to provide safety protection to the user, a low voltage activating switches is replaced current electrical switches. Moreover, implementation of wireless connection in control board allows the system installation in more simple way.

The control board is directly installed beside the electrical switches thereby the switching connection is controlled by relay. Furthermore, flexible types of connections are designed as backup connections to the system

REFERENCES

[1] Arnaud S.R.M. Ahouandjinou and CinaMotamed, on "Smart and Pervasive ICU based-IOT for improving intensive health care" IEEE internet of things journals, jan.2017.

[2]Mohammad Salah Uddin and Suraiya Banu, on "Real time patient monitoring system based on Internet of Things"IEEE internet of things journals, jan.2017.

[3] Barathram Ramkumarand M. Sabarimalai Manikandan on "Real-Time Signal Quality-Aware ECG Telemetry System for IoT-Based Health Care Monitoring"IEEE internet of things journals, jan.2017.

[4] Debeshi Dutta and Kunal Pal on "Finger movement based attender calling system for ICU patient management" IEEE internet of things journals, jan.2015.

[5]Malati Bansal and Bani Gandhi on"IoT based smart health care system using CNT electrodes"IEEE internet of things journals, jan.2017

[6]Deepika Agarwal and Punit Gupta on "IoT based smart healthcare kit" IEEE internet of things journals, jan. 2016

[7]IkhwanKim andYajie Qin on "Towards an IoT-based upper limb rehabilitation assessment system" IEEE internet of things journals, jan.2015.

[8]Limin Son and Yuan Zhang on "Ubiquitous WSN for Healthcare: Recent Advances and Future Prospects"IEEE internet of things journals, jan.2014