REPUBLIC OF YEMEN
SANA'A UNIVERSITY
FACTULTY OF ENGINEERING
ELECTRICAL DEPARTMENT
Communication Department

الجمهورية اليمنية
جامعة صنعاء
كلية الهندسة
قسم الهندسة الكهربائية
شعبة الاتصالات

Healthcare Based On Internet of Things

Prepared by:

Tasneem Abd-Albagi Mohammed Al_Mansoab (108/2016)

Nahla Yehia Saleh Obadi Al-Matari (125/2016)

Dua'a Kamel Haiderah Al-Afifi (247/2016)

Donia Shaker Mohammed Zaied (321/2016)

Entesar Yehia Yehia Al-Shobi (3055/2016)

Osama Yahya Ahmed Al-Marhabi (3082/2016)

Supervisors:

Dr. MOHAMMED HANKEL

مشروع مقدم لقسم الهندسة الكهربائية وهو جزء من متطلبات الحصول على درجة البكالوريوس في الهندسة الكهربائية.

صنعاء

2020

Acknowledgment

Our deepest thanks to our respectful supervisor

Dr. Mohammed Hankel for providing all the support and guidance through all stages of designing, implementing and documenting the project.

also to the largest and most famous encyclopedias which have provided assistance with sincerity all the time without any charge GOOGLE &YOUTUBE

We would like to thank our families for everything, since words will never fulfil.

ABSTRACT

Abstract The increased use of mobile technologies and smart devices in the area of health has caused great impact on the world. Health experts are increasingly taking advantage of the benefits these technologies bring, thus generating a significant improvement in health care in clinical settings and out of them. Likewise, countless ordinary users are being served from the advantages of the MHealth (Mobile Health) applications and E-Health (health care supported by ICT) to improve, help and assist their health.

Applications that have had a major refuge for these users, so intuitive environment. The Internet of things is increasingly allowing to integrate devices capable of connecting to the Internet and provide information on the state of health of patients and provide information in real time to Physicians who assist. It is clear that chronic diseases sign vital such as diabetes, heart, pressure and Temperature among others, are remarkable in the world economic and social level problem. In our project, we installed sensors that read vital indicators such as temperature, heart rate and oxygen in the blood. The data generated from the sensors is sent to the Thingspeak site, which stores patient data to be sent to the application database where the Thingspeak site is considered as an intermediary between the sensors and the application. The Physician has a large number of patients so it is difficult to review all the files of patients due to lack of time, Therefore, this application allows the Physician to review the patient's data according to time and at any time and then send any observations to the patient at that time or any other time since the application provides a special communication service between patients and Physician. where this application does not require the presence of Physician. and patient at the same time when measuring and sending Sensor data. The presence of patients in need of continuous supervision and suffering from chronic diseases and they are located in remote places and isolated or their physical condition is difficult to enable them to travel and mobility or the elderly, but this application provides these patients to follow their case and send their data in their places and homes This is because the wireless WAN service is now available in most areas and isolation.

Therefore, they only need the process of measuring and sending data through the application to follow up on their situation by the Physician. Because of the preoccupation of patients in their work and the lack of time and they need continuous follow-up of their situation by Physician. so

this application provides them to measure their condition at any time and space they get even when they do their work and in their offices. Often patients cannot keep all the papers to measure their previous data that they have done by the same thing for the Physician cannot work for the guidance of all patients and all their previous measurements have a defect or sometimes a defect in the database of the clinic if the Physician is doing a conservation of each data This application contains a database containing all the measurements for each patient that the Physician or patient can review at any time.

Contents

List of Figure

List of Table

Abbreviations

BLE	Bluetooth Low-Energy
ECG	Electrocardiogram
ECP	Embedded context prediction
EMG	Electromyography
GPS	Global position system
HTTP	Hypertext Transfer Protocol
IDE	Integrated Development Environment
IoT	Internet of Things
IoMT	Internet of Medical Things
IPv6	Internet protocol version 6
M2M	machine-to-machine
MOSFET	metal-oxide-semiconductor field-effect transistor
PAN	Personal Area Network
PLC	Power-line communication
RFID	radio-frequency identification
SMA	semantic medical access
WBANs	Wireless Body Area Networks
WSNs	Wireless sensor networks

Chapter 1

Introduction to IOT

The term “Internet of Things” is considered to be first coined in the starting of this century when work was done on MIT Auto-ID Center, to make a smart identification technology which will help to reduce the error rate subsequently increasing efficiency and to automate. But since then, the concept of IOT has evolved rapidly in various ways, as now with the help of this huge number small networks which can remain connected to each other and can directly send data to the main network without any human interaction. Quality of service in healthcare has always been under constant criticism in the modern era, as it is a very touchy subject. Health monitoring specially for patients or elderly people is a concern and as most people in the modern times are job holders and have so hectic life. It is difficult to manage to keep a constant watch on the patients or elderly of the house. Keeping a nurse or housekeeper is also a very costly issue nowadays. In this situation, remote health monitoring based on IOT can help to solve the problem.

1.1 IOT

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 (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

The definition of the Internet of Things has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of Things .The most prominent field that the Internet of Things is expected to develop is medicine. With the inclusion of medical devices in the concept of the Internet of Things the world will change completely, to make it clear to you that it is sufficient to tell you that a Chinese doctor has been able to perform a complete successful surgery for a patient in a different province from his place of residence through contacting a surgical system Full based on Internet of Things with the help of 5G Internet speeds.

Surgeries are not the only application of the Internet of Things, there are numerous researches that provide slides and devices that collect information about patients and link them to integrated health systems (the project model of what we can see later), that is, the sudden rise in blood pressure, clots, fainting and its causes Everything that might happen in an emergency will not be the subject of research and examination by doctors, as access to cloud services that contain your health information may explain everything in a matter of seconds.

1.2 History

The concept of a network of smart devices was discussed as early as 1982, with a modified Coke vending machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold or not. Mark Weiser's 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of the IoT. In 1994, Reza Raji described the concept in IEEE Spectrum as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories" .Between 1993 and 1997, several companies proposed solutions like Microsoft's at Work or Novell's NEST. The field gained momentum when Bill Joy envisioned device-to-device communication as a part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999.

The term "Internet of things" was likely coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999, though he prefers the phrase "Internet for things". At that point, he viewed radio-frequency identification (RFID) as essential to the Internet of things, which would allow computers to manage all individual things.

Defining the Internet of things as "simply the point in time when more 'things or objects' were connected to the Internet than people", Cisco Systems estimated that the IoT was "born" between 2008 and 2009, with the things/people ratio growing from 0.08 in 2003 to 1.84 in 2010.

The key driving force behind the Internet of things is the MOSFET (metal-oxide-semiconductor field-effect transistor, or MOS transistor), which was originally invented by Mohamed M. Atalla and Dawon Kahng at Bell Labs in 1959. The MOSFET is the basic building block of most modern electronics, including computers, smartphones, tablets and Internet services. MOSFET scaling miniaturization at a pace predicted by Dennard scaling and Moore's law has been the driving force behind technological advances in the electronics industry since the late 20th century. MOSFET scaling has been extended into the early 21st century with advances such as reducing power consumption, silicon-on-insulator (SOI) semiconductor device fabrication, and multi-core processor technology, leading up to the Internet of things, which is being driven by MOSFETs scaling down to Nano electronic levels with reducing energy consumption.

1.3 ThingSpeak

Cloud storage is a model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. Channels store all the data that a ThingSpeak application collects. Each channel includes eight fields that can hold any type of data, plus three fields for location data and one for status data. Once we collect data in a channel, we can use ThingSpeak apps to analyze and visualize it. The IOT Based Health Care System for the Elderly is cheapest healthcare device based on the IOT platform for the patients and Physicians. It provides a solution for measurement of body parameters like SpO2, Temperature, and Heartbeat. It also detects the body condition of the patients. The mobile application for the patient and Physicians contain a very simple GUI Interface for reading all the parameters in the mobile or at anywhere in the world by using internet connectivity. In this project, we are using various sensors and modules for performing a different type of functions and the „Thingspeak"hingspeake body condition of the patients. The mobile application for the patient and Physicians contain a very simple GUI Interface for reading all the parameters in the mobile or at anywhere in the world

1.4 Medical and healthcare

The Internet of Medical Things (IoMT), (also called the Internet of health things), is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. The IoMT has been referenced as "Smart Healthcare", as the technology for creating a digitized healthcare system, connecting available medical resources and healthcare services.

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. A 2015 Goldman Sachs report indicated that healthcare IoT devices "can save the United States more than $300 billion in annual healthcare expenditures by increasing revenue and decreasing cost.

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. These sensors create a network of intelligent sensors that are able to collect, process, transfer, and analyze valuable information in different environments, such as connecting in-home monitoring devices to hospital-based systems. Other consumer devices to encourage healthy living, such as connected scales or wearable heart monitors, are also a possibility with the IoT. End-to-end health monitoring IoT platforms are also available for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

Advances in plastic and fabric electronics fabrication methods have enabled ultra-low cost, use and-throw IoMT sensors. These sensors, along with the required RFID electronics, can be fabricated on paper or e-textiles for wirelessly powered disposable sensing devices. Applications have been established for point-of-care medical diagnostics, where portability and low system-complexity is essential.

As of 2018 IoMT was not only being applied in the clinical laboratory industry, but also in the healthcare and health insurance industries. IoMT in the healthcare industry is now permitting doctors, patients, and others, such as guardians of patients, nurses, families, and similar, to be part of a system, where patient records are saved in a database, allowing doctors and the rest of the medical staff to have access to patient information. Moreover, IoT-based systems are patient-centered, which involves being flexible to the patient's medical conditions, IoMT in the insurance industry provides access to better and new types of dynamic information. This includes sensor-based solutions such as biosensors, wearables, connected health devices, and mobile apps to track customer behavior. This can lead to more accurate underwriting and new pricing models.

The application of the IOT in healthcare plays a fundamental role in managing chronic diseases and in disease prevention and control. Remote monitoring is made possible through the connection of powerful wireless solutions. The connectivity enables health practitioners to capture patient's data and applying complex algorithms in health data analysis.

1.5 Technologies for IoT

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

1.5.1 Addressability

The original idea of the Auto-ID Center is based on RFID-tags and distinct identification through the Electronic Product Code. 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 distinct identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion different 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.

1.5.2 Short-range wireless

- Bluetooth mesh networking – Specification providing a mesh networking variant to Bluetooth low energy (BLE) with increased number of nodes and standardized application layer (Models).
- 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.

- Radio-frequency identification (RFID) – Technology using electromagnetic fields to read data stored in tags embedded in other items.
- Wi-Fi – technology for local area networking based on the IEEE 802.11 standard, where devices may communicate through a shared access point or directly between individual devices.
- 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.
- Z-Wave – Wireless communications protocol used primarily for home automation and security applications.

1.5.3 Medium-range wireless

- LTE-Advanced – High-speed communication specification for mobile networks. Provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency.

1.5.4 Long-range wireless

- Low-power wide-area networking (LPWAN) – Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission. Available LPWAN technologies and protocols: Lora Wan, Sigfox, NB-IoT, Weightless, RPMA.
- Very small aperture terminal (VSAT) – Satellite communication technology using small dish antennas for narrowband and broadband data.

1.5.5 Wired

- Ethernet – General purpose networking standard using twisted pair and fiber optic links in conjunction with hubs or switches.
- Power-line communication (PLC) – Communication technology using electrical wiring to carry power and data. Specifications such as Home Plug or G.hn utilize PLC for networking IoT devices.

1.6 IoT architecture

Before revealing the secrets and providing a clear structure of this initiative, it’s important to understand what this concept actually means. In essence, IoT architecture is the system of numerous elements: sensors, protocols, actuators, cloud services, and layers. Given its complexity, there exist 4 stages of IoT architecture. Such a number is chosen to steadily include these various types of components into a sophisticated and unified network.

In addition, Internet of Things architecture layers are distinguished in order to track the consistency of the system. This should also be taken into consideration before the IoT architecture process start. Basically, there are three IoT architecture layers:

1. The client side (IoT Device Layer)
2. Operators on the server side (IoT Getaway Layer)
3. A pathway for connecting clients and operators (IoT Platform Layer)

In fact, addressing the needs of all these layers is crucial on all the stages of IoT architecture. Being the basis of feasibility criterion, this consistency makes the result designed really work. In addition, the fundamental features of sustainable IoT architecture include functionality, scalability, availability, and maintainability. Without addressing these conditions, the result of IoT architecture is a failure. An Overview of the Main Stages in the IoT Architecture Diagram In simple terms, the 4 Stage IoT architecture consists of as shown in figure 2.1:

1. Sensors and actuators
2. Internet getaways and Data Acquisition Systems
3. Edge IT
4. Data center and cloud.

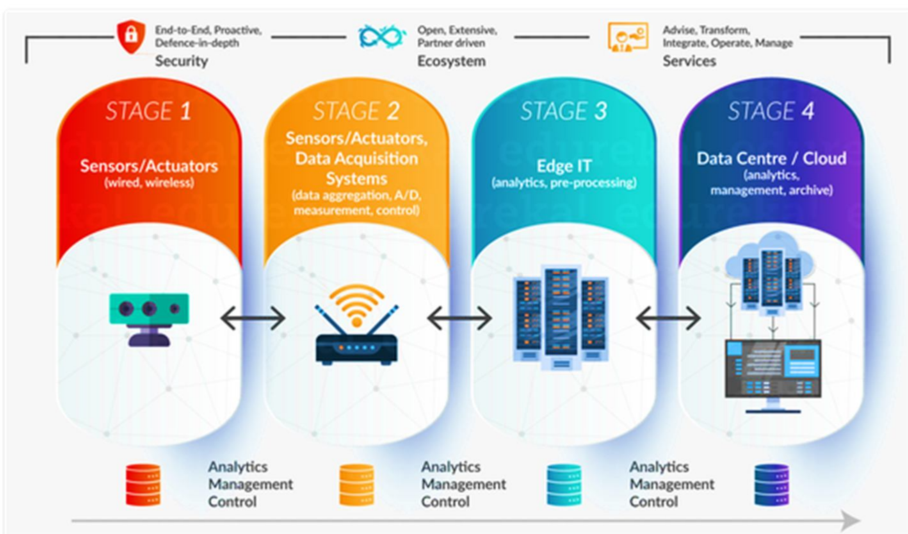


Figure 0-1 The 4 Stage IoT architecture

➢ <u>Stage 1 :</u> Networked things (wireless sensors and actuators)

The outstanding feature about sensors is their ability to convert the information obtained in the outer world into data for analysis. In other words, it's important to start with the inclusion of sensors in the 4 stages of an IoT architecture framework to get information in an appearance that can be actually processed.
For actuators, the process goes even further — these devices are able to intervene the physical reality. For example, they can switch off the light and adjust the temperature in a room. Because of this, sensing and actuating stage covers and adjusts everything needed in the physical world to gain the necessary insights for further analysis.

- Stage 2: Sensor data aggregation systems and analog-to-digital data conversion

Even though this stage of IoT architecture still means working in a close proximity with sensors and actuators, Internet getaways and data acquisition systems (DAS) appear here too. Specifically, the later connect to the sensor network and aggregate output, while Internet getaways work through Wi-Fi, wired LANs and perform further processing.
The vital importance of this stage is to process the enormous amount of information collected on the previous stage and squeeze it to the optimal size for further analysis. Besides, the necessary conversion in terms of timing and structure happens here.
In short, Stage 2 makes data both digitalized and aggregated.

- Stage 3: The appearance of edge IT systems

During this moment among the stages of IoT architecture, the prepared data is transferred to the IT world. In particular, edge IT systems perform enhanced analytics and pre-processing here. For example, it refers to machine learning and visualization technologies. At the same time, some additional processing may happen here, prior to the stage of entering the data center. Likewise, Stage 3 is closely linked to the previous phases in the building of an architecture of IoT. Because of this, the location of edge IT systems is close to the one where sensors and actuators are situated, creating a wiring closet. At the same time, the residing in remote offices is also possible.

- Stage 4: Analysis, management, and storage of data

The main processes on the last stage of IoT architecture happen in data center or cloud. Precisely, it enables in-depth processing, along with a follow-up revision for feedback. Here, the skills of both IT and OT (operational technology) professionals are needed. In other words, the phase already includes the analytical skills of the highest rank, both in digital and human worlds. Therefore, the data from other sources may be included here to ensure an in-depth analysis.

1.6.1 IOT Layer Architectures

Different architectures have been proposed by different researchers. Three- and Five-Layer Architectures. The most basic architecture is a three-layer architecture as shown in Figure 2.2. It was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers.

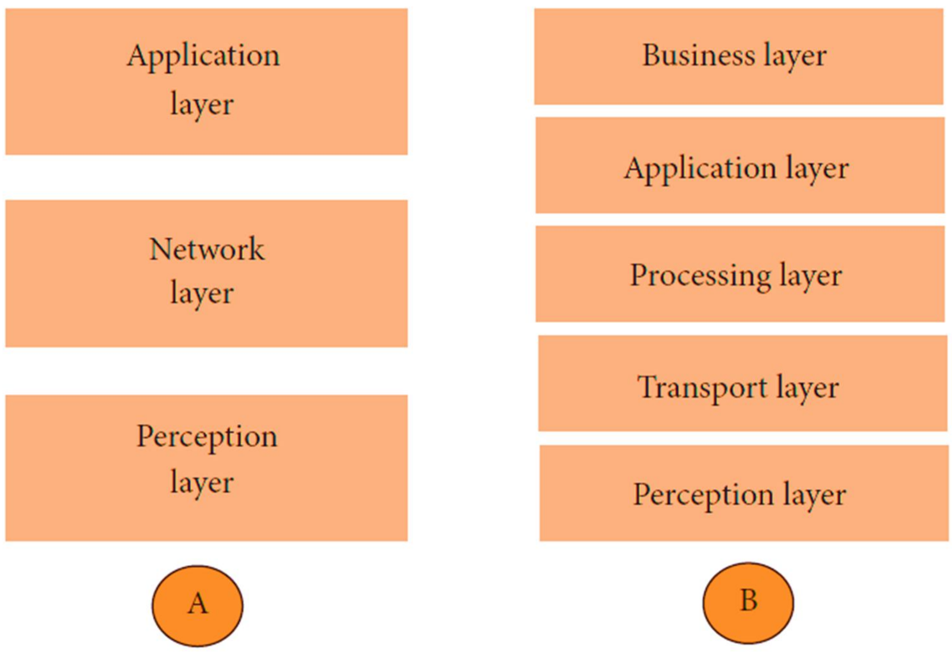


Figure 0-2 Architecture of IoT (A: three layers) (B: five layers)

I. The perception layer

The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.

II. The network layer

is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.

III. The application layer

is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.

The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the five layer architecture, which additionally includes the processing and business layers. The five layers are perception, transport, processing, application, and business layers (see Figure2.2). The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers.

I. The transport layer

Transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.

II. The processing layer

Is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.

III. The business layer

Manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further.

Another architecture proposed by Ning and Wang is inspired by the layers of processing in the human brain. Itis inspired by the intelligence and ability of human beings to think, feel, remember, make decisions, and react to the physical environment. It is constituted of three parts. First is the human brain, which is analogous to the processing and data management unit or the data center. Second is the spinal cord, which is analogous to the distributed network of data processing nodes and smart gateways. Third is the network of nerves, which corresponds to the networking components and sensors.

1.7 The major components of Internet of Things

IoT is a transformation process of connecting our smart devices and objects to network to perform efficiently and access remotely, the major components of Internet of Things as shown in figure2.3.

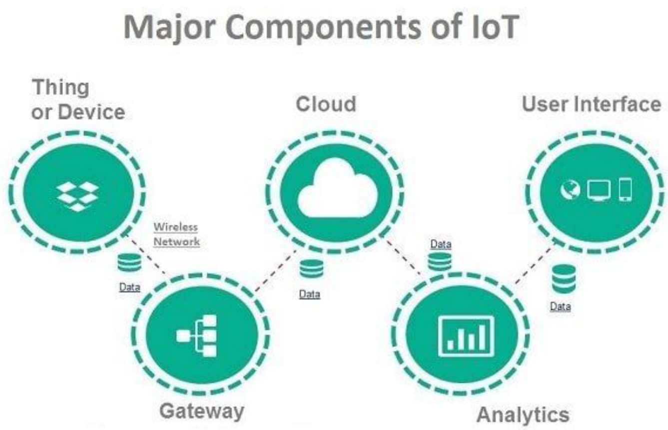


Figure 0-3components of internet of things

1.7.1 Smart devices and sensors – Device connectivity

Devices and sensors are the components of the device connectivity layer. These smart sensors are continuously collecting data from the environment and transmit the information to the next layer. Latest techniques in the semiconductor technology is capable of producing micro smart sensors for various applications.
Common sensors are:

- Temperature sensors and thermostats
- Pressure sensors
- Humidity / Moisture level
- Light intensity detectors
- Moisture sensors
- Proximity detection
- RFID tags

Most of the modern smart devices and sensors can be connected to low power wireless networks like Wi-Fi, ZigBee, Bluetooth, Z-wave, Lora WAN etc.… as sown in figure2.4 Each of these wireless technologies has its own pros and cons in terms of power, data transfer rate and overall efficiency.

Developments in the low power, low cost wireless transmitting devices are promising in the area of IoT due to its long battery life and efficiency. Latest protocols like 6LoWPAN- IPv6 over Low Power Wireless Personal Area Networks have been adapted by many companies to implement energy efficient data transmission for IoT networks. 6LoWPAN uses reduced transmission time (typically short time pulses) and thus saves energy.

Figure 0-4 Wireless Technologies

1.7.2 Gateway

IoT Gateway manages the bidirectional data traffic between different networks and protocols. Another function of gateway is to translate different network protocols and make sure interoperability of the connected devices and sensors as shown in figure2.5.

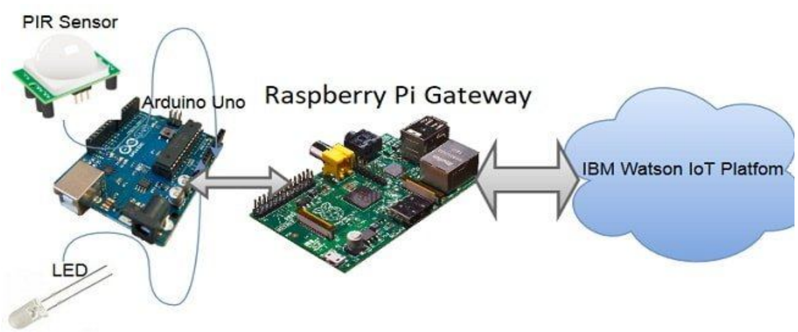


Figure 0-5 Function of Gateway

Gateways can be configured to perform pre-processing of the collected data from thousands of sensors locally before transmitting it to the next stage. In some scenarios, it would be necessary due to compatibility of TCP/IP protocol.

IoT gateway offers certain level of security for the network and transmitted data with higher order encryption techniques. It acts as a middle layer between devices and cloud as shown in figure 6 to protect the system from malicious attacks and unauthorized access.

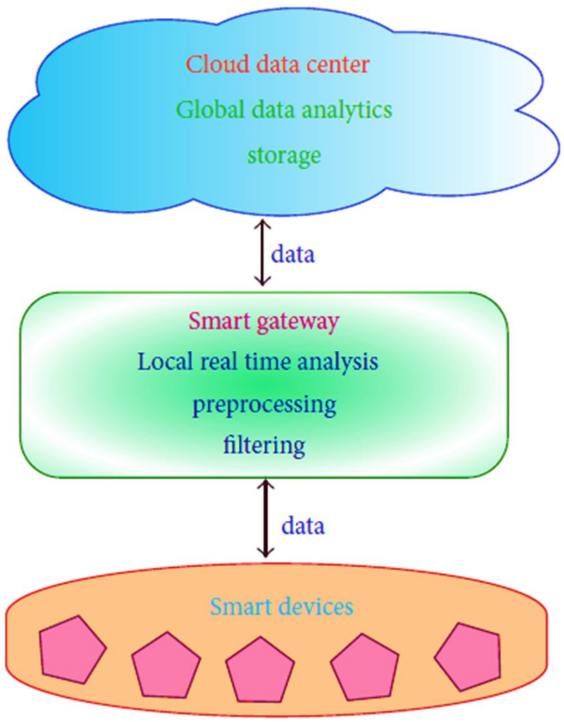


Figure 0-6 Smart gateway

1.7.3 Cloud

Internet of things creates massive data from devices, applications and users which has to be managed in an efficient way. IoT cloud offers tools to collect, process, manage and store huge amount of data in real time (see as shown in figure2.6). Industries and services can easily access these data remotely and make critical decisions when necessary. Basically, IoT cloud is a sophisticated high performance network of servers optimized to perform high speed data processing of billions of devices, traffic management and deliver accurate analytics. Distributed database management systems are one of the most important components of IoT cloud.

Cloud system integrates billions of devices, sensors, gateways, protocols, data storage and provides predictive analytics. Companies use these analytics data for improvement of products and services, preventive measures for certain steps and build their new business model accurately.

1.7.4 Analytics

Analytics is the process of converting analog data from billions of smart devices and sensors into useful insights which can be interpreted and used for detailed analysis. Smart analytics solutions are inevitable for IoT system for management and improvement of the entire system.

One of the major advantages of an efficient IoT system is real time smart analytics which helps engineers to find out irregularities in the collected data and act fast to prevent an undesired scenario. Service providers can prepare for further steps if the information is collected accurately at the right time.

Big enterprises use the massive data collected from IoT devices and utilize the insights for their future business opportunities. Careful analysis will help organizations to predict trends in the market and plan ahead for a successful implementation.

Information is very significant in any business model and predictive analysis ensures success in concerned area of business line.

1.7.5 User interface

User interfaces are the visible, tangible part of the IoT system which can be accessible by users. Designers will have to make sure a well-designed user interface for minimum effort for users and encourage more interactions. Modern technology offers much interactive design to ease complex tasks into simple touch panels controls. Multicolor touch panels have replaced hard switches in our household appliances and the trend is increasing for almost every smart home device.

User interface design has higher significance in today's competitive market, it often determines the user whether to choose a particular device or appliance. Users will be interested to buy new devices or smart gadgets if it is very user friendly and compatible with common wireless standards.

1.8 IOT Protocols

IoT network protocols are used to connect devices over the network. These are the set of communication protocols typically used over the Internet. Using IoT network protocols, end-to-end data communication within the scope of the network is allowed. Following are the various IoT Network protocol as shown in figure 2.7 bellow:

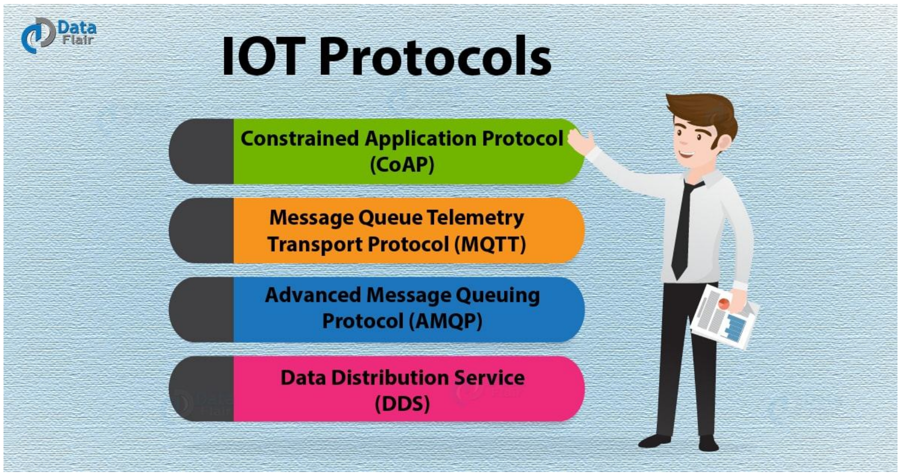


Figure 0-7 IoT Network Protocols

1.8.1 Constrained Application Protocol(CoAP)

CoAP is an internet utility protocol for constrained gadgets. It is designed to enable simple, constrained devices to join IoT through constrained networks having low bandwidth availability. This protocol is primarily used for machine-to-machine (M2M) communication and is particularly designed for IoT systems that are based on HTTP protocols.

CoAP protocol is used mainly in automation, mobiles, and microcontrollers as shown in figure2.8. The protocol sends a request to the application endpoints such as appliances at homes and sends back the response of services and resources in the application.

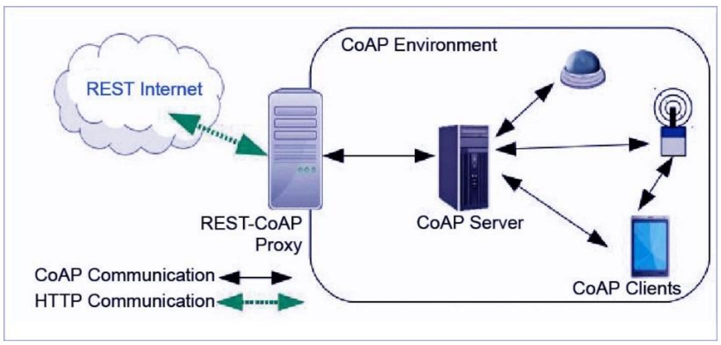


Figure 0-8 CoAP Architecture

1.8.2 Message Queue Telemetry Transport Protocol(MQTT)

MQTT (Message Queue Telemetry Transport) is a messaging protocol developed with the aid of Andy Stanford-Clark of IBM and Arlen Nipper of Arcom in 1999 and is designed for M2M communication. It's normally used for faraway tracking in IoT. Its primary challenge is to gather statistics from many gadgets and delivery of its infrastructure. MQTT connects gadgets and networks with packages and middleware. All the devices hook up with facts concentrator servers like IBM's new message sight appliance. MQTT protocols paintings on top of TCP to offer easy and dependable streams of information.

These IoT protocols include 3 foremost additives: subscriber, publisher, and dealer. The writer generates the information and transmits the facts to subscribers through the dealer. The dealer guarantees safety by means of move-checking the authorization of publishers and subscribers.

1.8.3 Advanced Message Queuing Protocol(AMQP)

This was evolved by John O'Hara at JP Morgan Chase in London. AMQP is a software layer protocol for message-oriented middleware environment. It supports reliable verbal exchange through message transport warranty primitives like at-most-once, at least once and exactly as soon as shipping.
The AMQP – IoT protocols consist of hard and fast components that route and save messages within a broker carrier, with a set of policies for wiring the components together. The AMQP protocol enables patron programs to talk to the dealer and engage with the AMQP model. This version has the following three additives as shown in figure2.9, which might link into processing chains in the server to create the favored capabilities:

- Exchange: Receives messages from publisher primarily based programs and routes them to 'message queues'.
- Message Queue: Stores messages until they may thoroughly process via the eating client software.
- Binding: States the connection between the message queue and the change.

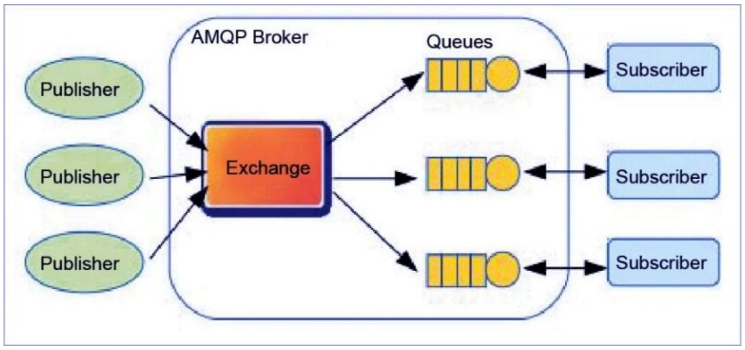


Figure 0-9processing in the server by AMQP

1.8.4 Data Distribution Service (DDS)

It enables a scalable, real-time, reliable, excessive-overall performance and interoperable statistics change via the submit-subscribe technique. DDS makes use of multicasting to convey high-quality QoS to applications.

DDS is deployed in platforms ranging from low-footprint devices to the cloud and supports green bandwidth usage in addition to the agile orchestration of system additives.

The DDS – IoT protocols have fundamental layers as shown in figure2.10, facts centric submit-subscribe (dcps) and statistics-local reconstruction layer (dlrl). Dcps plays the task of handing over the facts to subscribers, and the dlrl layer presents an interface to dcps functionalities, permitting the sharing of distributed data amongst IoT enabled objects.

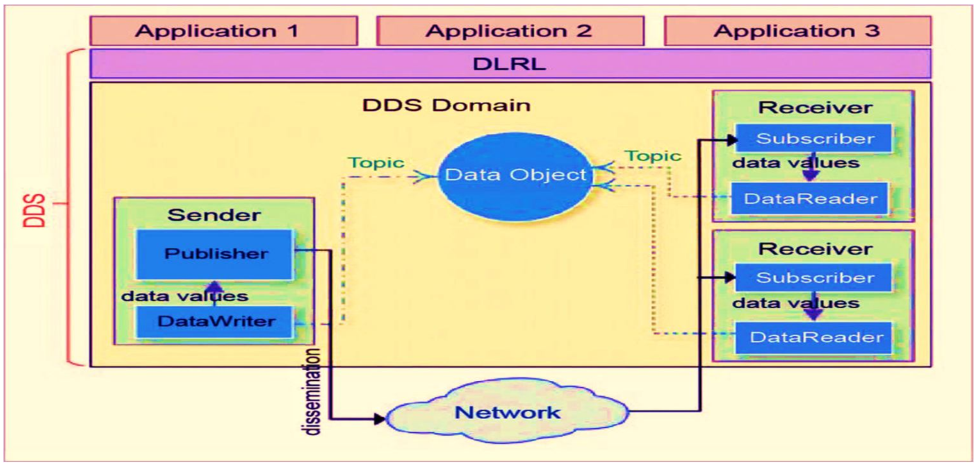


Figure 0-10 DDS layer

1.9 IoT Communication Protocols/ Technology

Several Communication Protocols and Technology used in the internet of Things as shown in figure 2.11. Some of the major IoT technology and protocol (IoT Communication Protocols) are Bluetooth, Wi-Fi, Radio Protocols, LTE-A, and Wi-Fi-Direct. These IoT communication protocols cater to and meet the specific functional requirement of an IoT system.

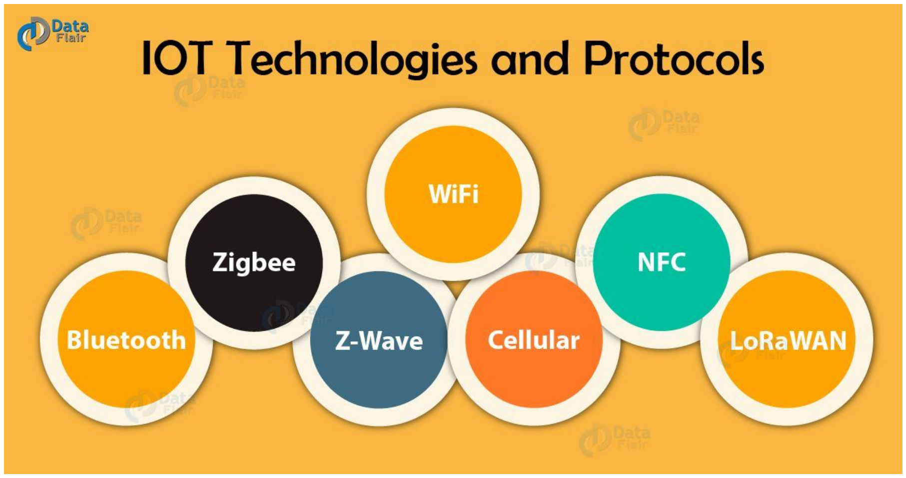
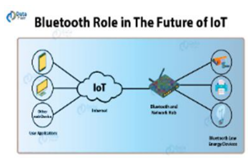


Figure 0-11 IoT Communication Protocols/ Technology

a. Bluetooth



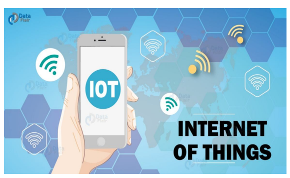
An important short-range IoT communications Protocols / Technology. Bluetooth, which has become very important in computing and many consumer product markets. It is expected to be key for wearable products in particular, again connecting to the IoT albeit probably via smartphone in many cases. The new Bluetooth Low-Energy (BLE) – or Bluetooth Smart, as it is now branded – is a significant protocol for IoT applications. Importantly, while it offers a similar range to Bluetooth it has been designed to offer significantly reduced power consumption.

b. ZigBee

ZigBee is similar to Bluetooth and is majorly used in industrial settings. It has some significant advantages in complex systems offering low-power operation, high security, robustness and high and is well positioned to take advantage of wireless control and sensor networks in IoT applications. The latest version of ZigBee is the recently launched 3.0, which is essentially the unification of the various ZigBee wireless standards into a single standard.

c. Z-Wave 

Z-Wave is a low-power RF communications IoT technology that primarily design for home automation for products such as lamp controllers and sensors among many other devices.
A Z-Wave uses a simpler protocol than some others, which can enable faster and simpler development, but the only maker of chips is Sigma Designs compared to multiple sources for other wireless technologies such as ZigBee and others.

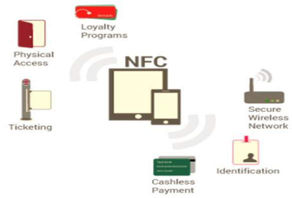
d. Wi-Fi 

Wi-Fi connectivity is one of the most popular IoT communication protocol, often an obvious choice for many developers, especially given the availability of Wi-Fi within the home environment within LANs. There is a wide existing infrastructure as well as offering fast data transfer and the ability to handle high quantities of data. Currently, the most common Wi-Fi standard used in homes and many businesses is 802.11n, which offers range of hundreds of megabit per second, which is fine for file transfers but may be too power-consuming for many IoT applications.

e. Cellular 

Any IoT application that requires operation over longer distances can take advantage of GSM/3G/4G cellular communication capabilities. While cellular is clearly capable of sending high quantities of data, especially for 4G, the cost and also power consumption will be too high for many applications. But it can be ideal for sensor-based low-bandwidth-data projects that will send very low amounts of data over the Internet.

f. NFC



NFC (Near Field Communication) is an IoT technology. It enables simple and safe communications between electronic devices, and specifically for smartphones, allowing consumers to perform transactions in which one does not have to be physically present. It helps the user to access digital content and connect electronic devices. Essentially it extends the capability of contactless card technology and enables devices to share information at a distance that is less than 4cm.

g. LoRaWAN

LoRaWAN is one of popular IoT Technology, targets wide-area network (WAN) applications. The LoRaWAN design to provide low-power WANs with features specifically needed to support low-cost mobile secure communication in IoT, smart city, and industrial applications. Specifically meets requirements for low-power consumption and supports large networks with millions and millions of devices, data rates range from 0.3 kbps to 50 kbps.

1.10 IoT Challenges

Despite the amount of work and standards on IoT, developing a successful IoT application is still not an easy task due to multiple challenges. These challenges include: mobility, reliability, scalability, management, availability, interoperability, cost and energy harvesting. In the following, we briefly describe each of these challenges.

1.10.1 Mobility

IoT devices are supposed to move freely in the environment and, hence, change their IP addresses and connect to networks relative to their locations. Thus, routing protocols, such as RPL have to reconstruct the DODAG each time a node goes off the network or joins the network which adds a lot of overhead. In addition, mobility might result in a change of service provider which can add another layer of complexity due to service interruption and changing gateway.

1.10.2 Reliability

For emergency response applications, it is very critical to keep the system perfectly working and delivering all of its specifications correctly. Hence, in IoT applications, the system should be highly reliable and fast in collecting data, communicating them and making decisions. Wrong decisions can lead to disastrous scenarios.

1.10.3 Scalability

As millions and trillions of devices get connected in a single IoT application, scalability becomes a challenge that needs to be solved. Managing device distribution and functionalities is not an easy task. In addition, IoT applications should be tolerant of new services and devices constantly joining the network and, therefore, must be designed to enable extensible services and operations.

1.10.4 Management

Even though several protocols to manage devices remotely were discussed, these protocols can't be applied to all IoT applications, and hence, management is still a big challenge. Providers need to manage faults, configuration, accounting, performance and security (FCAPS) of their interconnected devices.

1.10.5 Availability

Availability of IoT platforms should guarantee both software and hardware availability for system users and service subscribers. Software availability means that the services are provided to the users, even when failures happen. Hardware availability means that the existing devices are easy to access and are compatible with various protocols. In addition, these protocols should be compact enough to be embedded within the constrained IoT devices.

1.10.6 Interoperability

Interoperability means that heterogeneous devices and protocols need to be able to inter-work with each other. This is challenging due to the large number of different platforms used in IoT systems. Interoperability should be handled by both application developers and device manufacturers to deliver the services regardless of the platform or hardware specification used by the customer.

1.10.7 Cost and complexity

Despite the relatively cheap prices of IoT devices such as sensors and smart transducers, it still costs too much to build an IoT application. Such complex integration of different protocols and standards makes IoT applications not available for general public usage. Reducing the cost and complexity is a massive challenge that needs to be solved.

1.10.8 Power Harvesting

Power harvesting is still a challenge in IoT devices due to a lack of harvesting technologies for such small, resource constrained devices. Power is a critical issue in IoT as these devices need to last for years without battery changing and might be embedded in a body or environment which makes it difficult to change. Hence, collecting energy from motion or any other energy source and transforming it into stored energy seems to be a critical solution for such devices. However, such transformers and collection devices are still too weak to be applied to small devices due to their space and power needs.

CHAPTER 2

Smart Healthcare

2.1 INTRODUCTION

Traditional healthcare is unable to accommodate everyone's needs due to the tremendous increase in population. Despite having excellent infrastructure, and cutting-edge technologies, medical services are not approachable or affordable to everyone. One of the goals of smart healthcare is to help users by educating them about their medical status and keeping them health-aware. Smart healthcare empowers users to self-manage some emergency situations. It provides an emphasis on improving the quality and experience of the user. Smart healthcare helps in utilizing available resources to their maximum potential. It aids remote monitoring of patients and helps in reducing the cost of the treatment for the user. It also helps medical practitioners to extend their services without any geographical barriers. With an increasing trend towards smart cities, an effective smart healthcare system assures a healthy living for it citizens.

Connected health in general refers to any digital healthcare solution that can operate remotely and is a collective term for subsets such as telemedicine and mobile-health, but with an additional component of continuous monitoring of health, emergency detection and alerting suitable individuals automatically. Connected health mainly focuses on the mission to improve the quality and efficiency of healthcare by enabling self-care and complementing it with remote-care. It has its origin in the era of telemedicine, where the users are educated about their health and are given feedback whenever required. While smart healthcare refers to solutions which can operate completely autonomously, connected healthcare offers solutions for the users to receive feedback from clinicians. The most important classification, which redefines the economy of the smart healthcare, is the end user market. Depending upon whether the healthcare network is to be implemented for individuals or hospitals, the cost, power, and architecture varies widely.

Figure 2.1 shows the broad classification of the smart healthcare market based on the services, medical devices, technologies used, applications, system management and end users. Connectivity technologies used play a vital role in expanding the applications for which the healthcare system is designed. Efficient integration of small devices through wireless technologies can help in implementing remote health monitoring through the Internet of Things (IoT). If a personalized monitoring device such as a wrist band is used, a Bluetooth module, 6LowPAN or RFID can be used to connect the device to the internet. But in a hospital scenario where a healthcare network is maintained, Wi-Fi and ground cables are required to maintain constant internet connectivity and support heavy data traffic. The medical devices used to implement the smart healthcare can be classified into on-body sensors and stationary medical devices. On-body sensors are usually bio-sensors which are attached to the human body for physiological monitoring. These sensors can be further classified into in-vitro and in-vivo sensors.

In-vitro sensors are attached externally to the human body which helps in reducing the involvement of lab or hospital facilities in healthcare. In-vivo sensors are implantable devices which are placed inside the body after fulfilling the regulations and standards on sterilization.

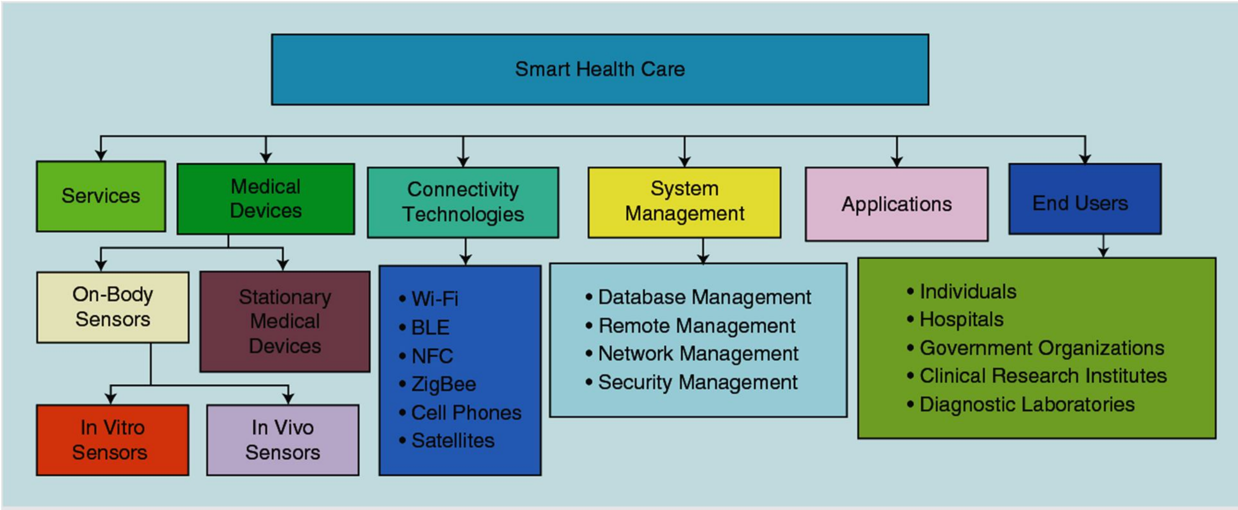


Figure 2-1Classification of Smart Health

2.2 ARCHITECTURES: REQUIREMENTS, COMPONENTS AND CHARACTERISTICS

Requirements of smart healthcare can be broadly classified into functional requirements and non-functional requirements, as shown in Figure 2.2. Functional requirements address specific requirements of a smart healthcare architecture. For example, if a temperature monitoring system is deployed, based on the application it is used for, the range of operation of the thermistor/thermometer, data collection mechanism, and frequency of operation might vary. Hence functional requirements are specific to each component used in that healthcare system based on their application.

On the other hand, non-functional requirements are not very specific. Nonfunctional requirements refer to attributes based on which the quality of the healthcare system can be determined. On a broader perspective, non-functional requirements of smart healthcare can be classified into performance requirements and ethical requirements. Due to the large number of verticals involved in designing a complete smart healthcare system, performance requirements can be further classified into software and hardware requirements. Essential requirements for an efficient smart healthcare system are low power, small form factor, system reliability, quality of service, enriched user experience, higher efficiency, ability to interoperate across different platforms, ease of deployment, popularity of the smart healthcare system to offer continuous support, scalability of the system to upgrade to newer versions and technologies, and ample connectivity since the very prime motive of designing a smart healthcare is to ensure medical service promptly. In advanced applications, along with these requirements, the system also needs to have ambient intelligence to improve the quality of service.

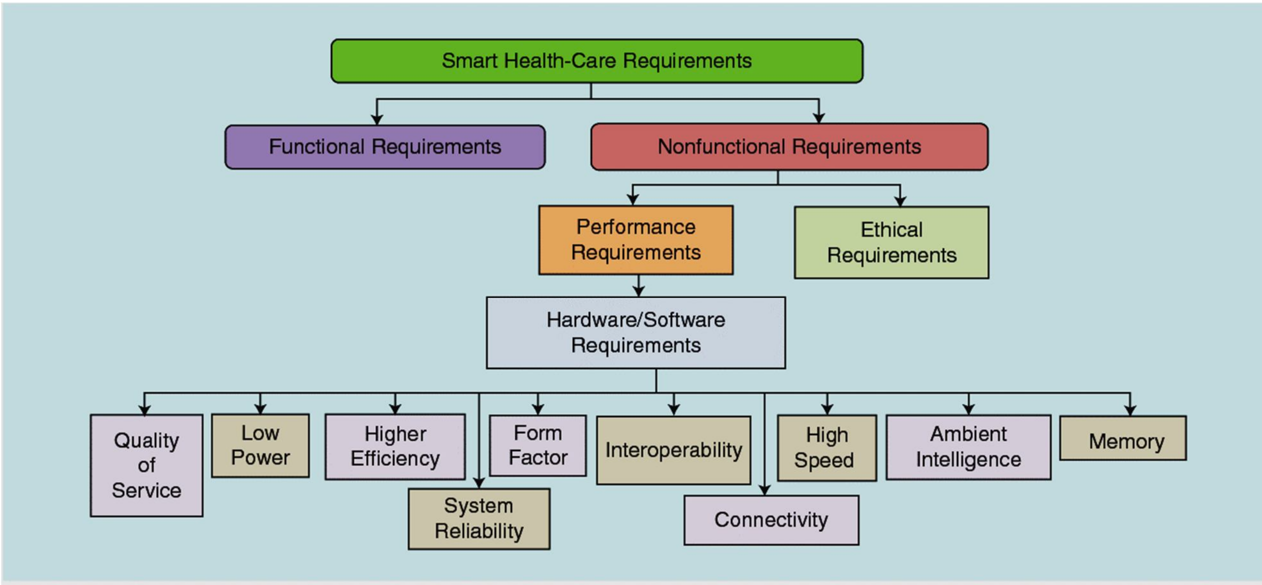


Figure 2-2Requirements of smart healthcare

Perspectives of smart heath care widely vary amongst researchers and industries, based on the chosen goal to be achieved. Components of smart healthcare system can be classified based on the sensors or actuators, computing devices, data storage elements and networking components. A sensor is an analytical device which combines with a biological element that creates a recognition of events. Sensors or actuators vary based on the monitoring systems. Temperature sensors, ECG, blood pressure, blood glucose, EMG, heart rate, SpO_2, gyroscope, motion sensors, and accelerometers, are the common sensors used in smart healthcare. Computing devices used in the present era range from smart phones, tablets, and PDAs to complex and advanced devices such as super computers and servers. Memories play a very important role in smart healthcare since storing the information is the most important function of these systems. Data storage components in the smart heath care network cover a broader spectrum starting from embedded memory on the sensing devices to big servers that are used to handle big data analytics. Networking components vary from link sensors to routers and base stations. Based on the severity of the problem addressed, the sophistication of the components varies. Wireless technologies are the backbone of the smart healthcare network. Different wireless technologies such as Wi-Fi, Bluetooth, 6LoWPAN, RFID etc., as shown in Figure2.3, play a vital role in exchanging the information among different physical elements that are configured to form the healthcare network.

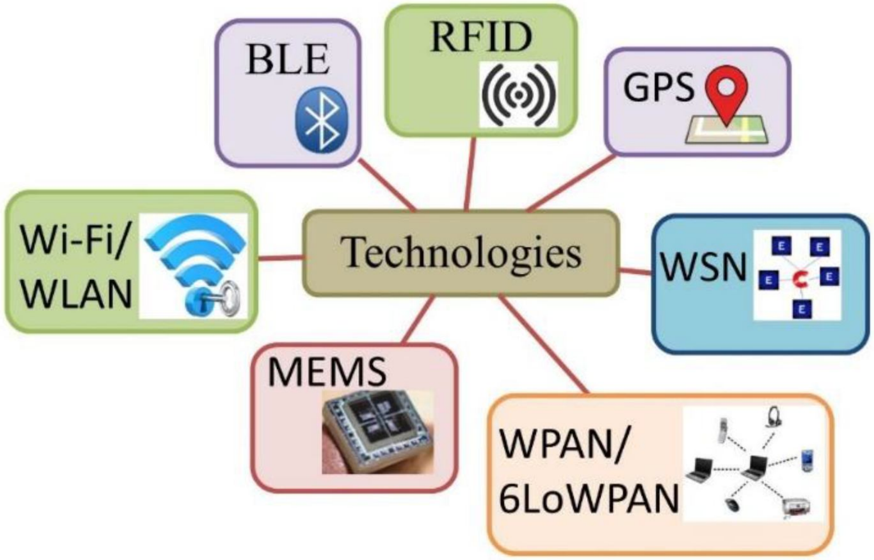


Figure 2-3Different Technologies used Deploy Smart Healthcare

The most important characteristics required for smart healthcare system are shown in Figure2.4. Characteristics of smart healthcare can be broadly classified based on three categories: App-oriented, Things-oriented and Semantics-oriented. App-oriented architectures need to ensure reliable transmission between the applications in smart phones and the sensors, establish a personalized network between the sensors and the user's computing device and secure the information. Things-oriented architectures need to be adaptive based on the application, real time monitoring, on-time delivery, higher sensitivity, maintain higher efficiency at lower power dissipation, and embark on intelligent processing. Semantic-oriented systems need to be able to develop behavioral patterns based on the previously acquired information, process natural language processing techniques to enrich user experience and have ubiquitous computing capabilities.

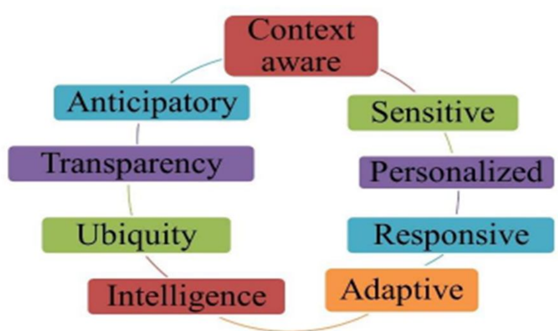


Figure 2-4Characteristics of Smart Healthcare

2.3 NETWORKS: CONFIGURATION, ORGANIZATION AND FRAMEWORK

Wireless sensor networks (WSNs) were the initial research effort for the IoT. Using WSNs in different applications led to efficient architectures for healthcare applications There are many dimensions to the architectures and platforms used to deploy smart healthcare. Research in healthcare networks, can be categorized into three major research dimensions: Configuration, Organization and Framework. Healthcare configuration refers to the assembly of different physical elements in appropriate applications which can be used to address key issues. By placing the right sensors/actuators in environments, heterogeneous computing grids can be configured to use such configurations in seamless healthcare computing environments. On the other hand, the organization groups the specifications of the healthcare physical elements along with the hierarchy of the design. Smart healthcare architectures need to be interoperable across different technologies. For example, the sensors used in the body would communicate amongst each other through a personal area network or body area network. This information would be transferred to a smart phone through a Bluetooth or Wi-Fi technology and further will be processed across the network through IPV6.

Thus, organization helps in discussing the working principles and techniques involved in the network architectures. Research on exploring big data techniques in healthcare services, using cloud assistive architectures and integrating multiple technologies to assure quality of service has been constantly gaining more attention from researchers worldwide.

A framework for smart healthcare architecture includes the libraries and environments in which the healthcare architecture is used. Healthcare platforms can be widely classified into network platforms, computing platforms and service platforms. Network platforms refer to the networking libraries used to interconnect different architectures. Computing platforms can vary widely based on the technologies used. Due to diversity in the application environments of smart healthcare networks, the frameworks for computing platforms are usually an intersection of wider concepts such as database management, optimization, human-machine interface, machine learning algorithms and so on. Service platform refers to the support layer which acts as

a middleware between the technologies and the users. This support layer can either be agents or call center representatives or, in advanced applications, robots or algorithms with cognitive and behavioral perspective.

A framework for processing health information using the IoT has been proposed in. Figure1.5 shows the various attributes which are to be considered before modeling the frameworks, organizations and platforms, Specifically, for smart healthcare.

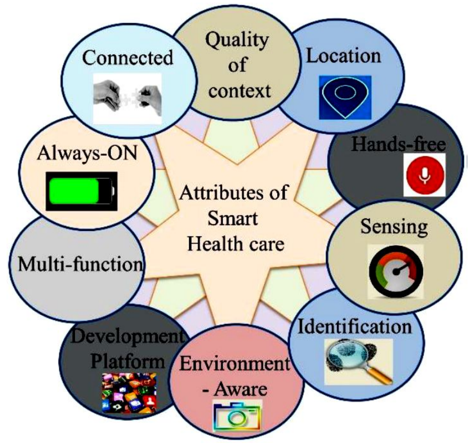


Figure 2-5Attributes of Smart Healthcare

2.4 SERVICES & APPLICATIONS

From the healthcare perspective, services can vary from push-notifications on the healthcare mobile App to cross-connectivity protocols required for connected devices, as shown in Figure 2.6. Modifications in already existing healthcare systems might help in integrating these systems in smart healthcare. In addition to being secure and fast, these services should also be easily accessible to the patient. Context-aware services use the current location of the user to provide additional services. This could be used in mobile or wearable sensors. For example, based on the information received from the sensor, the walking trail can be tracked to analyze the number of miles covered. In some cases, where the user needs additional help to call an ambulance or a paramedic, the required assistance can be provided based on the geographical data obtained from the user. Embedded context prediction (ECP) provides a framework with appropriate mechanisms which can be used to build context aware system. Context aware systems can operate in ubiquitous environments.

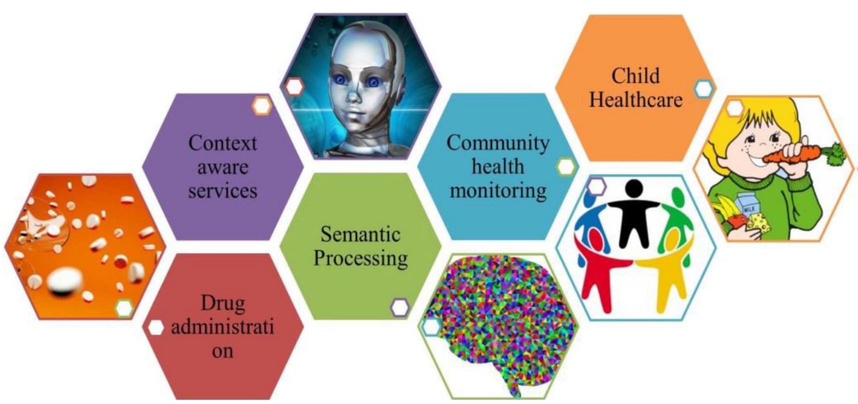


Figure 2-6 Service Available Through Smart healthcare

Semantic processing is a behavior of the human brain to understand colors, patterns, objects etc. based on the context that helps in deeper processing. For example, when a familiar word is heard, the brain processes its meaning based on semantic memory which involves common knowledge. In smart healthcare, the use of semantics and ontologies has led to a service called semantic medical access (SMA). This helps in processing ubiquitous data available in the medical cloud and providing emergency services by integrating these services.

Wireless Body Area Networks (WBANs) are the basic components of community healthcare monitoring. Community healthcare monitoring helps in creating a network around the local community. Multiple WBAN constitute a community healthcare network and multiple community healthcare networks constitute a cooperative network. A community healthcare network might include schools, residential areas, hospitals etc. which helps in providing energy efficient monitoring in rural area.

Figure 2.7 demonstrates the applications of smart healthcare, which start from fitness monitoring on one end of the spectrum to vital sign monitoring in hospitals. Based on the application, the quality of health care systems is improved with additional machine learning algorithms and artificial intelligence. The wide range of applications can be grouped into inter-body sensing, intra-body sensing and environmental management.

Figure 2-7applications of smart healthcare

Intra body sensing applications refer to those which help in monitoring multiple vital signs. For example, in fitness tracking through a smart watch, along with parameters such as number of calories burned, steps taken, active hours etc., it is also important to track the ph sensitivity of the sweat, oxygen intake of the body, heart rate monitoring, etc. In order to meet the competitive smart healthcare market, companies are trying to incorporate as many sensors as possible to offer ubiquitous sensing. Heart rate monitoring and remote ECG monitoring through wearables, have offered cost effective solutions in smart healthcare. In smart watches, it is also necessary to keep a track of the previous monitoring analysis. Algorithms that incorporate cognitive and behavioral processes are being deployed in these sensors to discover patterns. Such patterns from various users can help researchers and industries to develop models that can be used in treating a condition better. Examples for this group of applications can be again found in fitness monitoring through smart watches where, with emergence of virtual reality, these applications are used to set a walking or hiking trail. Along with providing features such as localization and tracking, they help in tracking the fitness of the user. Creating sensitive and responsive digital environments has made the smart healthcare domain a multi and inter-disciplinary research area. Mobile applications that are associated with wearables learn from the users, reason about their intensions of using the device and help them plan in achieving their fitness goals. Environmental management applications help in establishing communication between the hospital and the patient. Monitoring the first responder's health status in an endemic or epidemic outbreak, getting ambulance assistance in case of emergency, developing evacuation schemes for disaster management in hospitals, maintaining active databases to ensure correct delivery of organs/blood to the users in need, accurate billing of surgical procedures through RFID tags are some of the significant applications in environmental management.

2.5 THE IoT IN SMART HEALTHCARE

The IoT is a combination of ubiquitous communication, connectivity and computing along with ambient intelligence. It refers to a cyber physical paradigm, where all the real-world components can stay connected. The IoT gives users the ability to plan every day and it integrates real physical world elements such as electronic devices, smart phones and tablets which can communicate both physically and wirelessly. The IoT helps in managing virtually any number of devices. It aims in extending the benefits of internet such as remote access, data sharing and connectivity to various other application domains such as healthcare, transportation, parking activities, agriculture, surveillance, etc. With enormous benefits and attributes such as identification, location, sensing and connectivity, attached to the IoT, it is the integral component of smart healthcare, as shown in Figure2.8.

In implementing a smart healthcare system, the IoT can be broadly implemented in a wide range starting from calibrating medical equipment to personalized monitoring system. The IoT plays a significant role in healthcare applications, from managing chronic diseases at one end of the spectrum to monitoring day-to-day physical activities which could help in maintaining one's fitness goals. The IoT can be used to monitor the process of production and tracing of medical equipment delivery. IoT-based architectures can be used to collect medical information from the user.

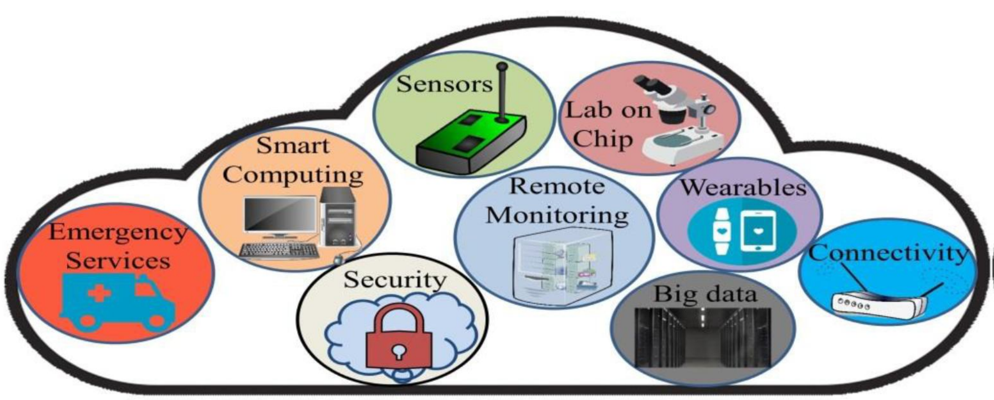


Figure 2-8The IOT in Smart Healthcare

The IoT functions as a bridge between the doctor and the patient by providing remote access, which can help the doctor continuously monitor the patient and give remote consultation. Combining sensors, actuators, microcontrollers, processors, along with cloud computing, the IoT helps in getting accurate results and makes healthcare attainable to everyone.

2.6 BIG DATA AND ARTIFICIAL INTELLIGENCE IN SMART HEALTHCARE

In healthcare data, three main challenges need to be addressed: quantity, variety and velocity. There are enormous applications and services which require the storage of patient information and each time a service is used or the patient visits the healthcare facility, the information needs to be updated. Currently, with the increase in smart sensors, social networks, and web services, mobile devices are estimated to be generating more than 2.5 quintillion bytes per day Hence traditional databases and data storage mechanisms might not prove efficient in handling such large amounts of data. To address these challenges, a mix of non-relational and relational databases need to be used to store clinical data that are present in electronic format. Data collected by the smart healthcare systems need to be consistent. A high-level of semi-structured databases enabling multitude of queries are required. Cloud computing technology makes
on-demand services scalable to large amounts of users. It has many features such as virtualization, scalability, pay-per-use and multitenancy. Cloud assistive treatment can help medical professionals offer services to users irrespective of the geographical location. Combining big data techniques with cloud computing, helps in achieving better analysis.
Assisted living, especially for the elderly, has been a primary research area involving Artificial Intelligence in smart healthcare. With intelligent systems that have ambient intelligence, the system increases the quality of life and ensures safety of elderly people. Along with the benefits it offers for the individual, it also helps in providing higher effectiveness of limited resources and improves the living standards.

2.7 SMART HEALTHCARE: INDUSTRY TRENDS AND PRODUCTS

The scope of smart healthcare products has expanded its horizons and has been predicted by Frost & Sullivan to be a 348.5 Billion USD market by 2025. With a lot of ongoing research and a scope to address new issues, entrepreneurs and well-established industries are competing at their best with remarkable creativity. Smart syringes, smart pills and smart RFID cabinets are gaining everyone's interest in the smart healthcare domain. RFID has been widely used for infection safety, radiology and control of infections such as TB. Electronic health records are the most significant products of smart healthcare which has given an altogether new perspective for addressing big data issues. These products fall across different verticals such as health data and storage, monitoring and treatment and inventory management.

In the present digital health revolution, Intel is leading the list with their Digital Health Foundation. The company is constantly coming up with innovative technologies for data analytics, assistive technology and improving the home environment for the elderly population. IBM's Watson, an artificially intelligent computer system, can look at the content of the patient's health record and considers the medical information faster, to provide better health care models. IBM has partnered with Apple, Johnson & Johnson and Medtronic to continue their digital health research in a large scale. Google has a dedicated life sciences division to develop and research new technologies in digital health. Qualcomm Life helps in capturing the medical device data and integrates it to the nearby database partner through a wireless medical device and secures the information. This platform offered by Qualcomm provides high range of system interoperability and security. Microsoft's "Connected Health Platform", helps in offering digital health services through desktop frameworks. Microsoft Lync is used by Doctor's to offer medical services to patients in rural areas. Samsung has a $50 million investment in digital health through their Digital Health Initiative which is a collaboration of smart sensors, algorithms and data processing techniques through open source hardware and software platforms. Apple has an open source framework, Research Kit, which aids researchers to develop apps that can facilitate medical research

Figure 2-9Features of smart watch

On the retail front, Amazon offers a unified healthcare platform where the users can access healthcare information, availability of latest products, health insurance and "on-demand" services. Wearables, especially in the form of smart watches or bands, have been revolutionizing the market. Notable products include Fitbit, moov, Proteus, Pebble Time, Withings AliveCor Health monitor, Beddit and so on. Significant amongst the healthcare products are smart watches. Smart watches are becoming more ubiquitous, as shown in Figure2.9. The projected annualized rate is expected to reach 70 million units at a growth of 18% annualized rate by 2021. Apple is expected to have a hold of the larger share in the market, however, Android wear devices are continuously emerging. Apple's I Watch offers a package of built-in GPS, and heart rate sensors with a fast dual-core processor.

2.8 CHALLENGES, VULNERABILTIES AND OPPORTUNITIES

Though smart healthcare helps in providing better healthcare to everyone in the world, it also becomes more vulnerable to threats. Due to the dynamic nature and smaller form factors, the security requirements in smart healthcare systems vary from the traditional security techniques. Figure 2.10 shows the key security requirements or challenges in maintaining a secured smart healthcare system. Healthcare networks contain personal information which can be easily tampered with. In order to reduce the cost of the design, the processors used in smart healthcare systems are low speed processors and have low on-device memory, which cannot accommodate additional security mechanisms.

Figure 2-10 Security requirements of smart hospital

Health care devices are mobile, which leads the user to connect to different networks such as home networks, office networks, and public networks. This increases the chance of attacks on the device. Due to the increase in the number of IoT devices in the healthcare network, it is a very challenging task for developers to provide dynamic security updates or a sound solution for multi-protocol information. Smart healthcare systems are vulnerable for security attacks at various levels of the system. By maintaining data freshness in the healthcare network, the passwords and keys need to be updated frequently. Attacks targeting data transmitted in the network can include interruption of the service availability, modification of original data, forging the messages and replaying the messages to disrupt the flow of data and create a false impression. Attacks can also tamper the hardware i.e. the interconnected physical devices or the software, namely the operating systems and applications.

A specific example of tampering with a personal medical device, an insulin delivery system, is now discussed. In this system, a personal digital device (such as a cell phone), an insulin pump, a continuous glucose sensor, and a remote-control device are all connected through a wireless Personal Area Network (PAN), as illustrated in Figure2.11(a). Possible security attacks on this system can be active, passive, or both, as depicted in Figure2.11(b). An example of a passive attack is to intercept the communications in the PAN between the remote control to the insulin pump with the objective of reverse engineering the communication protocol. On the other hand, an active attack is to use this reverse-engineered protocol to attach an impersonating remote-control device to the insulin pump. This allows the attacker full control of the insulin pump with potentially lethal consequences for the patient. Two different defenses for these attacks are rolling code protocols, and body-coupled communication. The rolling code encoder, as presented in Figure2.11(c), generates rolling codes which avoids the system's dependency on a fixed device PIN every time. Since the rolling sequence is random (but known to the receiver and synchronized with it), a security breach is nearly impossible. This approach is equivalent to the use of one-time pad cryptography, universally considered as the strongest possible cryptographic protocol. As illustrated in Figure2.11(d), the data are decrypted in the insulin pump using the shared key. The decrypted sequence number is then compared to the receiver's counter. If the difference between the two is within a certain range, to allow for small timing differences, then the insulin system validates the received control code, synchronizes the sequence counter, and performs its task. On the other hand, a security model based on body-coupled communication as defense reduces the signal strength, which makes passive attacks very difficult unless the attacker is in physical contact with the patient, which is normally not possible.

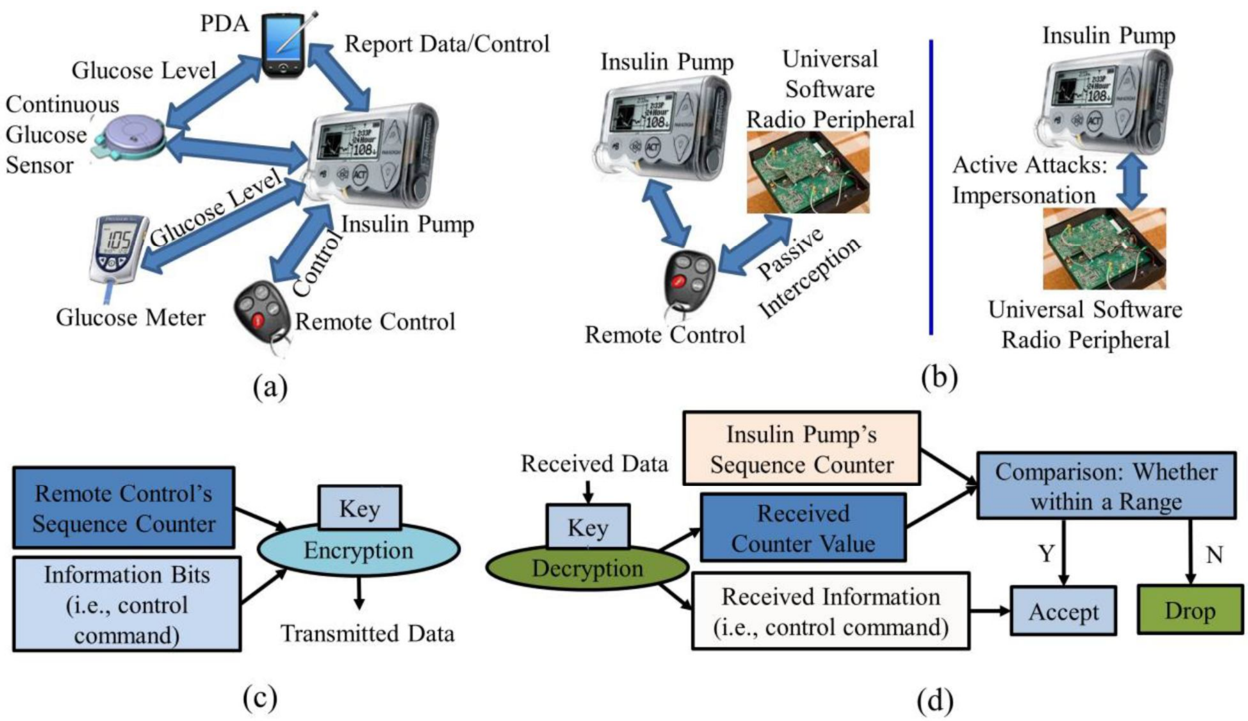


Figure 2-11A specific example of security attack on a medical device. (a) an insulin delivery system, (b) passive and active security attacks on the insulin delivery system, (c) the rolling-code encoder in the remote control, and (d) the rolling-code decoder in the insulin pump.

Confidentiality is a key security requirement in smart healthcare. Data, which includes private information about the user, needs to be shared only with authorized users. Only authorized nodes and users should have access to the services or resources. At least two-level authentication needs to be implemented to ensure the identity of the peer.

Integrity needs to be maintained in the healthcare network, assuring the users that the data which are transmitted and received are not altered or compromised. If the interconnected device is compromised, the security system should ensure that there is no attack on the information or device in the healthcare network. The interconnected devices need to be self-healing to some degree, which ensures that if a device fails, it has minimum impact on the healthcare network.

2.9 NANO-SMART HEALTHCARE

Consumer electronics empowered with the latest wireless technologies and seamless architectures help in improving the quality of life through smart healthcare. One such example is the pill camera. Endoscopy or colonoscopy are procedures which are generally used by doctors for monitoring the internal organs for any gastrointestinal infections. It is generally prescribed for patients with colon cancer, irritable bowel syndrome, stomach ulcers, tumors, piles and so on. These procedures are not just expensive; they also make the patient uncomfortable as a long tube is put inside a person. A pill camera makes the job easier for both the patient and the doctor. It is as simple as swallowing a pill and getting high resolution pictures of the internal organs. Figure2.12 shows the overall architecture of the pill camera. The pill camera is a light device with image sensors to capture the footage, and an RF transmitter and antenna to wirelessly transmit this acquired data in real time to the data recorder which is a waist belt or a shoulder strap.

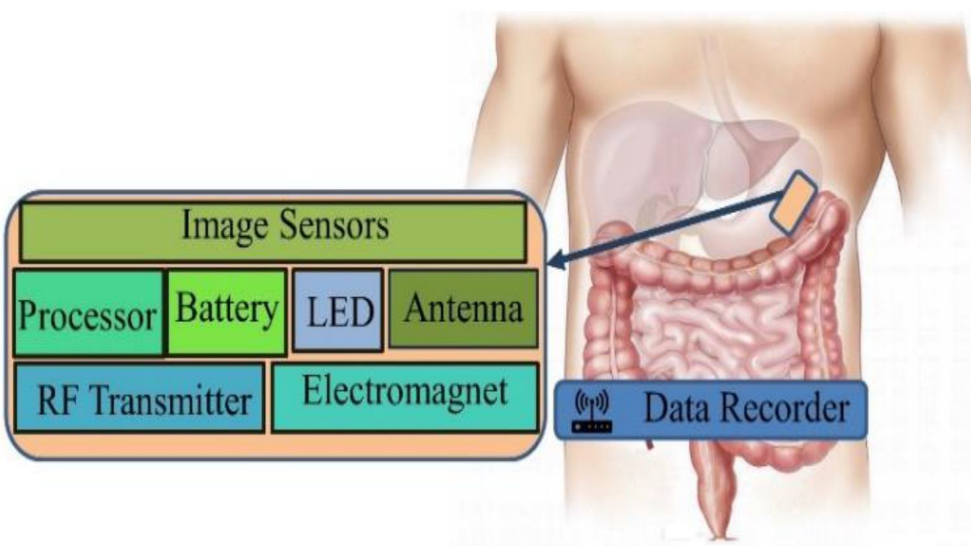


Figure 2-12pill camera

The magnetic strips help in activating the camera as and when required. The LEDs are timed in such a way that when the camera reaches the appropriate position, they are turned ON to monitor the exact location and obtain better images. This camera is either powered by a small battery or through induction charging with the help of the data recorder strap. As there is no on board memory in the pill camera, it makes it very light to navigate through the intestine. Though pill cameras have been around for almost a decade, the latest advancements can produce over 800,000 images in 8 hours, with the camera turning at around 60 degrees every 12 seconds.

Chapter 3

Hardware of Healthcare System

3.1 Introduction:

All the hardware units of the system were implemented, tested and it was ensured that they were in a good working condition.

Then, each and every unit ware interfaced and implemented individually with the microcontroller board and drove with the software according to the necessity of the application.

The testing of application was not done at once after it was completed. rather each unit of the application was tested individually. the second unit was not tested unit the first unit gave the expected result and until it was not working according to the necessity of the application. after all of the units were working correctly, the units were kept together and then the whole system was developed and tested .it was easy to figure out the bugs and the problem of the system as the behavior of each unit was known while testing it.

It would be impossible to figure out the problems and the bugs in the system if the system was developed and tested after it was completed. after the hardware units were tested ,the communication of the Ethernet module was tested.

3.2 Design overview

In this part of chapter ,we will show initial investigation of the general components which will be used to build the project hardware part, also includes an explanation of the system design techniques and the circuit used to connect the sensors to the Wi-Fi panel, which we have used to design the control unit.

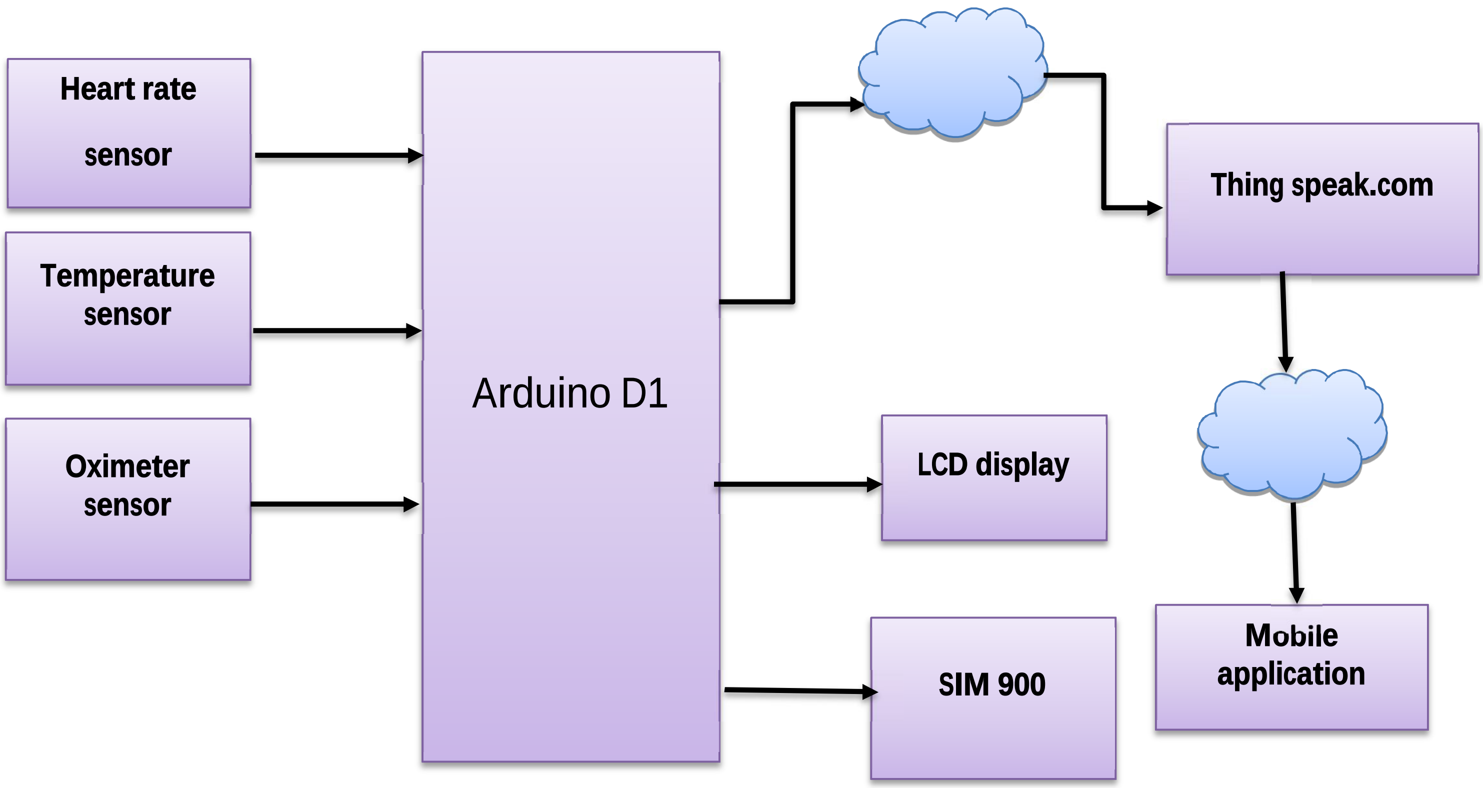


Figure 0-1The general block diagram

3.3 Hardware Cost

Table 0-1 Cost of Hardware

NO.	List of components	amount	cost
1	Arduino D1	1	7$
2	Max30100(Pulse and Oxygen in Blood Sensor)	1	10$
3	Temperature sensor	1	2$
4	Wires	10	1$
5	LCD &I2C	1	2$
6	SIM900	1	13$

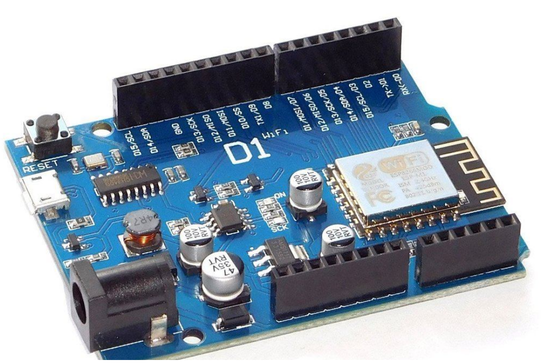
3.4 Device description

3.4.1 Arduino D1

The ESP8266-D1 is a wireless 802.11 (Wi-Fi) microcontroller development board compatible with the Arduino IDE. It turns the very popular ESP8266 wireless (Wi-Fi) module into a fully-fledged development board. The layout of this board is based on a standard Arduino hardware design with similar proportions to the Arduino Uno and Leonardo. It also includes a set of standard Arduino headers which means many existing Arduino shields can be plugged directly into the board (see note below figure 3.2).

Features:

- Product code: HCDVBD0028
- Integrated ESP8266 module with 32-bit 80MHz microcontroller/4M flash
- microUSB serial/programming interface
- Can be powered via USB cable – no external PSU required
- Arduino Compatible headers
- Directly supported by the Arduino IDE
- 2.1mm external DC PSU socket (6.5 - 12V)



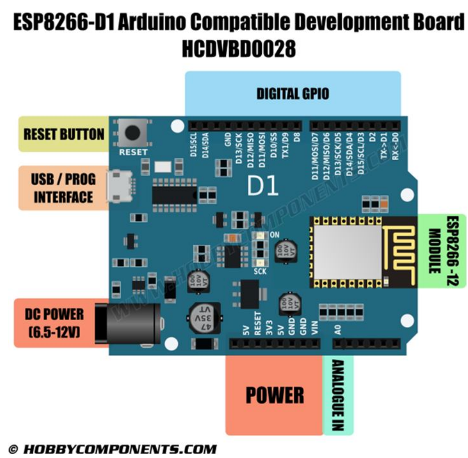


Figure 0-2Arduino D1

3.4.2 Temperature Sensor

Analog Devices analog temperature sensors as shown in fig 3.3 provide current or voltage output proportional to the absolute temperature with accuracies of up to ±1°C.

This thermistor-based analog temperature sensor can be used with an Arduino to return the ambient temperature value in Celsius. Uses a 10K Ohm resistor in series with a thermistor to give an analog output. It has specification table 3.2

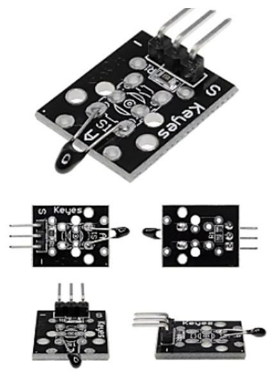


Figure 0-3 Analog temperature sensor

Table 0-2 Specification of Analog Temperature Sensor

Temperature Range	**-55°C – +125°C**
Resolution	9–12 bits (configurable)
Protocol	Dallas 1-Wire
Accuracy	±5°C
Dimensions	20mm x 15mm x 5mm (LxWxH)
Software	Arduino library available
Color	Black or Reed
Material	PCB

Features

- Thermistor-based analog temperature sensor
- Accurately measure temperature without calibration
- Applications include gardening & home alarm systems

3.4.2.1 Normal body temperature

Normal body temperature varies by person, age, activity, and time of day. The average normal body temperature is generally accepted as 98.6°F (37°C). Some studies have shown that the "normal" body temperature can have a wide range, from 97°F (36.1°C) to 99°F (37.2°C). A temperature over 100.4°F (38°C) most often means you have a fever caused by an infection or illness. Body temperature normally changes throughout the day.

3.4.3 Pulse and Oxygen in Blood Sensor(Max30100)

Pulse oximetry is a way to measure how much oxygen your blood is carrying. By using a small device called a pulse oximeter (see figure 3.4), your blood oxygen level can be checked without needing to be stuck with a needle. The blood oxygen level measured with an oximeter is called your oxygen saturation level (abbreviated O2 sat or SaO2). This is a percentage of how much oxygen your blood is carrying compared to the maximum it is capable of carrying. Normally, more than 89% of your red blood should be carrying oxygen. In its most common (trans missive) 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 absorbance's due to the pulsing arterial blood alone, excluding venous blood, skin, bone, muscle and fat.

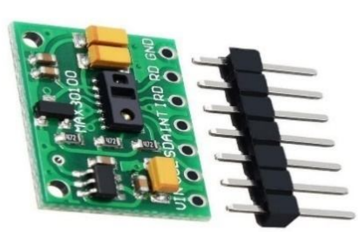


Figure 0-4 Pulse and Oxygen in Blood Sensor

3.4.3.1 Normal Heart Rate Level:

A normal resting heart rate for adult's ranges from 60 to 100 beats per minute.
Generally, a lower heart rate at rest implies more efficient heart function and better cardiovascular fitness. For example, a well-trained athlete might have a normal resting heart rate closer to 40 beats per minute. When you feel your pulse, count the number of beats in 15 seconds. Multiply this number by four to calculate your beats per minute.
Although there is a wide range of normal, an unusually high or low heart rate may indicate an underlying problem. Consult your Physician if your resting heart rate is consistently above 100 beats a minute (tachycardia) or if you are not a trained athlete and your resting heart rate is below 60 beats a minute (bradycardia) — especially if you have other signs or symptoms, such as fainting, dizziness or shortness of breath.

many factors can influence heart rate, including:

- Age
- Fitness and activity levels
- Being a smoker
- Having cardiovascular disease, high cholesterol or diabetes
- Air temperature
- Body position (standing up or lying down, for example)
- Emotions
- Body size
- Medications

3.4.3.2 Normal Oxygen Level

Everyone's oxygen saturation fluctuates, especially when changing activities throughout the day. To determine your normal oxygen range, simply check your oxygen saturation 4 times a day for 5 days using your personal Nonin Gaseous Oxygen (GO2) brand fingertip oximeter. Record each measurement in the activity log and be sure to record what you were doing prior to checking.

Oxygen saturation measures how much oxygen the blood is carrying compared with its full capacity.

1. A SpO2 of greater than 95% generally is considered normal.

2. A SpO2 of 92% or less (at sea level) suggests hypoxemia.

In a patient with acute respiratory illness (e.g., influenza) or breathing difficulty (e.g. an asthma attack), a SPO2 of 92% or less may indicate a need for oxygen supplementation.

In a patient with stable chronic disease (e.g. Chronic Oxygen Provision Depletion (COPD)), an SpO2 of 92% or less should prompt referral for further investigation of the need for long-term oxygen therapy. Good blood oxygenation is necessary to supply the energy your muscles need in order to function, which increases during a sports activity. If your SpO2 value is below 95%, that could be a sign of poor blood oxygenation, also called hypoxia (Hypoxemia).

3.4.4 SIM900-GSM

SIM900 GSM/GPRS shield is a GSM modem as shown in figure 3.5, which can be integrated into a great number of IoT projects. You can use this shield to accomplish almost anything a normal cell phone can; SMS text messages, Make or receive phone calls, connecting to internet through GPRS, TCP/IP, and more, to top it off, the shield supports quad-band GSM/GPRS network, meaning it works pretty much anywhere in the world.

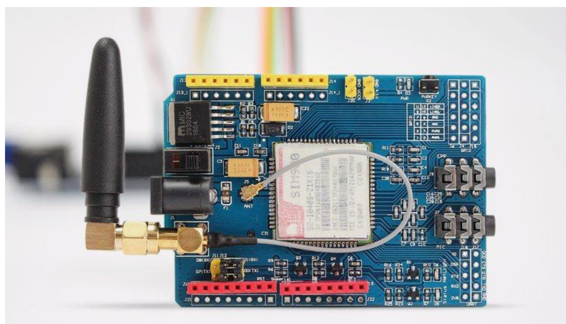


Figure 0-5SIM900-GSM

3.4.4.1 Hardware Overview of SIM900 GSM/GPRS Shield

The SIM900 GSM/GPRS shield is designed to surround the SIM900 chip with everything necessary to interface with Arduino, plus a few extra goodies to take advantage of the chip's unique features. Let's familiarize ourselves with these features and abilities of the shield. Here's a quick overview:(see figure 3.6)

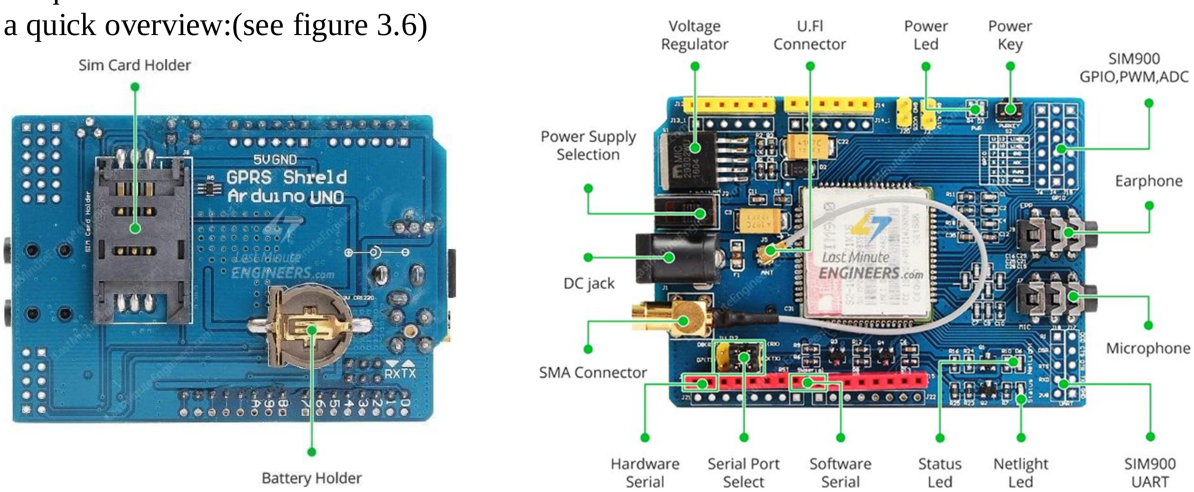


Figure 0-6 SIM900-GSM-GPRS-Shield-Top and Bottom -Hardware-Overview

The SIM900 shield packs a surprising amount of features into its little frame. Some of them are listed below:

- Supports Quad-band: GSM850, EGSM900, DCS1800 and PCS1900
- Connect onto any global GSM network with any 2G SIM
- Make and receive voice calls using an external earphone & electret microphone
- Send and receive SMS messages
- Send and receive GPRS data (TCP/IP, HTTP, etc.)
- Scan and receive FM radio broadcasts
- Transmit Power:
- Class 4 (2W) for GSM850
- Class 1 (1W) for DCS1800
- Serial-based AT Command Set
- U. FL and SMA connectors for cell antenna
- Accepts Full-size SIM Card

3.4.4.2 LED Status Indicators

There are three LEDs on the SIM900 GSM/GPRS shield which indicates connectivity or power status. By observing these LEDs, you can get a visual feedback on what’s going on with the shield.

PWR: This LED is connected to the shield’s power supply line. If this LED is on, the shield is receiving power.

Status: This LED indicates SIM900’s working status. If this LED is on, the chip is in working mode.

Net light: This LED indicates the status of your cellular network. It’ll blink at various rates to show what state it’s in.

- off: The SIM900 chip is not running
- 64ms on, 800ms off: The SIM900 chip is running but not registered to the cellular network yet.
- 64ms on, 3 seconds off: The SIM900 chip is registered to the cellular network & can send/receive voice and SMS.
- 64ms on, 300ms off: The GPRS data connection you requested is active.

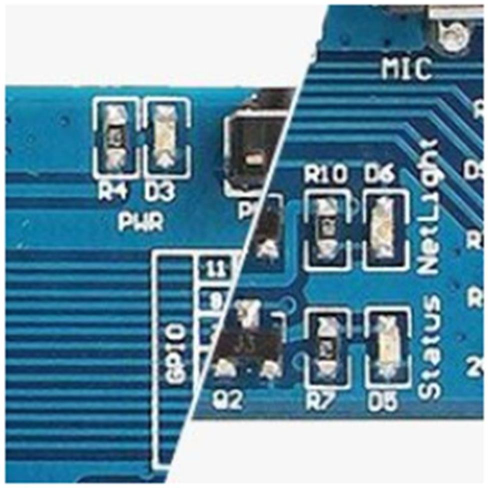


Figure 0-7 Led at SIM900-GSM

3.4.4.3 Supplying Power for SIM900 Shield

One of the most important parts of getting the SIM900 shield working is supplying it with enough power.

Depending on which state it's in, the SIM900 can be a relatively power-hungry device. The maximum current draw of the chip is around 2A during transmission burst. It usually won't pull that much, but may require around 216mA during phone calls or 80mA during network transmissions. This chart from the datasheet summarizes what you may expect as table3.3.

Table 0-3 Suppling power for SIM900

Modes	Frequency	Current Consumption
Power down		60 uA
Sleep mode		1 mA
Stand by		18 mA
Call	GSM850	199 mA
	EGSM900	216 mA
	DCS1800	146 mA
	PCS1900	131 mA
GPRS		453 mA
Transmission burst		2 A

The operating voltage of SIM900 chip is from 3.4V to 4.4V. To keep supply voltage safe at 4.1V, the shield comes with a high current, high accuracy, low-dropout voltage regulator MIC29302WU from Micrel – capable of handling load currents up to 3A.

3.4.4.4 Antenna

An antenna is required to use the SIM900 for any kind of voice or data communications as well as some SIM commands.

The shield has two interfaces for connecting antenna viz. a U. FL connector and a SMA connector. They are connected through a patch cord.

The shield usually comes with a 3dBi GSM antenna and allows you to put the shield inside a metal case (as long the antenna is outside).

3.4.4.5 SIM Socket

There’s a SIM socket on the back. Any activated, 2G full-size SIM card would work perfectly.

The workings of the SIM card socket can take some getting used to. To unlock the latch, push the top part of the assembly, and then lift it up. Place the SIM card into the bottom part of the socket. Then fold the arm back into the body of the socket, and gently push it forward towards the LOCK position.

3.4.4.6 RTC (Real Time Clock)

The SIM900 shield can be configured to keep time. So there is no need for any separate RTC. This will keep the time even when the power is OFF.

Chapter 4

Hardware Connection

4.1 Arduino D1 Connection

We use the Arduino Uno and ESP8266 for showing the connection of component replacing the D1 (there is no D1 at simulation program). When we connect the ESP8266 with Arduino we need a Logical Level Converter – Bi-Directional.

The LLC is used to coordinate levels between 5V controllers and 3.3V components and vice versa.

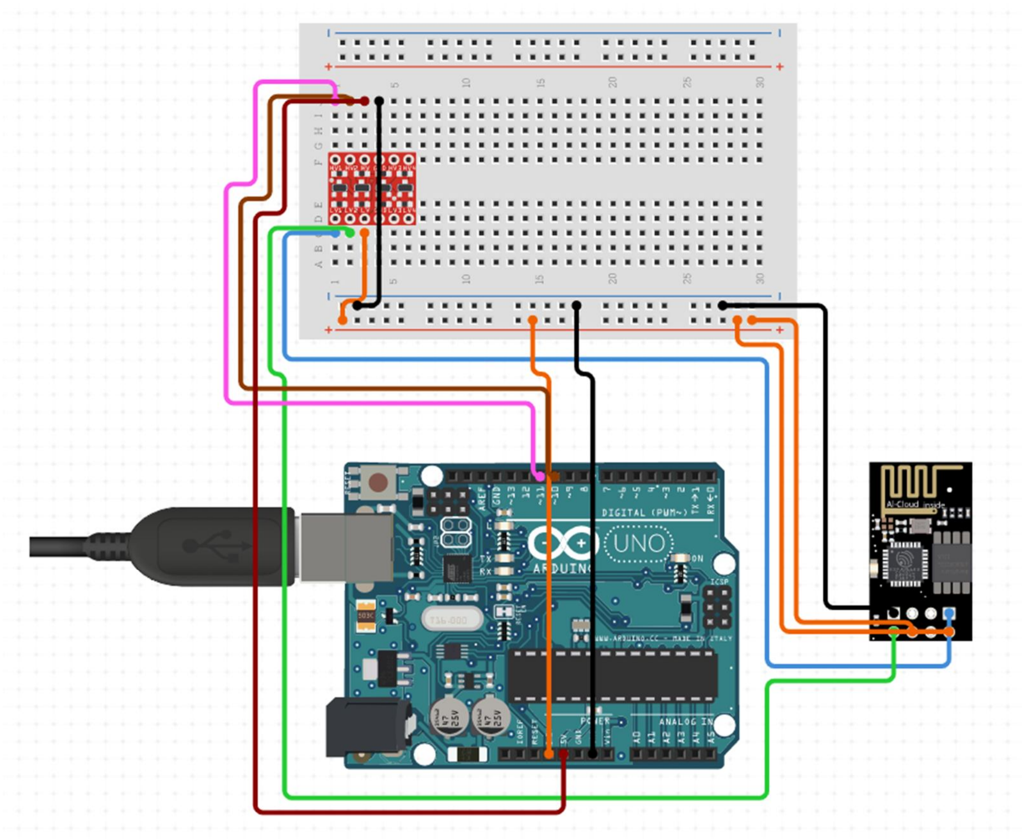


Figure 0-1 Arduino D1 connection

4.2 Temperature Sensor Connection

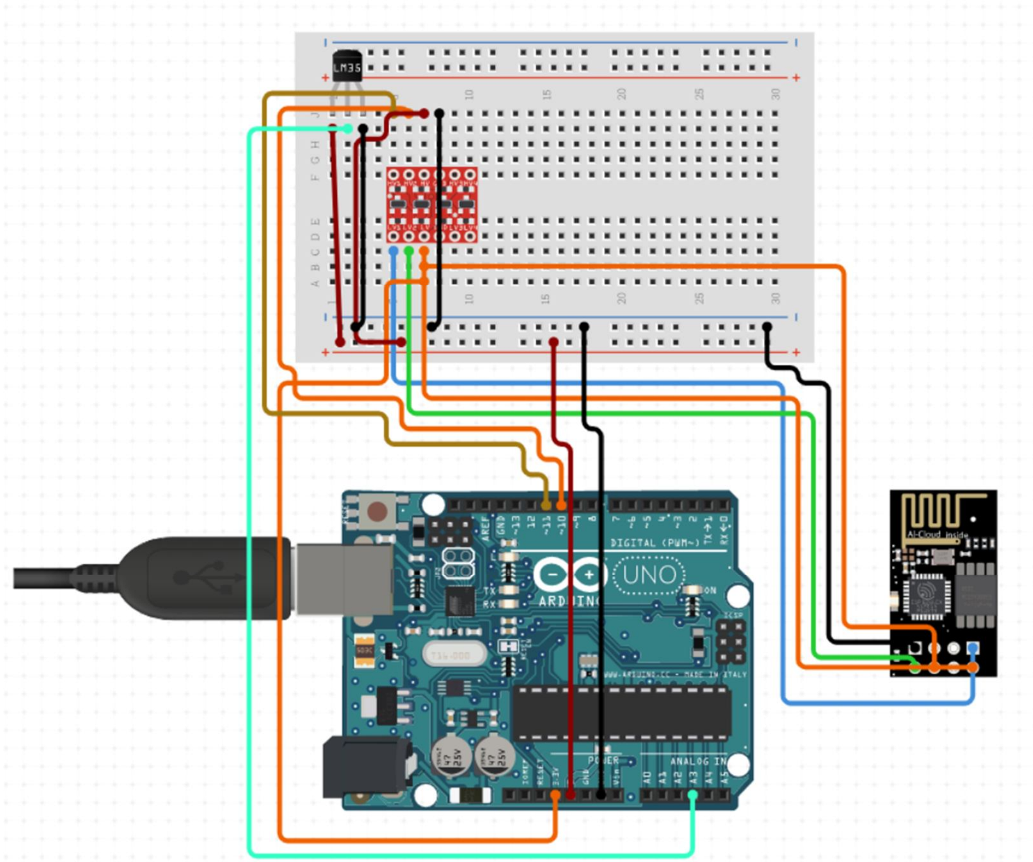


Figure 0-2 Temperature sensor connection

4.3 Pulse and Oxygen in Blood Sensor Connection

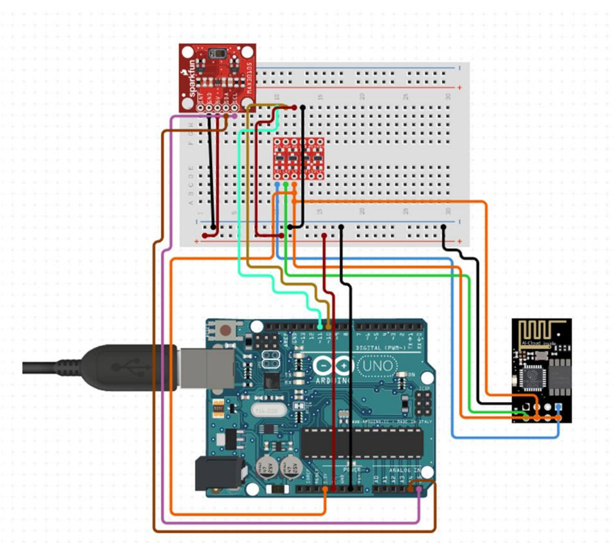


Figure 0-3 Pulse and Oxygen in Blood Sensor Connection

4.4 SIM900-GSM Connection

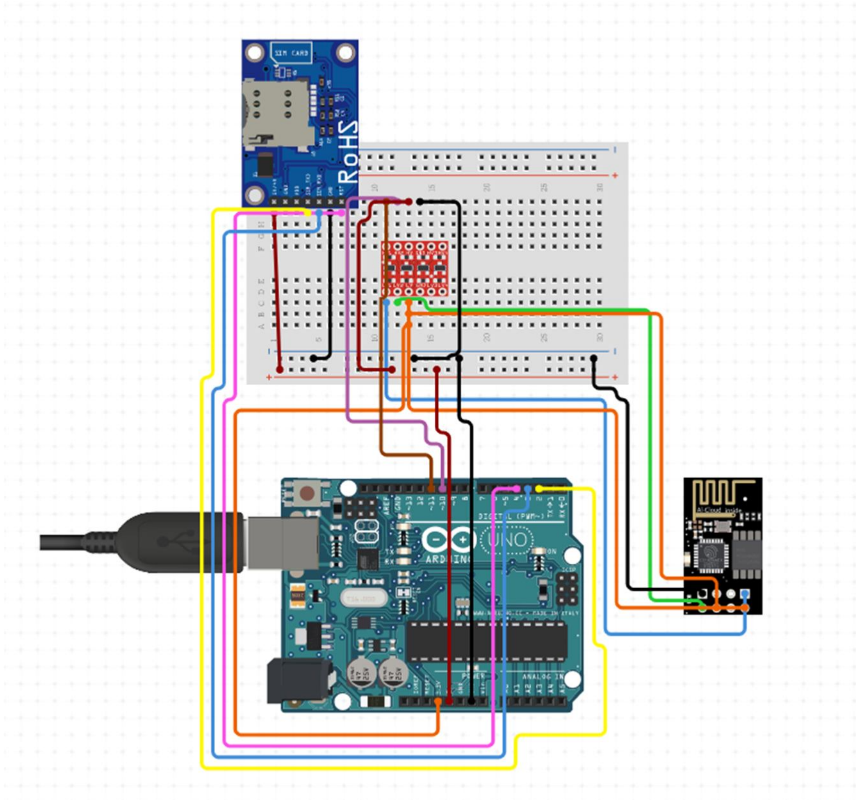


Figure 0-4 SIM900-GSM Connection

4.5 Final Circuit Connection with LCDI2C

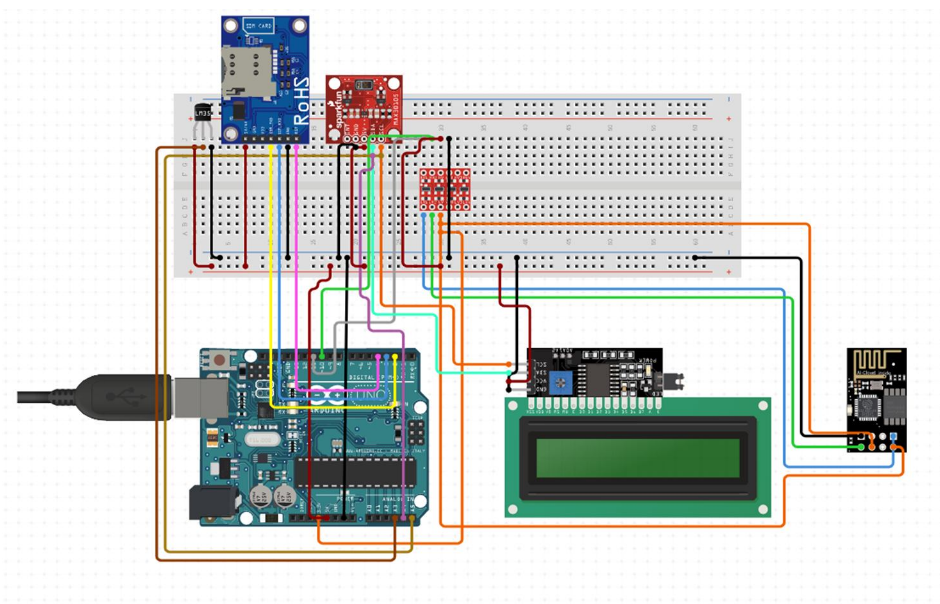


Figure 0-5 Final Circuit Connection with LCDI2C

CHAPTER 5

SOFTWARE

5.1 ARDUINO IDE

The Arduino integrated development environment (IDE) is a cross-platform application written in Java, and derives from the IDE for the Processing programming language and the Wiring projects. It is designed to introduce programming to artists and other newcomers unfamiliar with software development. It includes a code editor with features such as syntax highlighting, brace matching, and automatic indentation, and is also capable of compiling and uploading programs to the board with a single click. A program or code written for Arduino is called a "sketch".

Arduino programs are written in C or C++. The Arduino IDE comes with a software library called "Wiring" from the original Wiring project, which makes many common input/output operations much easier. The users need only to define two functions to make an executable cyclic executive program:

- setup(): a function that runs once at the start of a program and that can initialize settings.
- loop(): a function called repeatedly until the board powers off.

Most Arduino boards contain an LED and a load resistor connected between the pin 13 and ground, which is a convenient feature for many simple tests. The previous code would not be seen by a standard C++ compiler as a valid program, so when the user clicks the "Upload to I/O board" button in the IDE, a copy of the code is written to a temporary file with an extra include header at the top and a very simple main() function at the bottom, to make it a valid C++ program.

The Arduino IDE uses the GNU toolchain and AVR Libc to compile programs, and uses avrdude to upload programs to the board.

5.1.1 GETTING STARTED WITH ARDUINO

As the Arduino platform uses Atmel microcontrollers, Atmel's development environment, AVR Studio or the newer Atmel Studio, may also be used to develop software for the Arduino.

5.1.1.1 Get an Arduino board and USB cable

We use an Arduino WeMos D1R1

Also need a standard USB cable (A plug to B plug): the kind you would connect to a USB charger for Samsung phone,

5.1.1.2 Connect the board

The arduino WeMos D1R1 automatically draw power from either the USB connection to the computer or an external power supply. The power source is selected with a jumper, a small piece of plastic that fits onto two of the three pins between the USB and power jacks. Check that it's on the two pins closest to the USB port.

Connect the Arduino board to your computer using the USB cable. The green power LED (labelled PWR) should go on.

5.1.1.3 Install the drivers

Installing drivers for the Arduino Uno or Arduino Mega 2560 with Windows 10,8,7, Vista, or XP:

- Plug in your board and wait for Windows to begin its driver installation process. After a few moments, the process will fail, despite its best efforts
- Click on the Start Menu, and open up the Control Panel.
- While in the Control Panel, navigate to System and Security. Next, click on System. Once the System window is up, open the Device Manager.
- Look under Ports (COM & LPT). You should see an open port named " Arduino WeMos D1R1 (COMxx)". If there is no COM & LPT section, look under "Other Devices" for "Unknown Device".
- Right click on the "Arduino UNO (COmxx)" port and choose the "Update Driver Software" option.
- Next, choose the "Browse my computer for Driver software" option.
- Finally, navigate to and select the driver file named "arduino.inf", located in the "Drivers" folder of the Arduino Software download (not the "FTDI USB Drivers" sub-directory).
- Windows will finish up the driver installation from there.

5.1.1.4 Launch the Arduino Application

Double-click the Arduino application (arduino.exe) you have previously downloaded.

5.1.1.5 Open the program and paste it in Arduino

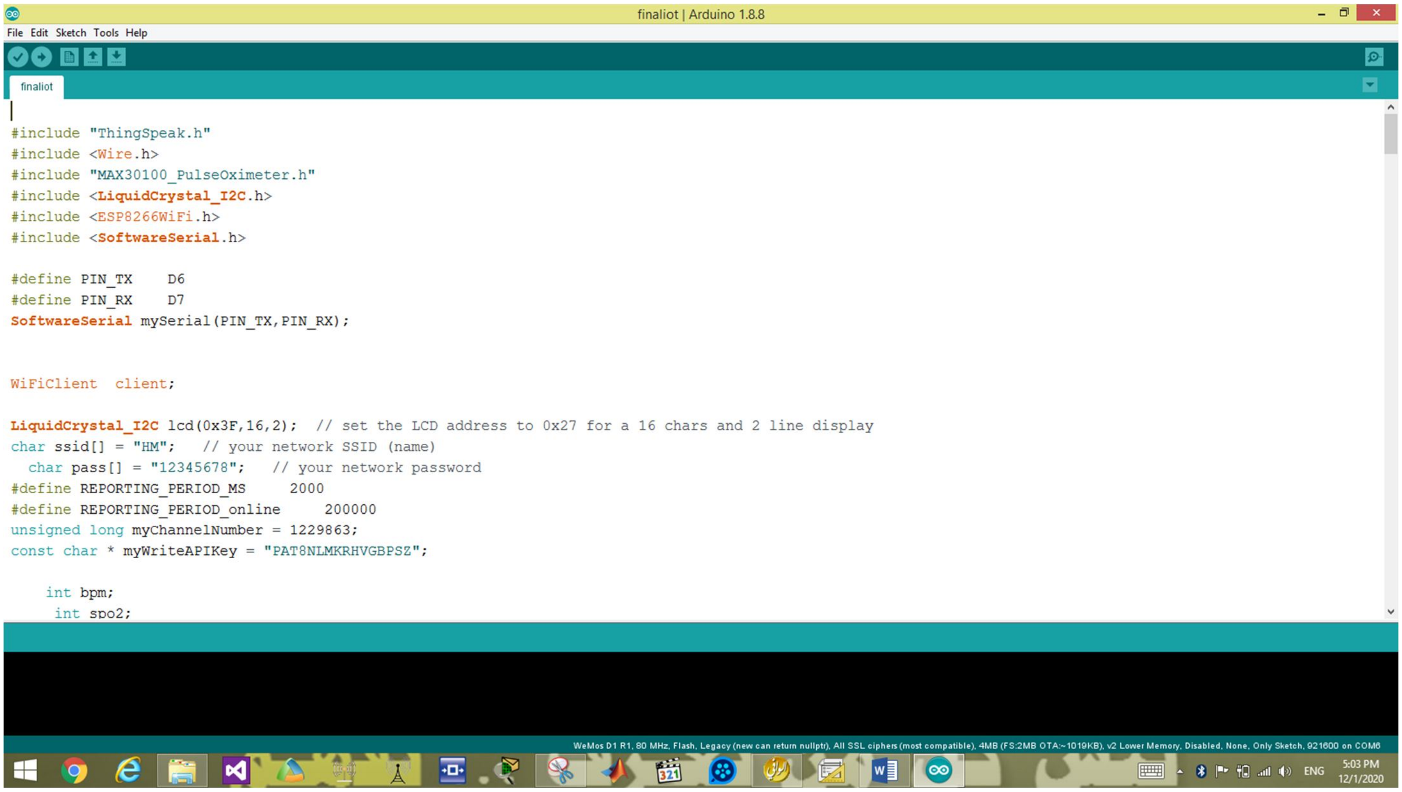


Figure 0-1 Running the code

5.1.1.6 Open Tools and Select the Board

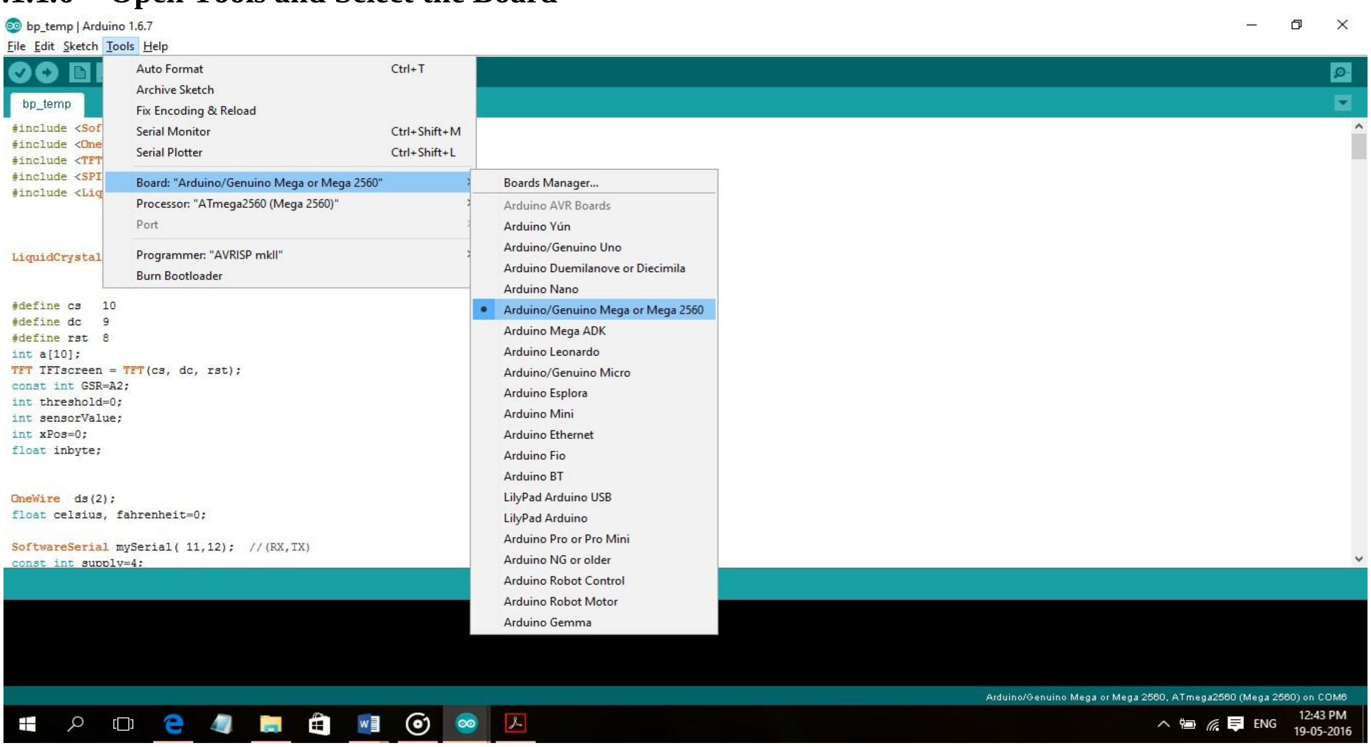


Figure 0-2 Selecting the board

5.1.1.7 Select your serial port

Select the serial device of the Arduino board from the Tools | Serial Port menu. This is likely to be COM3 or higher (COM1 and COM2 are usually reserved for hardware serial ports). To find out, you can disconnect your Arduino board and re-open the menu; the entry that disappears should be the Arduino board. Reconnect the board and select that serial port.

5.1.1.8 Upload the program

Now, simply click the "Upload" button in the environment. Wait a few seconds - you should see the RX and TX led on the board flashing. If the upload is successful, the message "Done uploading." will appear in the status bar

Figure 0-3 Uploading the code

A few seconds after the upload finishes, you can monitor your program through Arduino serial monitor.

5.2 Thingspeak

Thingspeak is an open source platform that provides various services exclusively targeted for development of IoT (Internet of Things) applications. It enables various services like real time data collection, analysis and visualisation of collected data via charts. It enables the creation of various plugins, apps collaborating with various web services, social networking and other APIs.

5.2.1 Thingspeak Channel

'Thingspeak channel' is the core element of the thingspeak platform. This channel is used to store the real-time data or the data transferred through various sensors and embedded systems. Data stored at the channel is further used for analysis and visualisation.

5.2.2 Creating a channel

Before creating a channel you need to sign in to things speak. You can easily sign in either using your either thingspeak account or mathswork account, or create a new mathswork account via following link:

https://thingspeak.com/users/sign_up

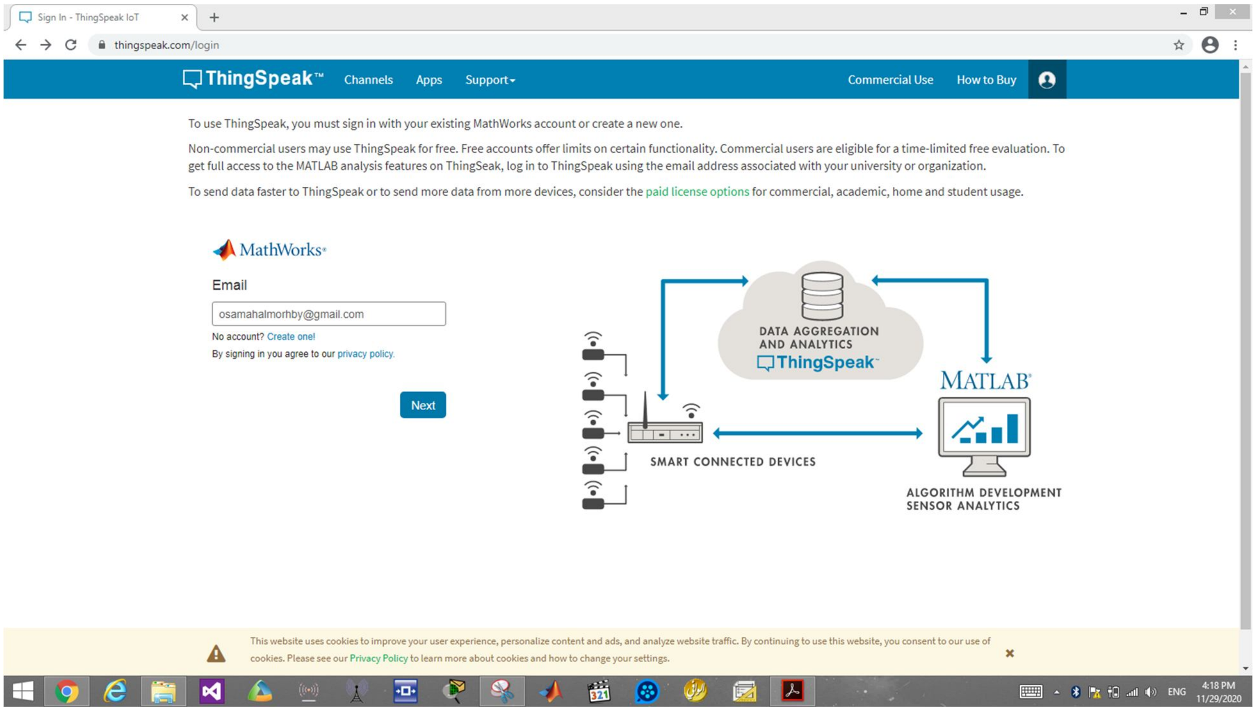


Figure 0-4 Login page

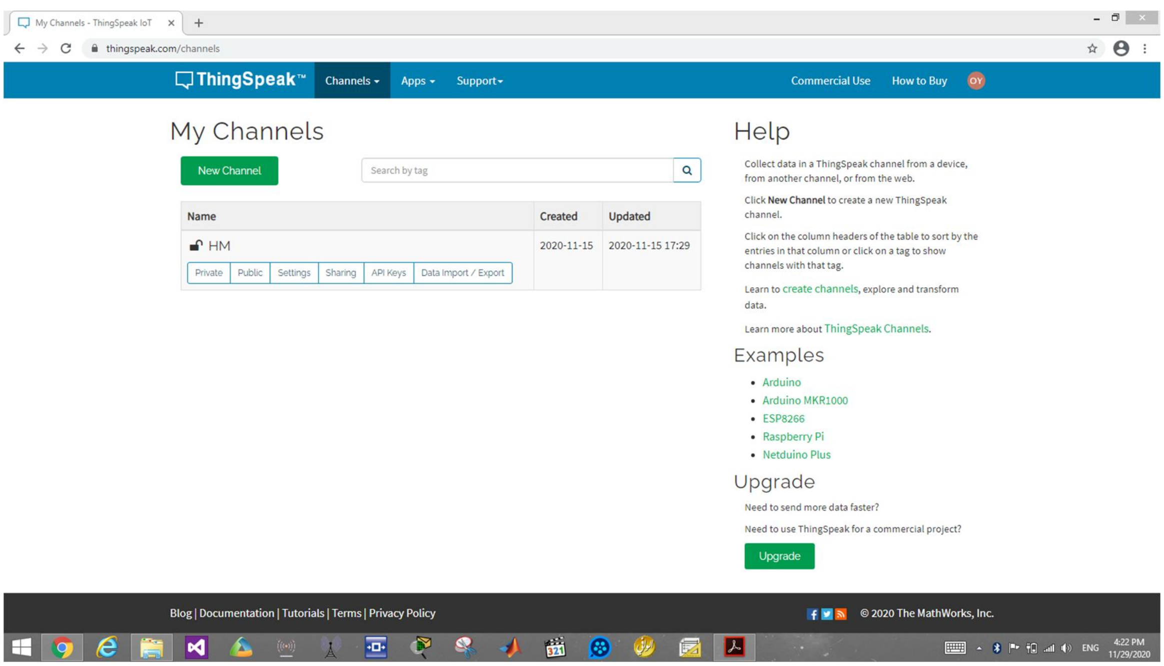


Figure 0-5 Home page

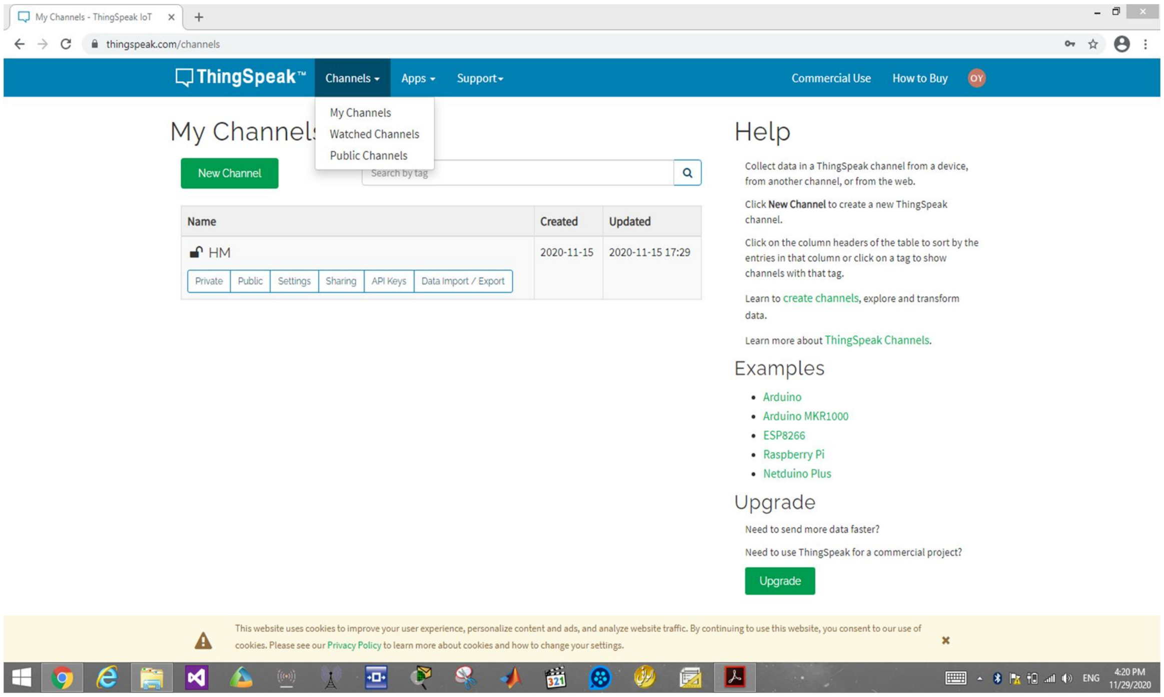


Figure 0-6 Select channels

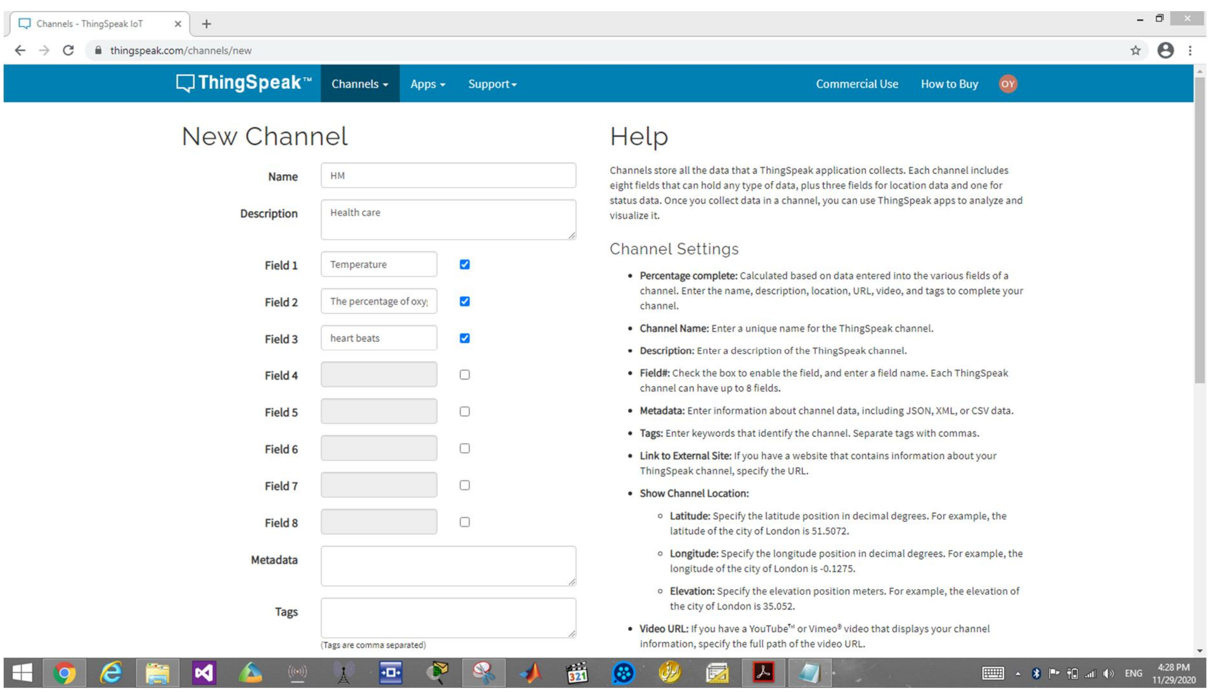


Figure 0-7 Great new channel

1. Click on the menu bar ‘**Channels > My Channels**.’
2. Now on the channels page click on the button ‘**New Channel’**.

3. New channel page have various text box fields showing the settings of the channel.
    a. **Name** – provide a unique name to your channel.
    b. **Fields** – Click the check boxes next to the field and then enter the field name.
    c. To make your channel public check the '**Make Public**'check box.
    d. Similarly, you can also add the location to your channel by clicking the '**Show Location'** check box.
    e. Check the '**Show video**' check box to make the video visible uploaded by you.
    f. Now click the '**Save channel**' button to save your channel.

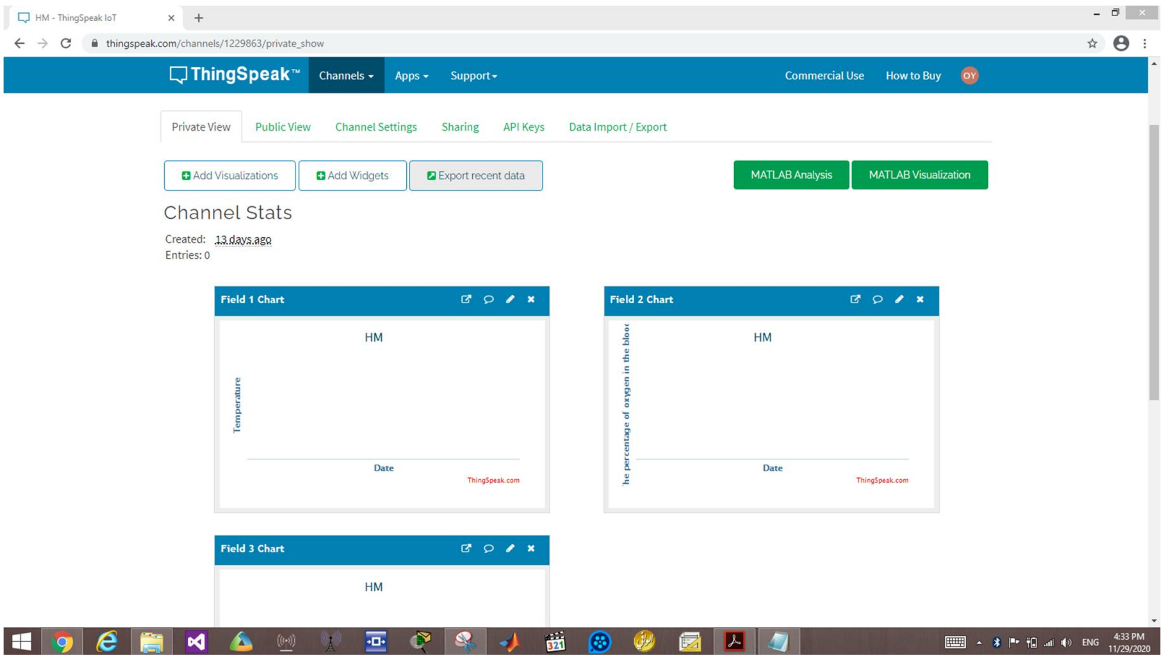


Figure 0-8 My channel page

4. Now , the channel page opens with the following tabs:
    a. **Private View**- It displays the information about your channel that is only visible to you.

    b. **Public View**- If you have chosen to make your channel publically visible then it will display the selected fields and information

    c. **API Keys**- In this tab you will have two API Keys – Read API key (to read from your channel), write API Key (to write to your channel).

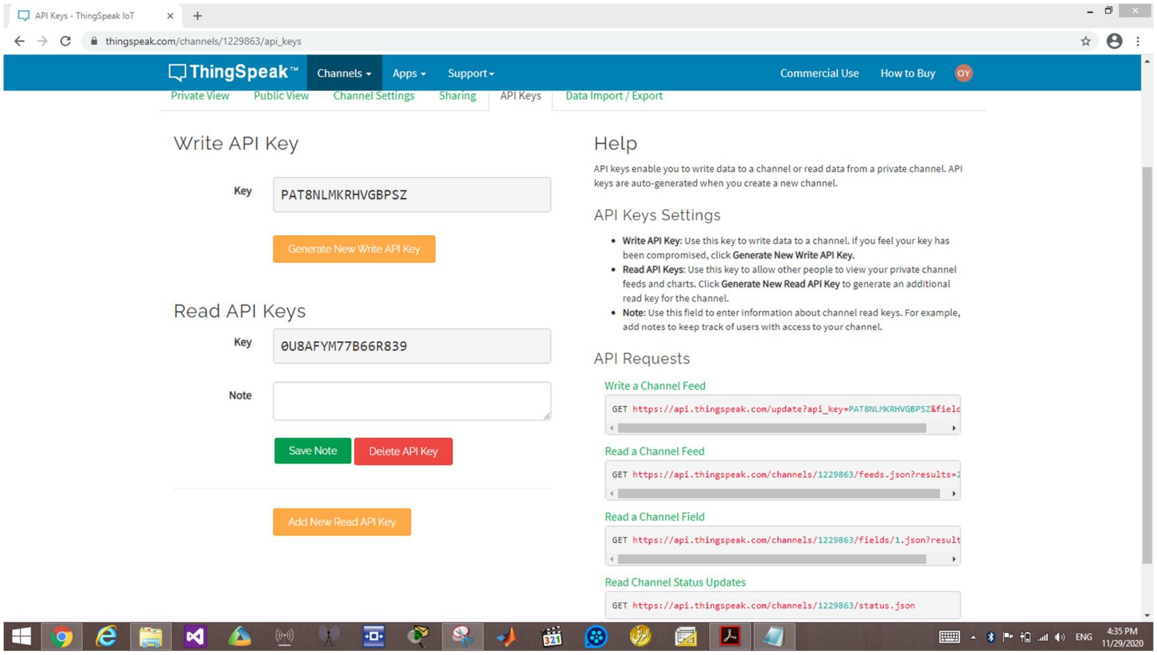


Figure 0-9 API keys

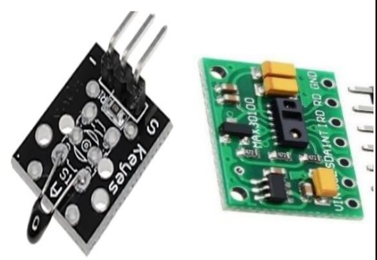
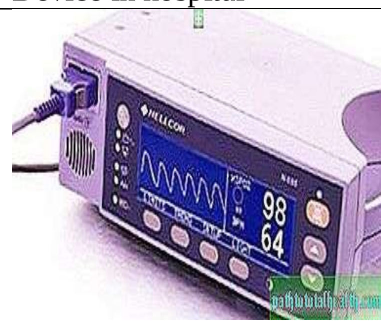
CHAPTER 6

RESULT AND ANALYSIS

6.1 Introduction

This chapter is the last chapter in our project ,we will talk about the results, challenges, and problems we faced while working on the project , we will also mention our interview with science and technology hospital .

Table 0-1 The difference between devices using in hospital and the device of our project including results

Differences	Our device	Device in hospital	Other devices
Pictures			 
Duties	measuring temperature, heartbeat and oxygen in blood .	measuring heartbeat and oxygen only .	Oximeter :measuring oxygen and heartbeat . Thermometer :measuring temperature.
Depends on	Sensors Of temperature And of oxygen with heartbeat .	Same as Oximeter .	Oximeter: transmissive sensor and reflective sensor. Thermometer: mercury inside tube (if temperature is high, mercury spreads but if temperature is low, mercury cowers).
Results	Heartbeat=90 Oxygen =94 Temperature =35	Heartbeat=97 Oxygen =94	Heartbeat =94 Oxygen =96 Temperature =37

6.2 Conclusion

the project that has undertaken has helped us to gain a better perspective on various aspects related to our course of study as well as practical knowledge of electronic equipment and communication. We became familiar with software analysis ,designing , implementation, testing and maintenance concerned with our project .

we visited science and technology hospital and we met doctor Talal Farhan who helped us to get more information about devices are used in hospitals which can be replaced by our device and helped us to get results from their device and compared them with results of our device .

we got some problems one of them that the devices those we have used were not high efficient then the reading was not fixed so we solved it by define the range of all sensors in code to get better results .

another problem was the size of the devices are big so we could change those by using IC instead of individual pieces .

6.3 Future work

the smart hospital objective and scope have been successfully achieved but in order many improvement can be done to make it more practical. we make the following recommendations for next phase of the project development :

1. Relocate the device from scientific to product by changing the d1 Arduino to an IC piece.
2. Healthcare monitoring center that can monitor the vitals of the patients.
3. Providing android application to monitor the patient by the doctor .

REFERENCES

- HTTPS://DATA-FLAIR.TRAINING/BLOGS/IOT-PROTOCOLS/
- HTTPS://WWW.RESEARCHGATE.NET/PUBLICATION/322187294_EVERYTHING_YOU_WANTED_TO_KNOW_ABOUT_SMART_HEALTH_CARE_EVALUATING_THE_DIFFERENT_TECHNOLOGIES_AND_COMPONENTS_OF_THE_INTERNET_OF_THINGS_FOR_BETTER_HEALTH
- HTTP://WWW.CSE.WUSTL.EDU/~JAIN/CSE570-15/FTP/IOT_PROT.PDF
- HTTPS://WWW.KELLTONTECH.COM/KELLTON-TECH-BLOG/INTERNET-OF-THINGS-PROTOCOLS-STANDARS
- HTTPS://WWW.RESEARCHGATE.NET/PUBLICATION/322187294
- HTTPS://DOI.ORG/10.1155/2017/9324035
- HTTPS://WWW.GOOGLE.COM/URL?SA=T&SOURCE=WEB&RCT=J&URL=HTTPS
- HTTPS://WWW.HINDAWI.COM/JOURNALS/JECE/2017/9324035/

APENDIX

Code in Arduino

```
#include "ThingSpeak.h"
#include <Wire.h>
#include "MAX30100_PulseOximeter.h"
#include <LiquidCrystal_I2C.h>
#include <ESP8266WiFi.h>
#include <SoftwareSerial.h>

#define PIN_TX    D6
#define PIN_RX    D7
SoftwareSerial mySerial(PIN_TX,PIN_RX);



WiFiClient  client;

LiquidCrystal_I2C lcd(0x3F,16,2);  // set the LCD address to 0x27 for a 16 chars and 2 line
display
char ssid[] = "HM";   // your network SSID (name)
  char pass[] = "12345678";   // your network password
#define REPORTING_PERIOD_MS     2000
#define REPORTING_PERIOD_online     200000
unsigned long myChannelNumber = 1229863;
const char * myWriteAPIKey = "PAT8NLMKRHVGBPSZ";
```

```
int bpm;
 int spo2;
 int temp;
 int m;
 int x1;
 int only1=0;
  int bpmc;
 int spo2c;
 int tempc;
// PulseOximeter is the higher level interface to the sensor
// it offers:
//  * beat detection reporting
//  * heart rate calculation
//  * SpO2 (oxidation level) calculation
PulseOximeter pox;

uint32_t tsLastReport = 0;
uint32_t pre = 0;

// Callback (registered below) fired when a pulse is detected
void onBeatDetected()
{
      pox.update();

    Serial.println("Beat!");
   bpm=pox.getHeartRate();
   spo2=pox.getSpO2();
```

```
        x1=1;
  lcd.setCursor(7,1);
 lcd.print("beat");
}

void setup()
{
    pinMode(D5,OUTPUT);digitalWrite(D5,0);
delay(3000);
digitalWrite(D8,0);
    Serial.begin(115200);
mySerial.begin(9600);
delay(500);
  delay(500);

  digitalWrite(D0,0);
    Serial.print("Initializing pulse oximeter..");
lcd.init();                      // initialize the lcd
  // Print a message to the LCD.
  lcd.backlight();
  lcd.clear();
  lcd.setCursor(2,0);
  lcd.print("smart health !");
  lcd.setCursor(2,1);
  lcd.print("initilizeing");
```

```
if (!pox.begin()) {
        Serial.println("FAILED");
        for(;;);
    } else {
        Serial.println("SUCCESS");
    }
  WiFi.mode(WIFI_STA);
  WiFi.disconnect();
  delay(100);
      Serial.print("Connecting Wifi: ");
  Serial.println(ssid);
  WiFi.begin(ssid,pass);
  while(WiFi.status() != WL_CONNECTED){
      Serial.print(".");
      delay(1000);

    }



  ThingSpeak.begin(client);  // Initialize ThingSpeak
    // Initialize the PulseOximeter instance
    // Failures are generally due to an improper I2C wiring, missing power supply
    // or wrong target chip
    if (!pox.begin()) {
        Serial.println("FAILED");
        for(;;);
    } else {
```

```
      Serial.println("SUCCESS");
   }
 mySerial.println("AT"); //Once the handshake test is successful, it will back to OK
   pox.setOnBeatDetectedCallback(onBeatDetected);
}

void loop()
{
   // Make sure to call update as fast as possible
   pox.update();

   // Asynchronously dump heart rate and oxidation levels to the serial
   // For both, a value of 0 means "invalid"
   if (millis() - tsLastReport > REPORTING_PERIOD_MS) {



temp=72-analogRead(0)/5;
if(temp<=31)
temp=0;
if(temp>=35)
tempc=temp;

if(bpm>90 || bpm<70){
  bpm=0;spo2=0;
  }
  if(spo2>100 || spo2<80){
  bpm=0;spo2=0;
```

```
   }
  if (bpm>70 & bpm<90){
    tempc=temp;
bpmc=bpm;
spo2c=spo2;
  Serial.println("sending");
  lcd.clear();
  lcd.setCursor(0,0);
  lcd.print("HR=");
  lcd.print(bpm);
  lcd.setCursor(6,0);
  lcd.print(" Temp=");
  lcd.print(temp);
  lcd.setCursor(0,1);
  lcd.print("spo2=");
  lcd.print(spo2);
  if(WiFi.status() == WL_CONNECTED){
     ThingSpeak.setField(1, tempc);
  ThingSpeak.setField(2, spo2c);
  ThingSpeak.setField(3,bpmc );
lcd.setCursor(7,1);
lcd.print("  send!");
int x = ThingSpeak.writeFields(myChannelNumber, myWriteAPIKey);
  if(x == 200){
    Serial.println("Channel update successful.");
  }
  else{
```

```
    Serial.println("Problem updating channel. HTTP error code " + String(x));
  }

   }   delay(500);    ESP.restart();

  }

    Serial.print("temp: ");
    Serial.println(temp);
        Serial.print("Heart rate:");
        Serial.print(bpm);
        Serial.print("bpm / SpO2:");
        Serial.print(spo2);
        Serial.println("%");

lcd.clear();
  lcd.setCursor(0,0);
  lcd.print("HR=");
  lcd.print(bpm);
  lcd.setCursor(6,0);
  lcd.print(" Temp=");
  lcd.print(temp);
  lcd.setCursor(0,1);
  lcd.print("spo2=");
  lcd.print(spo2);
```

```
if(x1==1){
 // m++;
}
if(m>=3){
  x1=0;
  bpm=0;
  spo2=0;
lcd.setCursor(7,1);
 lcd.print("      ");
}
if(bpm==0){
lcd.setCursor(7,1);
 lcd.print("      ");}
if(temp>28){
 // bpm= random(80,85);
   //spo2=random(94,98);
}
else{
  bpm=0;
  spo2=0;
  lcd.setCursor(9,1);
 lcd.print("      ");
}

 if(temp>38 &temp<=42 &only1==0){
  Serial.println("send massage");
  mySerial.println("AT+CMGF=1"); // Configuring TEXT mode
```

```
  updateSerial();
 mySerial.println("AT+CMGS=\"+967776877668\"");//change ZZ with country code and
xxxxxxxxxxx with phone number to sms
  updateSerial();
 mySerial.print("high temp of the patient "+String(temp)); //text content
  updateSerial();
 mySerial.write(26);
 updateSerial();
mySerial.println("ATH");
 updateSerial();
 only1=1;
 }
 if(temp>42 &only1==0){
  Serial.println("call");
  mySerial.println("AT+CMGF=1"); // Configuring TEXT mode
  updateSerial();
  updateSerial();
  updateSerial();
mySerial.println("ATD + +967775246785;");
 updateSerial();
 delay(15000);
mySerial.println("ATH");
 updateSerial();
 only1=1;


 }
 if(temp<35){
 only1=0;
```

```
 }
 tsLastReport = millis();


    }


}



void updateSerial()
{
  delay(500);
  while (Serial.available())
  {
   // mySerial.write(Serial.read());//Forward what Serial received to Software Serial Port
  }
  while(mySerial.available())
  {
    Serial.write(mySerial.read());//Forward what Software Serial received to Serial Port
  }
}
```