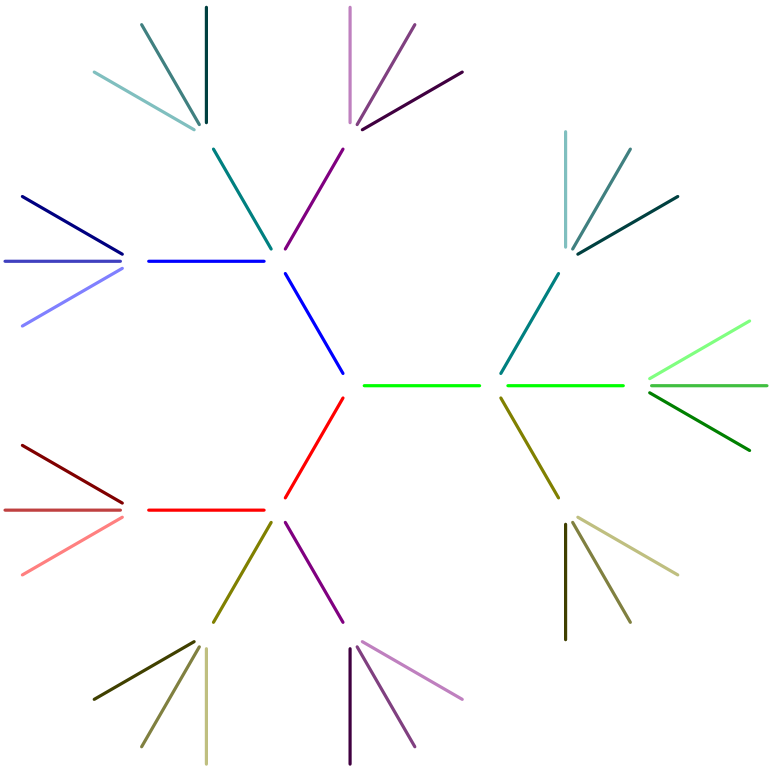


19EID 232 – Internet of Things

Unit wise Questions and Answers

Thursday 26th May, 2022

Acknowledgement

The satisfaction that accompanies successful completion of any task would be incomplete without the mention of people who made it possible. My special thanks goes to the following undergrad students of CSE department, GITAM Institute of Technology, Visakhapatnam, who made an effort to collect & contribute answers from various possible sources.

Harshita, Eswar, Pratiksha, Minie, Varun, Md Qadir Jelani, Sriram, Asritha sai, Kushal

I wish them all the best for their future endeavour.

List of Figures

List of Tables

Contents

1. Introduction to Internet of Things

1.1 Syllabus

1. Introduction and Definition of Internet of Things
2. IoT Growth
3. Application Areas of IoT,
4. Characteristics of IoT,
5. Things in IoT,
6. IoT Stack,
7. Enabling Technologies,
8. IoT Challenges,
9. IoT Levels
10. IoT vs. Cyberphysical Systems,
11. IoT vs WSN

1.2 Short Answer Questions

1. **Mention a few applications of IoT in daily life?**
    - In agriculture industry
    - Health Monitoring
    - Self - Driving Cars
    - Wearable's
    - Fitness industry
    - Smart Refrigerators

- Wireless Payment Systems

2. **List the advantages of IoT.**
   - Improved productivity of staff and reduced human labour
   - Efficient operation management
   - Better uses of resources and assets
   - Cost - effective operation
   - Improved Work Safety
   - Thorough marketing and business development
   - Improved customer service and retention
   - Better business opportunities
3. **Define Internet of Things**
   The Internet of Things describes the network of physical objects or "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.
4. **List the disadvantages of IoT.**
   - Security and privacy
   - Technical Complexity
   - Connectivity and power dependence
   - Integration
   - Higher costs
5. **List the characteristics of IoT**
   The characteristics of IoT are as follows:
   - **Connectivity**
     Connectivity is an important aspect/requirement of the IoT infrastructure. Things in IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime connectivity should be guaranteed at all times. Without connection, nothing makes sense.
   - **Intelligence and Identity**
     The extraction of knowledge (i.e. what is to be inferred) from the generated data is very important. For example, sensors generate data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity (something like an IP address). This identification is helpful in tracking the equipment and at times for querying its status.

- **Scalability**
  The number of elements (devices) connected to IoT zone is increased day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as outcome is enormous and it should be handled appropriately.
- **Dynamic and Self-Adapting**
  IoT devices should dynamically adapt themselves to the changing contexts or scenarios. Assume a camera meant for surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, night)
- **Architecture**
  IoT architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturer's products to function in the IoT network.
- **Safety**
  There is the danger of sensitive personal details of a user getting compromised when all his/her devices are connected to the Internet. This could cause a loss to the user. Hence, data security is a major challenge. Besides, the equipment involved in the huge IoT network may also be at risk. Therefore, equipment safety is also critical.

6. **What do you mean by "things" in IoT?**
   A thing in the context of the Internet Of Things (IoT), is an entity or a physical object that has a unique identifier, an embedded system and the ability to transfer data over a network.

7. **How many layers are there in the IoT stack, name them.**
   There are 7 layers in the IoT stack. From the top they are:
   (a) Layer 7 Application layer
   (b) Layer 6 User Experience layer
   (c) Layer 5 Session or Message layer
   (d) Layer 4 RF layer
   (e) Layer 3 Hardware Interface layer
   (f) Layer 2 Processing and Control action layer
   (g) Layer 1 Physical or Sensor layer.

8. **What are the challenges faced in developing IoT devices?**
   - Security and personnel safety
   - Privacy
   - Data extraction with consistency from complex environments
   - Connectivity

- Power requirements
- Complexity involved
- Storage

9. **What is WSN and what are differences between IoT and WSN?**
   Wireless Sensor Networks (WSNs) can be defined as a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analysed. In an IoT system, all of the sensors directly send their information to the internet. Conversely, in a WSN, there is no direct connection to the internet. Instead, the various sensors connect to a router or central node. A person may then route the data from the router or central node as they see fit.

10. **What is cyber physical system and what are the differences between cyber physical systems and IoT?**
    CPS is mainly concerned about the collaborative activity of sensors or actuators to achieve a certain goal and to this CPS uses an IoT system to achieve the collaborative work of the distributed systems.
    CPS is not IoT. IoT as one of its components. CPS is more complex than IoT and is very challenging as well. It is a combination of multiple engineering domains coming together, which includes computer science , electronics, electrical and mechanical engineering. A flight (aeroplane) can be seen as a CPS which has the influence of multiple domains of engineering. It also has IoT as one of the components. Obviously, the complexity increases by volume. CPS is expected to be much more brilliant and autonomous, taking appropriate decisions as and when needed. It is not merely about identifying, it is more about understanding and taking decisions in a much more dynamic way.

11. **Describe architecture of IoT?**
    IoT system architecture is often described as a four-stage process in which data flows from sensors attached to "things" through a network and eventually on to a corporate data center or the cloud for processing, analysis and storage. In the Internet of Things, a "thing" could be a machine, a building or even a person. IoT architecture essentially comprises of a number of elements: firstly, cloud service, then layers, protocols, sensors and devices and so on. To simplify it further, there are 3 main layers and 4 components to it.

    Three main layers of IoT architecture:

    (a) IoT Device Layer – which is nothing but the client layer

    (b) IoT Gateway Layer – that is server-side operators

(c) IoT Platform Layer – to connect the operator and client

Four components of IoT architecture which are:

(a) Connected devices (Sensors and actuators)

(b) Sensor Data Acquisition(Internet gateways and Data Acquisition Systems)

(c) Edge IT Data Processing

(d) Analyzing, Visualizing and Storing Data (Data center and cloud)

12. **What are communication protocols and what do they take care of?**
IoT communication protocols are modes of communication that enusure optimum security of the data being exchanged between IoT connected devices.we can connect the IoT devices via an IP network or a non-IP network. Though there is a difference in range ,power, and memory use.
Some of the major IoT technologies and protocols(IoT Communication Protocols) are Bluetooth, Wifi, Radio protocols, LTE-A, MQTT and Wifi-Direct. These IoT communication protocols cater to and meet the specific functional requirement of an IoT system.

Data exchange happens through these protocols. Protocols take care of the following:

- Addressing
- Format of the messages
- Message security(encryption and decryption)
- Routing
- Flow control
- Error monitoring
- Sequencing
- Re-transmission guidelines
- Segmentation of data packets

13. **Give examples of embedded computing boards**

- BeagleBone Black
- Node MCU
- Arduini Uno
- Raspberry Pi

14. **Enumerate the role of cloud in IoT**
Cloud computing in IoT facilitates seamless communication between IoT devices. This enables many robust APIs to interact between connected devices and smart devices. This way, cloud computing paves the way for the growth of connected technologies.

15. **How does IoT work?**

    An IoT system consists of sensors/devices which "talk" to the cloud through some kind of connectivity. Once the data gets to the cloud, software processes it and then might decide to perform an action, such as sending an alert or automatically adjusting the sensors/devices without the need for the user.

16. **How does IoT influence the development of smart cities?**

    The intuitive facets of IoT devices paired with enhanced network engagement enable IoT to promote versatility, transparency and efficiency in infrastructure planning. IOT also embeds energy-efficient projects to take off. Overall, with the whole array of advantages that IoT brings in, it is possible for the government to work towards building smart cities all across the globe.

    With the help of IoT, clever energy grids, automated waste management systems, smart homes, better security systems, improved traffic management mechanisms, advanced security features, water conservation mechanisms and so much more is possible. The two pronged blessings of artificial intelligence and innovation, IoT has allowed public utilities and urban planning to be highly intuitive. These have triggered the birth of smart homes and smart cities.

17. **Categorize cloud services.**

    They are categorized into three categories

    IaaS (Infrastructure-as-a-Service): In this cloud service, one can choose virtual machines over physical machines. In other words, it is a form of cloud computing that provides virtualized computing resources over the Internet. The users manage the machines. Select the OS and underlying applications, and pay per their use.

    PaaS (Platform-as-a-Service): It is a cloud computing model in which the cloud service provider (a third-party provider) delivers hardware and software tools needed for application development to users over the Internet. A PaaS provider hosts the hardware and software on its own infrastructure. Users have to build, manage and maintain the applications as per their requirement.

    SaaS (Software-as-a-Service): In this case, a complete software application is provided to the user. It can also be called application as a service. This service can be availed by paying a monthly, yearly, ctc. subscription.

    Some well-known service providers in the market are Amazon web services, Azure, Adafruit, etc.

1.3 Long Answer Questions

1. **List at least 6 challenges faced by IoT and describe them**
   As with any application, while building an IoT application one faces many challenges both technical and non-technical.
   Some of the challenges are listed as follows with a brief explanation.

   (a) **Security/ Personal safety-**
   It is one of the most prominent and very highly rated challenges to confront . Since a number of devices are used in the IoT zone, user data becomes more vulnerable to theft. So , it becomes necessary to make sure that the data is safe. Even the best of the social media websites get into trouble for misuse of the customer's data. Safeguarding the data is very important. Poor security features can let the attackers damage the whole network.
   People's personal safety is a concern and challenge too. The implants and wearable used by the users in the IoT infra should be safe. The devices should not cause any physical damage to the person using the same.
   Since many devices are in the loop, if one device get attacked, then the rest of the devices could also fall prey. To summarize, data security and personnel safety are major challenges in the typical IoT infrastructure.

   (b) **Privacy-**
   One could be tracked/monitored by anyone, as you are connected 24x7 to the Internet. At times, one could be tracked without the host's permissions in place. So, there is a threat on user data and a question on user privacy.

   (c) **Data Extraction with Consistency from Complex Environments-**
   It is a huge challenge to sense/extract data from complex environments. For instance, how to sense the data input(temperature, humidity etc)during the commute from a vehicle?. Assume, a very temperature- sensitive material is being transported, where the measurement is always expected to be perfect. Variation in the temperature could damage the products being transported as well. Particularly, if medicines/drugs are being transported, the temperature maintained is very critical and should be definitely monitored. In this case, if the temperature is about to be deviated, corrective action has to be taken to make sure that the drugs are not spoiled. Also, in IoT-based applications, the Internet is needed and is mandatory at most of the places. In hilly, technically not so up to date terrains, providing Internet may not be easy all the time. Hence, data extraction and sending the data to the cloud could be more challenging. Extracting data inside a room is different from extracting the data from an open environment.

   (d) **Connectivity-**

Connectivity is a serious challenge that the IoT world must acknowledge . Since the internet is itself a giant collection of networks and devices and IoT is a part of it, the requirement of wired and wireless connectivity is the heart and soul of IoT. Usage frequency/spectrum is also to be remembered (2.4Hz band is obvious band everywhere). There are spectrum regulations to be followed, based on the country for which the application is being developed. Hence, understanding the connectivity requirements is important.

(e) **Power Requirements-**
All the IoT devices need power. Most of them are battery operated. Even though we now have long-lasting batteries that are economical, however, demand for power is on the rise and hence usage of green power sources like solar/wind should be motivated. If the power requirements are met appropriately, IoT can still be more powerful.

(f) **Complexity Involved-**
IoT is not easy!Why so? It needs a lot of different domains to come together. There is a very limited expertise available in the market. But , the growth is very rapid. The tool kits, software, hardware are not abundant and it needs real skill to build an application. Over the next few years, IoT would get more and more technology experts to work.

(g) **Storage-**
Cloud is becoming mandatory for the data to be stored and analysed. The challenge with respect to this aspect would be connected to the following points:

- Which cloud to use(private, public or hybrid)?
- How to identify service providers?
- How much does it cost?
- Do we really need cloud?

2. **List the security challenges faced by IoT and describe them.**
Security Challenges in IoT:

(a) **Lack of encryption** –
Although encryption is a great way to prevent hackers from accessing data, it is also one of the leading IoT security challenges.
These drives like the storage and processing capabilities that would be found on a traditional computer.
The result is an increase in attacks where hackers can easily manipulate the algorithms that were designed for protection.

(b) **Insufficient testing and updating** –
With the increase in the number of IoT(internet of things) devices, IoT manufacturers

are more eager to produce and deliver their device as fast as they can without giving security too much of although.

Most of these devices and IoT products do not get enough testing and updates and are prone to hackers and other security issues.

(c) **Brute forcing and the risk of default passwords** –

Weak credentials and login details leave nearly all IoT devices vulnerable to password hacking and brute force.

Any company that uses factory default credentials on their devices is placing both their business and its assets and the customer and their valuable information at risk of being susceptible to a brute force attack.

(d) **IoT Malware and ransomware** –

Increases with increase in devices.

Ransomware uses encryption to effectively lock out users from various devices and platforms and still use a user's valuable data and info.

Example –

A hacker can hijack a computer camera and take pictures.

By using malware access points, the hackers can demand ransom to unlock the device and return the data.

(e) **IoT botnet aiming at cryptocurrency** –

IoT botnet workers can manipulate data privacy, which could be massive risks for an open Crypto market. The exact value and creation of cryptocurrencies code face danger from mal-intentioned hackers.

The blockchain companies are trying to boost security. Blockchain technology itself is not particularly vulnerable, but the app development process is.

3. **List the design challenges faced by IoT and describe them**

Design Challenges in IoT:

(a) **Battery life is a limitation** –

Issues in packaging and integration of small-sized chip with low weight and less power consumption. If you've been following the mobile space, you've likely see how every yr it looks like there's no restriction in terms of display screen size. Take the upward thrust of 'phablets', for instance, which can be telephones nearly as huge as tablets. Although helpful, the bigger monitors aren't always only for convenience, rather, instead, display screen sizes are growing to accommodate larger batteries. Computers have getting slimmer, but battery energy stays the same.

(b) **Increased cost and time to market** –

Embedded systems are lightly constrained by cost.

The need originates to drive better approaches when designing the IoT devices in order

to handle the cost modelling or cost optimally with digital electronic components.
Designers also need to solve the design time problem and bring the embedded device at the right time to the market.

(c) **Security of the system** –
Systems have to be designed and implemented to be robust and reliable and have to be secure with cryptographic algorithms and security procedures.
It involves different approaches to secure all the components of embedded systems from prototype to deployment.

4. **List the deployment challenges faced by IoT and describe them**
Deployment challenges in IoT :

(a) **Connectivity** –
It is the foremost concern while connecting devices, applications and cloud platforms. Connected devices that provide useful front and information are extremely valuable. But poor connectivity becomes a challenge where IoT sensors are required to monitor process data and supply information.

(b) **Cross platform capability** –
IoT applications must be developed, keeping in mind the technological changes of the future.
Its development requires a balance of hardware and software functions.
It is a challenge for IoT application developers to ensure that the device and IoT platform drivers the best performance despite heavy device rates and fixings.

(c) **Data collection and processing** –
In IoT development, data plays an important role. What is more critical here is the processing or usefulness of stored data.
Along with security and privacy, development teams need to ensure that they plan well for the way data is collected, stored or processed within an environment.

(d) **Lack of skill set** –
All of the development challenges above can only be handled if there is a proper skilled resource working on the IoT application development.
The right talent will always get you past the major challenges and will be an important IoT application development asset.

5. **Explain the IoT stack with a neat diagram and with appropriate examples for each layer**

There are 7 layers in the IoT stack. From the top they are:

(a) Layer 7 Application layer

(b) Layer 6 User Experience layer

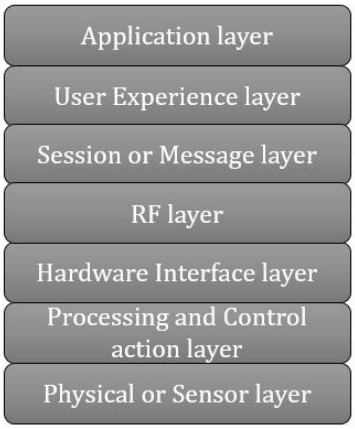


Figure 1.1: IoT stack

(c) Layer 5 Session or Message layer

(d) Layer 4 RF layer

(e) Layer 3 Hardware Interface layer

(f) Layer 2 Processing and Control action layer

(g) Layer 1 Physical or Sensor layer.

IoT Stack Layer 1-Physical or sensor layer:
This layer is concerned about the physical component; temperature sensor, pressure sensor, humidity sensor, etc. can all be referred to as physical layer components. While considering industrial automation, PLC, actuator, etc. are regarded as physical layer components. This layer is responsible for the data collection (i.e. sensing happens here). Choosing appropriate sensor is the challenge in this layer since there are many sensors available in the market, capable of performing the same tasks but, at different costs. Hence, selection of Sensors is pivotal.

IoT Stack Layer 2-Processing and control layer:
This layer is very important, and it comprises the core components for IoT. The microcontrollers or processors stay in this layer and the data is received by the microcontrollers from the sensors. Variety of development kits are available in the market. one can easily spot Arduino, NodeMCU, PIC, ARM development boards. Operating systems play a major role too and Android, IOS, Linux can very well execute the task. The data collected from the sensors are processed here in this layer and to determine if the data is meaningful, Microcontroller should be present.

IoT Stack Layer 3-Hardware Interface layer:
This layer include components or interfaces used for communication such as RS232, RS485, SPI, I2C, CAN, SCI etc. These interfaces are used for serial or parallel communication at

various baud rates in synchronous/asynchronous modes. The above mentioned interface protocols ensure flawless communication.

IoT Stack Layer 4-RF layer:
This radio frequency layer houses RF technologies based on short range or long range and data rate desired by the application of use. The common indoor RF/wireless technologies include Wifi, Bluetooth, Zigbee, Zwave, NFC, RFID etc. The common outdoor RF cellular technologies include GSM/GPRS, CDMA, LTE-M, NB-IoT, 5G etc. RF layer does communication of data using radio frequency based EM waves. There is another technology which uses light waves for data communication. This light based data communication is referred as LiFi.

IoT Stack Layer 5-Session/Message Layer:
This layer deals with various messaging protocols such as MQTT, CoAP, HTTP, FTP (or Secured FTP), SSH etc. It defines how messages are broadcasted to the cloud. Refer architectures of MQTT protocol and CoAP protocol.

IoT Stack Layer 6-User experience layer:
This layer deals with providing best experience to the end users of IoT products. To fulfill this, this layer takes care of rich UI designs with lots of features. Various languages and tools are developed for the design of GUI interface softwares. These include objected oriented and procedure oriented technologies as well database languages (DBMS, SQL) in addition to analytics tools.

IoT Stack Layer 7-Application layer:
Everything comes to perfection at this layer . Application layer talks about the possible applications which can be built with the support of rest of the layers. It can range from a simple automation application to smart city application.

6. **Describe any 6 applications of IoT in everyday life.**

   (a) **Smart Homes**
   One of the best and the most practical applications of IoT, smart homes really take both, convenience and home security, to the next level. Though there are different levels at which IoT is applied for smart homes, the best is the one that blends intelligent utility systems and entertainment together. For instance, your electricity meter with an IoT device giving you insights into your everyday water usage, your set-top box that allows you to record shows from remote, Automatic Illumination Systems, Advanced Locking Systems, Connected Surveillance Systems all fit into this concept of smart homes. As IoT evolves, we can be sure that most of the devices will become smarter, enabling enhanced home security.

   (b) **Smart City**
   Not just internet access to people in a city but to the devices in it as well – that's

what smart cities are supposed to be made of. And we can proudly say that we're going towards realizing this dream. Efforts are being made to incorporate connected technology into infrastructural requirements and some vital concerns like Traffic Management, Waste Management, Water Distribution, Electricity Management, and more. All these work towards eliminating some day-to-day challenges faced by people and bring in added convenience.

(c) **Self-driven Cars**

We've seen a lot about self-driven cars. Google tried it out, Tesla tested it, and even Uber came up with a version of self-driven cars that it later shelved. Since it's human lives on the roads that we're dealing with, we need to ensure the technology has all that it takes to ensure better safety for the passenger and those on the roads.

The cars use several sensors and embedded systems connected to the Cloud and the internet to keep generating data and sending them to the Cloud for informed decision-making through Machine Learning. Though it will take a few more years for the technology to evolve completely and for countries to amend laws and policies, what we're witnessing right now is one of the best applications of IoT.

(d) **IoT Retail Shops**

If you haven't already seen the video of Amazon Go – the concept store from the eCommerce giant, you should check it out right away. Perhaps this is the best use of the technology in bridging the gap between an online store and a retail store. The retail store allows you to go cashless by deducting money from your Amazon wallet. It also adds items to your cart in real-time when you pick products from the shelves.

If you change your mind and pick up another article, the previous one gets deleted and replaces your cart with the new item. The best part of the concept store is that there is no cashier to bill your products. You don't have to stand in line but just step out after you pick up your products from shelves. If this technology is effective enough to fetch more patronage, this is sure to become a norm in the coming years.

(e) **Farming**

Farming is one sector that will benefit the most from the Internet of Things. With so many developments happening on tools farmers can use for agriculture, the future is sure promising. Tools are being developed for Drip Irrigation, understanding crop patterns, Water Distribution, drones for Farm Surveillance, and more. These will allow farmers to come up with a more productive yield and take care of the concerns better.

(f) **Smart Grids**

One of the many useful IoT examples, a smart grid, is a holistic solution that ap-

plies an extensive range of Information Technology resources that enable existing and new gridlines to reduce electricity waste and cost. A future smart grid improves the efficiency, reliability, and economics of electricity.

7. **What is meant by the internet of things and what do you mean by things in IoT? Give the advantages and disadvantages of internet of things.**
   The Internet of Things describes the network of physical objects or "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.
   A thing in the context of the Internet Of Things (IoT), is an entity or a physical object that has a unique identifier, an embedded system and the ability to transfer data over a network.

   Advantages:

   - It can assist in the smarter control of homes and cities via mobile phones. It enhances security and offers personal protection.
   - By automating activities, it saves us a lot of time.
   - Information is easily accessible, even if we are far away from our actual location, and it is updated frequently in real time.
   - Electric Devices are directly connected and communicate with a controller computer, such as a cell phone, resulting in efficient electricity use. As a result, there will be no unnecessary use of electricity equipment.
   - Personal assistance can be provided by IoT apps, which can alert you to your regular plans.
   - It is useful for safety because it senses any potential danger and warns users.For example, GM OnStar, is a integrated device that system which identifies a car crash or accident on road. It immediately makes a call if an accident or crash is found.
   - It minimizes human effort because IoT devices connect and communicate with one another and perform a variety of tasks without the need for human intervention.
   - Patient care can be performed more effectively in real time without the need for a doctor's visit. It gives them the ability to make choices as well as provide evidence-based care.
   - Asset tracking, traffic or transportation tracking, inventory control, delivery, surveillance, individual order tracking, and customer management can all be made more cost-effective with the right tracking system

   Disadvantages:

   - Hackers may gain access to the system and steal personal information. Since we add so many devices to the internet, there is a risk that our information as it can be misused.

- They rely heavily on the internet and are unable to function effectively without it.
- With complexity of systems, there are many ways for them to fail.
- We lose control of our lives—our lives will be fully controlled and reliant on technology.
- Overuse of the Internet and technology makes people unintelligent because they rely on smart devices instead of doing physical work, causing them to become lazy.
- Unskilled workers are at a high risk of losing their jobs, which could lead to unemployment. Smart surveillance cameras, robots, smart ironing systems, smart washing machines, and other facilities are replacing security guards, maids, ironmen, and dry-cleaning services etc.
- It is very difficult to plan, build, manage, and enable a broad technology to IoT framework.

8. **What are the different levels in IoT and describe each level with an application for each level?** Based on the architectural approach, IoT can be classified into 5 level: Level-1 to Level-5

LEVEL-1

It has the minimal complexity involved and is the easiest to build.
The application will have one sensor- a device to sense. It could be the temperature sensor, pressure sensor etc. the data will be stored logically and the data analysis will lso be done locally. monitoring/control can be done through an application(.apk or webapp). This is used for simple applications involving limited or no complexity.data generated in this level application is not huge, that is, not a big data here!. All the control happens through the Internet. A simple example scenario is presented 1.2 where the temperature sensor senses the room temperature and the data is stored and analyzed locally. Based on the analysis the control action can be triggered through mobile application or it can help in monitoring the status.

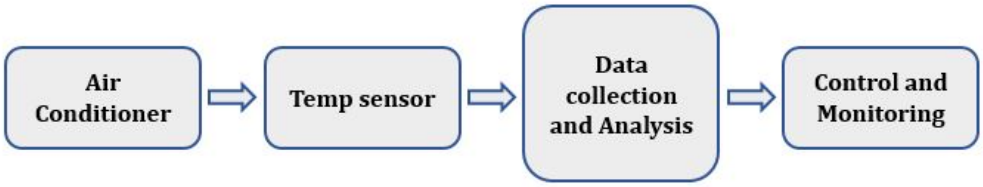


Figure 1.2: Level 1 IoT application

LEVEL-2

The second level is slightly more complex than the previous level. Here, the data is definitely voluminous and hence, cloud storage is preferred. The frequency of the sensing done by the sensor is faster;this means that the sensing happens fast and the number of

times sensing is done shall be much more than Level-1. Analysis is carried out locally. Cloud is meant for storage alone. Based on the data analysis, the control action can be triggered through the web app or mobile application. Some examples could be agriculture applications, room freshening solutions based on odour etc. figure 1.3 shows the Level-2 IoT application to air conditioner. The sensor reads the room temperature, at better pace and rate than Level-1;the data goes on to the cloud for storage. Analysis shall be done locally and the action can be triggered through the mobile app.

Figure 1.3: Level 2 IoT application

LEVEL-3

Here,also, since the data is voluminous, frequency of the sensing done by sensor is faster and is stored on the cloud. The difference here is that the analysis is *carried out on the cloud*. Based on the data analysis , the control action can be triggered through the web app or mobile application as shown in figure 1.4. Some examples are agriculture applications, room freshening solutions based on odour,etc where the analysis of data should happen in the cloud.

Figure 1.4: Level 3 IoT application

LEVEL-4

With every passing level, the volume of data goes up and hence the rate at which it is sensed also increases. At this level multiple nodes are present which are independent of each other. They upload data to the cloud as shown in figure 1.5. All the sensors upload the read sensory inputs. Here, cloud storage is preferred as data is huge. Analysis is also carried out on the cloud and based on the analysis carried out, the control action shall be triggered through a web application or mobile application.

LEVEL-5

At this level, the data is humongous and is sensed much faster. multiple nodes are involved in the applications categorized as Level-5 and these nodes are independent of each other. The sensing of data and its storage is the same as all the previous levels. When an

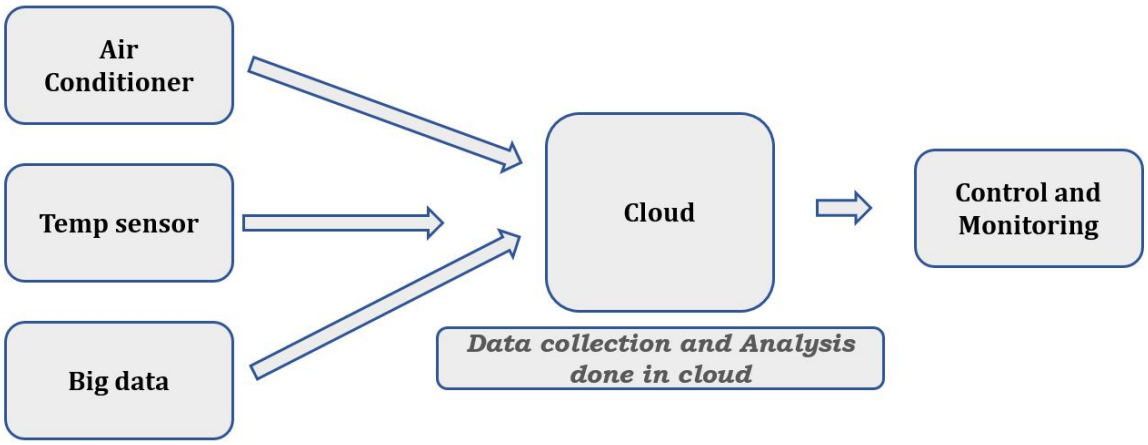


Figure 1.5: Level 4 IoT application

application is completely cloud oriented it is computationally intensive and real time. Based on the data analysis the control action can be triggered through the web app or mobile application as in all other level figure 1.6 shows an example of Level-5 IoT application.

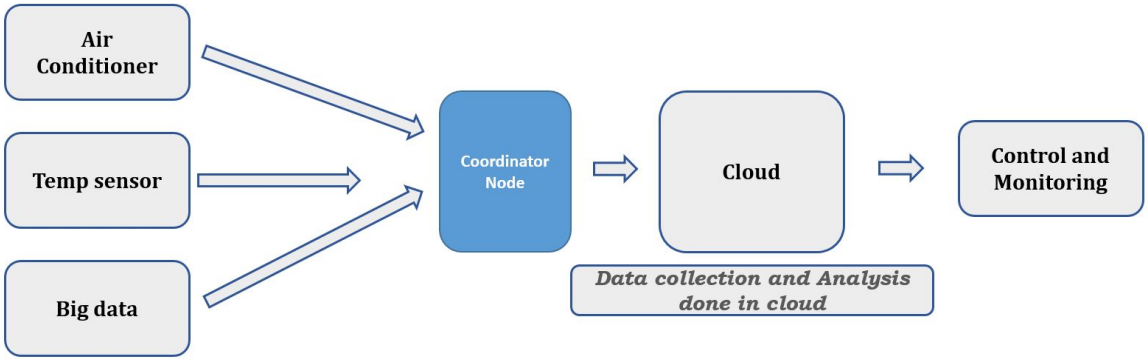


Figure 1.6: Level 5 IoT application

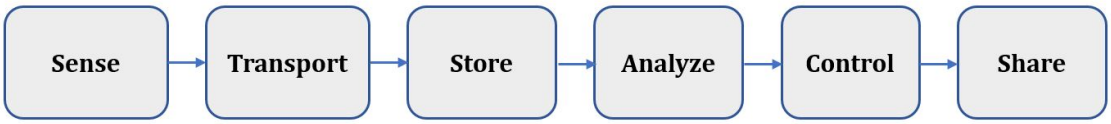


Figure 1.7: IoT in a nutshell

9. **List the different enabling technologies used for IoT design. Give example of different sensors that are used .**

   loT is a collection/group of many technologies and devices. Simplest of sensors, embedded systems (the boards), data analytics, mobile and mobile Internet, security aspects, and

protocols involved, cloud storage (computing), have all become enabling technologies. In general, enabling technologies/devices fall under one of the following sections:

- Technologies that help in acquiring data/sensing data.
- Technologies that help in analysing data/processing data.
- Technologies that help in taking control action.
- Technologies that help in enhancing the security/privacy.

Sensors are devices that detect changes in the environment condition and act accordingly. They detect specific types of conditions (such as light, heat, sound, distance, pressure, presence or absence of gas/liquid, etc.) in the physical world and then generate a signal (usually an electrical signal) as a measure of their magnitude. The different types of sensors in IoT are listed in table 1.1 .

10. **List the different enabling technologies used for IoT design.Give example of big data analytics and list the things it is majorly governed by.**
loT is a collection/group of many technologies and devices. Simplest of sensors, embedded systems (the boards), data analytics, mobile and mobile Internet, security aspects, and protocols involved, cloud storage (computing), have all become enabling technologies. In general, enabling technologies/devices fall under one of the following sections:

- Technologies that help in acquiring data/sensing data.
- Technologies that help in analysing data/processing data.
- Technologies that help in taking control action.
- Technologies that help in enhancing the security/privacy.

Data is everywhere, and from every function or operation we get more data. lo ts all about collecting data from various sensory nodes and handling the huge data ts cardinal to build the application fruitful. The biggest challenge with big data is its volume, the varicly it has, the speed (velocity) i which it comes and finally the veracity. These are fondly referred as the 4Vs of big data. Chapter 6 on data analytics will provide details of big data analytics. Big data is majorly governed by

(a) Scale (Volume): Huge volume of data is generated every minute! Storage has become inexpensive and hence, cost-related challenges have reduced. Cloud storage and hardware storage both have become affordable because of the tremendous growth in the semiconductor industry.

(b) Complexity (Variety): Data no longer comes from one single source. The data comes in different formats (e.g., audio, video, text, image, etc.) and has to be interpreted systematically. This provides a huge challenge.

(c) Speed (Velocity): Velocity is the rate at which new data is being created. The rate at which data is generated is very fast. Also, data dynamics changes very frequents. Nowadays, data can come from anywhere — from fitbit watches to refrigerators. All the data pours in at a very high speed which makes it very challenging to not to miss and oversee the actual data from the noise.

(d) Data in Doubt (Veracity): Veracity is perhaps the one hidden secret of all the data we now rely on. How accurate is all this data anyways. The data's nature alters dynamically and ambiguity is seen (incomplete data). Hence, it would be pretty challenging to process this unstable data.

the data is generated by

(a) Sensors from the security system.

(b) Sensors from weather monitoring system.

(c) Sensors from car/navigation system.

(d) Sensors from water quality monitoring system.

(e) Data from wearable (band).

11. **Describe the different components of IoT.**

An IoT device typically comprises four major components.

(a) **Sensors** –

Much of IoT involves environment adaptability and the major factor contributing to it are the sensors in the IoT devices. Sensors are devices which enable the IoT devices to gather data from its surroundings. Effectively, they may be perceived as instruments which sense the environment and perform multiple tasks. Senors make the IoT devices capable of real world integration. It can be of varied types. From a simple GPS in your phones to the live video feature on a social media platform.

(b) **Connectivity-**

With the advent of cloud computing, devices can be launched on a cloud platform and in the due course, devices can interact freely with each other at a cheaper and more transparent scale. For IoT devices, cloud computing facilitates freedom from exclusive network providers. Instead, small network connection mediums like mobile satellite networks, WAN, Bluetooth etc. are used.

(c) **Data Processing** –

As as soon as the environmental stimuli are gathered by the sensors and transmuted

to the cloud, it is the job of the data processors to process the information collected and perform the required tasks. From adjusting the temperatures of the AC to facial recognition on mobile phones or biometric devices, data processing software are largely responsible for enhancing the automation in IoT devices.

(d) **User Interface** –
The IoT introduced a new paradigm among the available devices for active interaction and engagement. This has transformed the user interface widely. Instead of one-way communication mechanisms of traditional devices, IoT enables cascading effects on end-user commands. This is precisely why IoT devices are all the more communicative and active.

12. **State the difference between IoT and IIoT. IoT (Internet of Things):**
Any device that can connect to the internet and transfer data to a remote data server is termed the Internet of Things (IoT). **IIoT (Industrial Internet of Things):**
In the case of IoT devices used for industrial purposes, these devices are referred to as Industrial Internet of Things (IIoT). IIoT is the subset of IoT. The comparision is shown in table 1.2

13. **State difference between Arduino and Raspberry Pi.**
We can use many different kinds of controller boards for our hardware projects. Arduino and Raspberry Pi are among the most popular. Difference between Arduino and Raspberry Pi is shown in table 1.3

14. **Explain IoT Protocols. Name some of the popular IoT Protocols.**
IoT protocols are a set of rules that guide how data gets sent to the internet. They ensure optimum security to the data being exchanged between connected IoT devices.
Some of the popular IoT protocols are shown in table 1.4.

15. **List the different enabling technologies used for IoT design. Give example of popular Embedded computing boards that you used in LAB and compare them.**
Internet of Things is system of internet connected devices having unique identification. They are capable of collecting data from environment and transferring it through the network without any human intervention. There is a need of improved technology which can be achieved by integration of various enabling technologies with help of which the devices can be identified and made to communicate with one another. The technologies which contributed in development of IoT are

(a) Hardware
   i. (RFID) radio frequency identification
   ii. Internet protocol
   iii. Wireless fidelity (Wi-Fi)
   iv. Bluetooth
   v. Zigbee
   vi. Near Field Communication
   vii. Actuators
   viii. Wireless sensor networks

(b) Software
   i. *Middleware* : Middleware includes application servers, web servers, content management systems and analogous related tools which supports development of application and delivery. Middle ware creates a framework which allows sharing of data across various distributed devices, locations applications
   ii. *Browsing and searching* : IoT enabled devices are dynamic, mobile and generates huge amount of periodically changing data and information. There is a need for an IoT browser which has the capability of identifying smart things or devices

(c) Architecture Architectures are required for representing, organizing and structuring IoT so as to function very efficiently

Popular IOT boards Used in LAB

Arduino is a platform that offers easy-to-use hardware and software to create electronics projects. It has a micro-controller (physical programmable circuit board) and a piece of software that can be used to write and upload computer code to the physical board. Arduino boards read inputs like a light on a sensor and turn them into an output like activating a motor.
Some of the features of Arduino are:

- Cross-platform – The Arduino IDE is designed to run on different operating systems, like Windows, mac OS, and Linux.
- Open source and extensible software and hardware.
- Easy-to-use for beginners.
- Inexpensive compared to other micro-controller platforms.

NodeMCU is an open source platform based on ESP8266 which can connect objects and let data transfer using the Wi-Fi protocol. In addition, by providing some of the most important features of microcontrollers such as GPIO, PWM, ADC, and etc, it can solve many of the project's needs alone

Some of the features of Node MCU board are:

- NodeMCU has 16 general purpose input-output pins on its board.
- NodeMCU has four pins available for SPI communication.
- NodeMCU has two UART interfaces, UART0 (RXD0 TXD0) and UART1 (RXD1 & TXD1). UART1 is used to upload the firmware/program
- NodeMCU has 128 KB RAM and 4MB of Flash memory to store data and programs. Its high processing power with in-built Wi-Fi / Bluetooth and Deep Sleep Operating features make it ideal for IoT projects.
- Inexpensive compared to other micro-controller platforms.

Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse.

Some of the features of Raspberry Pi board are:

- The Raspberry Pi is a very cheap computer that runs Linux, but it also provides a set of GPIO (general purpose input/output) pins, allowing you to control electronic components for physical computing and explore the Internet of Things (IoT).
- The Raspberry Pi operates in the open source ecosystem: it runs Linux (a variety of distributions), and its main supported operating system, Pi OS, is open source and runs a suite of open source software.
- 4 GB and 8 GB of RAM available.
- 4 usb ports available
- Audiojack available, hdmi output available.

Table 1.1: List of Sensors and their functions

Sensor	Function
Temperature sensor	Measures the amount of heat energy in a source.Detects temperature changes and converts them into data. LM35 is a temperature sensor that outputs an analog signal which is proportional to the instantaneous temperature. The output voltage can easily be interpreted to obtain a temperature reading in Celsius. The advantage of lm35 over thermistor is it does not require any external calibration.
Proximity sensor	It is responsible for the non-contact detection of objects near the sensor. Proximity Sensors detect an object without touching it, and they therefore do not cause abrasion or damage to the object. Devices such as limit switches detect an object by contacting it, but Proximity Sensors are able to detect the presence of the object electrically, without having to touch it.
Pressure sensor	A pressure sensor is a device or instrument which is able to measure the pressure in gases or liquids. A pressure sensor consists of a pressure-sensitive element which can determine the pressure being applied and components to convert the information into an output signal.
Humidity sensor	Measure the amount of water vapor in the atmosphere of air or other gases.
Motion detection sensor	It detects the physical movement (motion) in a given area and transforms motion into an electric signal. Motion sensors are like flashlights sending out a beam of light but with motion-detecting infrared energy waves instead of light waves. Just like a light is brighter closer to the bulb, the infrared radiation is denser nearer to the device and it spreads out farther away.
Optical Sensor	Measures a physical quantity of light and converts rays of light into electrical signals.
Smoke sensor	It detects smoke (airborne particulates and gases) and its level.
Accelerometers	Measures an object's linear acceleration based on vibration.
Gyroscope	It measures an angular position based on the principle of the rigidity of space.
Infrared sensor	It detects characteristics in the surroundings by either emitting or detecting infrared radiation.
Gas sensor	It monitors changes in the air quality and detects the presence of various gases.

Table 1.2: Comparison of IOT and IIOT

IIoT	**IoT**
It supports industrial-oriented applications such as manufacturing, power plants, oil and gas, etc.	It supports customer-oriented applications such as wearables to robots and machines.
The focus is on large scale networks.	The focus is on small scale networks.
Both wired and wireless communication methods are utilized.	Typically, wireless communication methods are utilized.
A large amount of data is handled.	It can handle data ranging from medium to high.
This is a B2B (business-to-business) and is designed to increase efficiency and safety at production facilities.	This is B2C (business-to-consumer) and is designed to make the lives of consumers more convenient.

Table 1.3: Comparison of Arduino and Raspberry pi

Arduino	**Raspberry Pi**
Arduino is an open-source, programmable USB microcontroller.	It is a microprocessor-based minicomputer (SBC single-board computer).
Arduino boards have a microcontroller that includes a CPU, RAM, and ROM. The Arduino Board has additional hardware for power supply, programming, and IO (Input/Output) connectivity.	The Raspberry Pi SBC (Single board computer) comes with everything you need to run a computer, from a processor, memory, storage, graphics driver, to connectors.
With Arduino, you can interface sensors and actuators.	With raspberry too you can interface sensors and actuators .
It has a simple hardware and software architecture.	On the other hand, Raspberry Pi boards have a complex architecture.
Arduino boards are programmable using C/C++ languages.	Raspberry Pi supports its own Linux-based operating system Raspberry Pi OS. You can also install the OS you like.It works well for developing Python-based applications.
It is used to run one single task at a time.	It can perform several tasks at once such as running software, web browsing, doing programming, etc..

Table 1.4: Layers and their Protocols

Layer	**Protocol**
Application layer	• Advanced Message Queuing Protocol (AMQP) • Message Queue Telemetry Transport (MQTT) • Constrained Application Protocol (CoAP)
Transport layer	• User Datagram Protocol (UDP) • Transmission Control Protocol (TCP)
Network layer	• 6LoWPAN(IPv6 over Low-Power Wireless Personal Area Networks) • IP
Datalink layer	• LPWAN • IEEE 802.15.4 low-rate wireless personal area network (LR-WPAN).
Physical layer	• Near field communication (NFC) • Radio frequency identification (RFID) • Bluetooth Low Energy (BLE) • Ethernet

2. Introduction to Sensors

2.1 Syllabus

1. Introduction to Sensor Interfacing
2. Types of Sensors
    - MQ-02/05-Gas sensor interfacing with NodeMCU/Arduino
    - Interfacing the Obstacle sensor
    - Interfacing the Heartbeat sensor
    - Interfacing the Ultrasonic sound sensor
    - Interfacing the Gyro sensor
    - Interfacing the LDR sensor
    - Interfacing the GPS
    - Interfacing the colour sensor
    - Interfacing the pH sensor
3. Controlling Sensors through webpage
    - Controlling LED with a webpage
4. Microcontrollers: A Quick Walkthrough
    - 8051:An architectural view
    - 8051:Family details
    - Registers in 8051 Microcontroller
    - Special function registers

2.2 Short Answer Questions

1. **Mention the importance of sensors in IoT applications with appropriate examples**
   The main purpose of sensors is to collect data from the surrounding environment. Sensors, or 'things' of the IoT system, form the front end. These are connected directly or indirectly to IoT networks after signal conversion and processing

   - Position Sensors
   - Pressure Sensors
   - Temperature Sensors
   - Force Sensors
   - Vibration Sensors
   - Piezo Sensors
   - Fluid Property Sensors
   - Humidity Sensor
   - Photo Optic Sensors

2. **Draw the pin diagram of the MQ 02/05 sensor and explain its working principle?**
   MQ2 gas sensor is an electronic sensor used for sensing the concentration of gases in the air such as LPG, propane, methane, hydrogen, alcohol, smoke and carbon monoxide. The Pin diagram of MQ 02/05 sensor is shown in figure 2.1. **Working** This sensor contains a

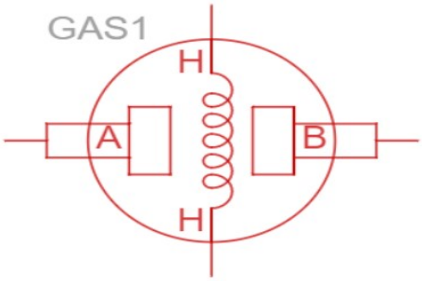


Figure 2.1: Pin diagram of Gas sensor

sensing element, mainly aluminium-oxide based ceramic, coated with Tin dioxide, enclosed in a stainless steel mesh. Sensing element has six connecting legs attached to it. Two leads are responsible for heating the sensing element, the other four are used for output signals.

Oxygen gets adsorbed on the surface of sensing material when it is heated in air at high temperature. Then donor electrons present in tin oxide are attracted towards this oxygen, thus preventing the current flow.

When reducing gases are present, these oxygen atoms react with the reducing gases thereby decreasing the surface density of the adsorbed oxygen. Now current can flow through the sensor, which generated analog voltage values. These voltage values are measured to know the concentration of gas. Voltage values are higher when the concentration of gas is high

3. **Explain the working of pH sensor using an application?**
   A pH meter is a scientific instrument that measures the hydrogen-ion activity in solutions , indicating acidity and basicity expressed as pH value.
   Working
   An acidic solution has far more positively charged hydrogen ions in it than an alkaline one, so it has greater potential to produce an electric current in a certain situation. In other words, it's a bit like a battery that can produce a greater voltage. A pH meter takes advantage of this and works like a viltmeter: it measures the voltage (electrical potential) produced by the solution whose acidity we're interested in, compares it with the voltage of a known solution, and uses the difference in voltage (the "potential difference") between them to deduce the difference in pH.The pin diagram is shown in figure 2.2.

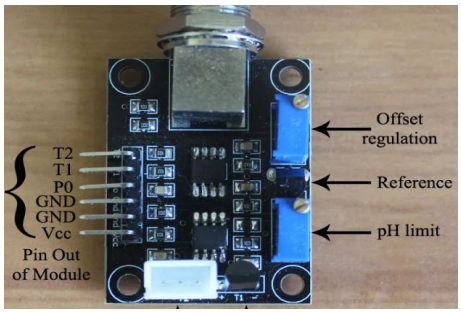


Figure 2.2: Pin diagram of pH sensor

- Vcc = Positive Power supply pin
- GND = Power supply Ground
- GND = Analog Sensor GND
- P0 = PH output pin (Analog Pin)
- T1 = Output pin of onboard temp. sensor LM35 (Analog Pin)
- T2 = Output pin of DS18B20 waterproof temp. sensor (Digital Pin)

Application

- In agriculture industries, it is used to measure the pH of soil.
- It is also used to measure water quality for municipal water supplies, swimming pools.
- In many chemical and pharmaceutical industries, it is used to measure the pH value of solutions.

- pH Meter is additionally employed in the Food industry particularly for dairy products like cheese, curds, yogurts, etc.

4. **Explain the working principle of an obstacle Sensor using an application?**

   Working

   The photo-diode's resistance and output voltage change in proportion to the IR light received. This is the underlying working principle of the IR sensor. When the IR transmitter emits radiation, it reaches the object and some of the radiation reflects back to the IR receiver

   Application

   IR sensos uses in radiation thermometers to measure the temperature depend upon the temperature and the material of the object and these thermometers have some of the following features

   - Measurement without direct contact with the object
   - Faster response
   - Easy pattern measurements

5. **Mention a few differences between microprocessor and microcontroller ?**

Table 2.1: Comparision of Microprocessor and Microcontroller

Microprocessor	**Microcontroller**
Microprocessor consists of only a Central Processing Unit	Micro Controller contains a CPU, Memory, I/O all integrated into one chip.
The microprocessor is useful in Personal Computers	Micro Controller is useful in an embedded system.
The microprocessor uses an external bus to interface to RAM, ROM, and other peripherals	Microcontroller uses an internal controlling bus.
Microprocessors are based on Von Neumann model	Microcontrollers are based on Harvard architecture.

6. **List the registers in Intel 8051 microcontroller?** Registers are a type of computer memory used to quickly accept, store, and transfer data and instructions that are being

used immediately by the CPU. Registers are used in the CPU to store information on temporarily basis which could be data to be processed, or an address pointing to the data which is to be fetched. In 8051, there is one data type is of 8-bits, from the MSB (most significant bit) D7 to the LSB (least significant bit) D0. With 8-bit data type, any data type larger than 8-bits must be broken into 8-bit chunks before it is processed.

The most widely used registers of the 8051 are A (accumulator), B, R0-R7, DPTR (data pointer), and PC (program counter). All these registers are of 8-bits, except DPTR and PC.

7. **Draw the structure of current program status register of Intel 8051 micro controller?**

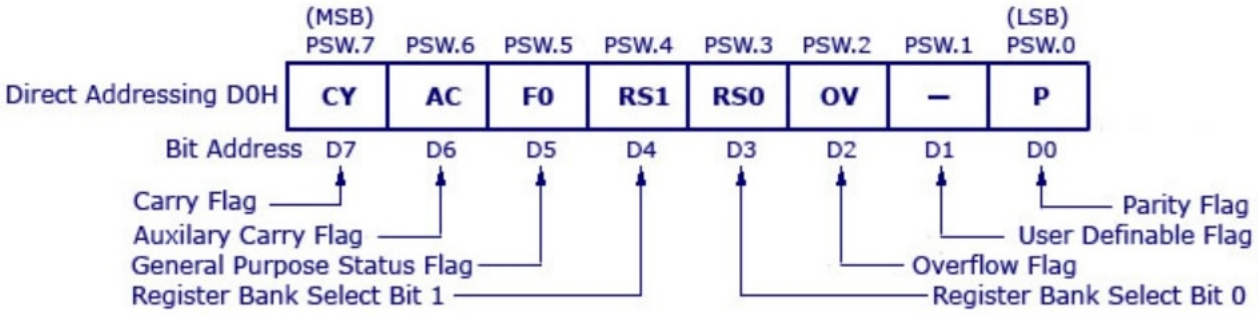


Figure 2.3: structure of current program status register of Intel 8051 micro controller

8. **List the applications of LDR Sensor?**

   - The LDR is used in the infrared astronomy
   - The LDR is used in light failure alarm circuits and used in light meter.
   - The LDR used in smoke detectors.
   - It is used for automatic contrast and brightness control in television receivers.
   - It is used in photosensitive relay
   - It is used in optical coding.
   - It is used in street light control circuits
   - It is used in camera light meters
   - It is used in the security alarm.
   - It is used as a proximity switch.
   - It is used in light activated control circuits

9. **Draw the pin diagram of the Obstacle sensor and explain its working principle?**
   Working Principle The principle of an IR sensor working as an Object Detection Sensor

can be explained using the following figure. An IR sensor consists of an IR LED and an IR Photodiode; together they are called as Photo – Coupler or Opto – Coupler. When the IR transmitter emits radiation, it reaches the object and some of the radiation reflects back to the IR receiver. Based on the intensity of the reception by the IR receiver, the output of the sensor is defined.

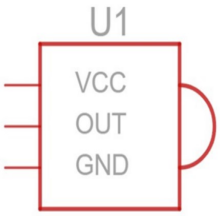


Figure 2.4: Pin diagram of obstacle sensor

10. **Draw pin diagram of PIR and ultrasonic sensor and explain working of the same?**

PIR sensor is specially designed to detect such levels of infrared radiation. It basically consists of two main parts: A Pyroelectric Sensor and A special lens called Fresnel lens which focuses the infrared signals onto the pyroelectric sensor.

A Pyroelectric Sensor actually has two rectangular slots in it made of a material that allows the infrared radiation to pass. Behind these, are two separate infrared sensor electrodes, one responsible for producing a positive output and the other a negative output. The reason for that is that we are looking for a change in IR levels and not ambient IR levels. The two electrodes are wired up so that they cancel each other out. If one half sees more or less IR radiation than the other, the output will swing high or low.

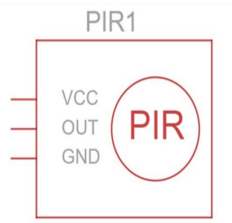


Figure 2.5: Pin diagram of Ultrasonic Sensor

2.3 Long Answer Questions

1. **Draw the architecture of intel 8051 microcontroller and explain?**

8051 microcontroller is designed by Intel in 1981. It is an 8-bit microcontroller. It is built with 40 pins DIP (dual inline package), 4kb of ROM storage and 128 bytes of RAM storage, 2 16-bit timers. It consists of are four parallel 8-bit ports, which are programmable as well as addressable as per the requirement. An on-chip crystal oscillator is integrated in the microcontroller having crystal frequency of 12 MHz.
Let us now discuss the architecture of 8051 Microcontroller.

In the following diagram, the system bus connects all the support devices to the CPU. The system bus consists of an 8-bit data bus, a 16-bit address bus and bus control signals. All other devices like program memory, ports, data memory, serial interface, interrupt control, timers, and the CPU are all interfaced together through the system bus

CPU (Central Processing Unit): CPU act as a mind of any processing machine. It synchronizes and manages all processes that are carried out in microcontroller. User has no power to control the functioning of CPU. It interprets the program stored in ROM and carries out from storage and then performs it projected duty. CPU manage the different types of registers available in 8051 microcontroller.

Interrupts: Interrupts is a sub-routine call that given by the microcontroller when some other program with high priority is request for acquiring the system buses the n interrupts occur in current running program.

Interrupts provide a method to postpone or delay the current process, performs a subroutine task and then restart the standard program again.
Memory: For operation Micro-controller required a program. This program guides the microcontroller to perform the specific tasks. This program installed in microcontroller required some on chip memory for the storage of the program.

Microcontroller also required memory for storage of data and operands for the short duration. In microcontroller 8051 there is code or program memory of 4 KB that is it has 4 KB ROM and it also comprise of data memory (RAM) of 128 bytes.

Bus : Bus is a group of wires which uses as a communication canal or acts as means of data transfer. The different bus configuration includes 8, 16 or more cables. Therefore, a bus can bear 8 bits, 16 bits all together.

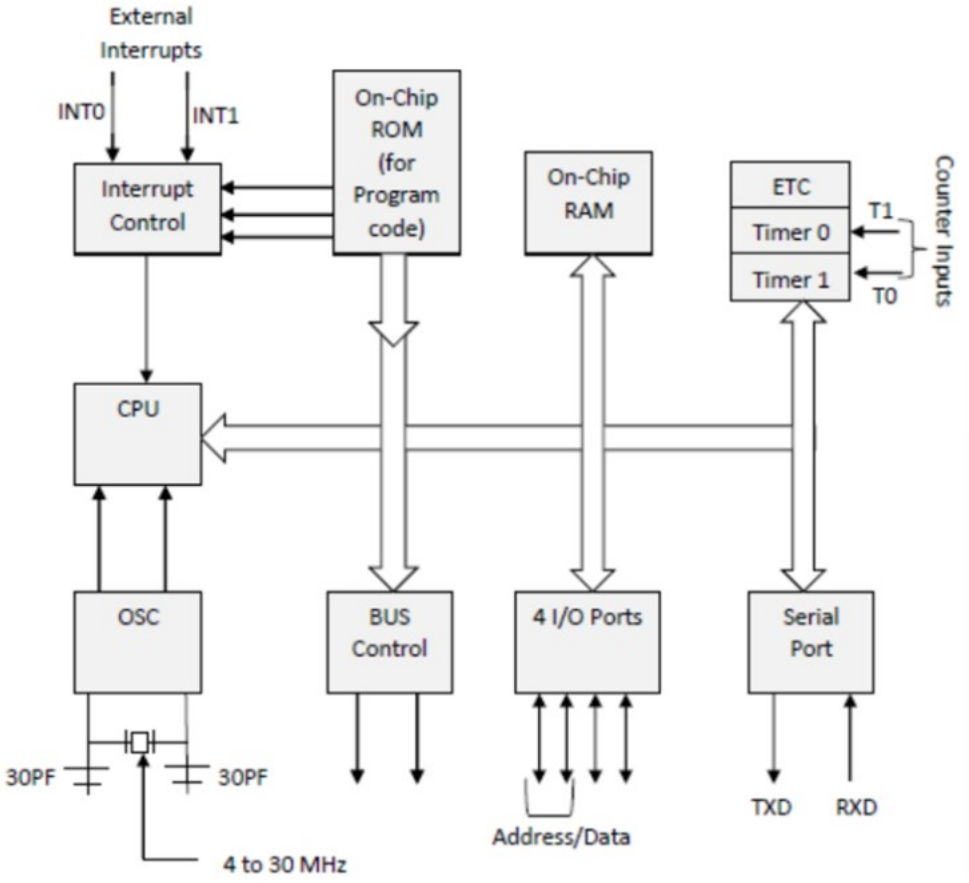


Figure 2.6: Architecture of 8051 microcontroller

Types of buses in 8051 Microcontroller:

- Address Bus: 8051 microcontrollers is consisting of 16 bit address bus. It is generally be used for transferring the data from Central Processing Unit to Memory.
- Data bus: 8051 microcontroller is consisting of 8 bits data bus. It is generally be used for transferring the data from one peripherals position to other peripherals.

Oscillator: As the microcontroller is digital circuit therefore it needs timer for their operation. To perform timer operation inside microcontroller it required externally connected or on-chip oscillator. Microcontroller is used inside an embedded system for managing the function of devices. Therefore, 8051 uses the two 16 bit counters and timers. For the

operation of this timers and counters the oscillator is used inside microcontroller.

2. **Mention clearly the procedure to interface temperature sensor with any microcontroller of your choice. Draw the circuit diagram and explain?**
The LM35 series are precision integrated-circuit temperature devices with an output voltage linearly proportional to the Centigrade temperature. The LM35 device has an advantage over linear temperature sensors calibrated in Kelvin, as the user is not required to subtract a large constant voltage from the output to obtain convenient Centigrade scaling.

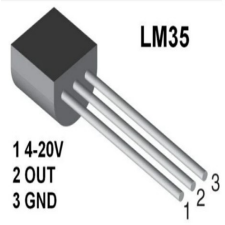


Figure 2.7: Temperature Sensors

Prodedure

To build the temperature sensor with Arduino Uno, follow the steps below:

- Connect Arduino Uno GND to LM35 GND
- Connect Arduino 5V pin to LM35 pin 1
- Connect Arduino Uno Analog Pin 0 to LM35 pin OUT

Schematic diagram

The schematic diagram of gas sensor with Arduino uno board is shown in figure 2.8.

Program and Read the sensor

```
float tempraw,tempmv,tempc;
int tempinput=A0;
void setup(){
    Serial.begin(9600);}
void loop(){
  tempraw = analogRead(tempinput);
  tempmv = tempraw*5000/1024;
  tempc = (tempmv/10)+(-50);
  Serial.print("temp:");
  Serial.print(tempc);
```

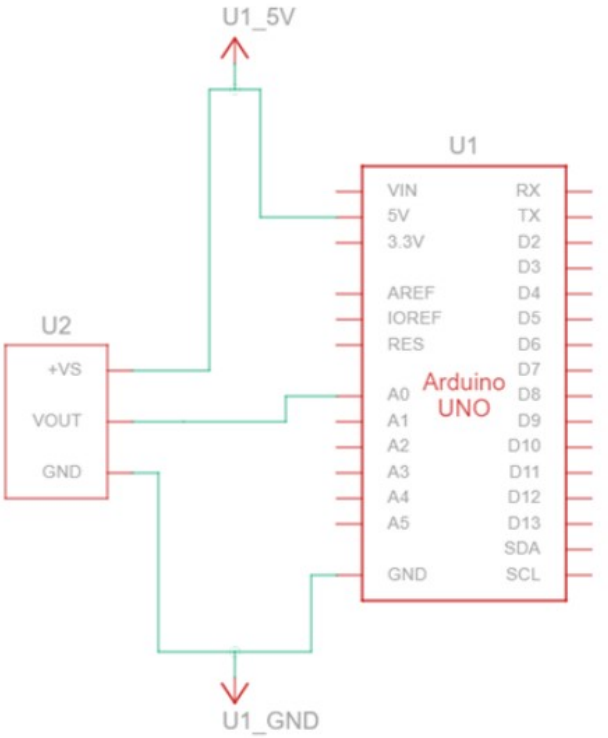


Figure 2.8: Schematic diagram of interfacing temperature sensor with arduino uno

```
  Serial.println("*C");
  delay(1000);
}
```

3. List the intel 8051 registers and their functions in brief?

The 8051 microcontroller contains mainly two types of registers:

- General-purpose registers (Byte addressable registers)
- Special function registers (Bit addressable registers

General Purpose Registers The general-purpose memory is called as the RAM of the 8051 microcontrollers, which is divided into 3 areas such as banks, bit-addressable area, and scratch-pad area. The banks contain different general-purpose registers such as R0-R7, and all such registers are byte-addressable registers that store or remove only 1-byte of data.

Banks and Registers The B0, B1, B2, and B3 stand for banks, and each bank contains eight general-purpose registers ranging from 'R0' to 'R7'. All these registers are byte-addressable. Data transfer between general-purpose registers to general-purpose registers is not possible. These banks are selected by the Program Status Word (PSW) register.

PSW (Program Status Word) Registe The PSW register is a bit and byte-addressable register. This register reflects the status of the operation that is carried out in the controller.

The PSW register determines bank selection by an RS1 and RS0, as shown below. The physical address of the PSW starts from D0h and the individual bits are accessed with D0h to D7h.

Special Function Registers (SFR) Special function registers are upper RAM in the 8051 microcontrollers. These registers contain all peripherally related registers like P0, P1, P2, P3, timers or counters, serial port, and interrupts-related registers. The SFR memory address starts from 80h to FFh. The SFR register is implemented by bit-address registers and byte-address registers.

Accumulator The accumulator which is also known as ACC or A is a bit as well as a byte-addressable register by an address of the accumulator. If you want to use a bit-addressable register, you can use a single bit (E0) of the register and you can use an 8-bit of the accumulator as a byte-addressable register. The accumulator holds the results of most Arithmetic and logical operations.

B-Register The B-register is a bit and byte-addressable register. You can access 1-bit or all 8-bits by a physical address F0h. Suppose to access a bit 1, we have to use f1. The B register is only used for multiplication and division operations.

Port Registers The 8051 microcontroller consists of 4-input and output ports (P0, P1, P2, and P3) or 32-I/O pins. Each pin is designed with a transistor and P registers. The pin configuration is very important for a microcontroller that depends on the logic states of the registers. The pin configuration as the input given by 1 or output 0 depends on the logic states. If logic 1 is applied to the bit of the P register, the output transistor switches off the appropriate pin that acts as an input pin.

Counters and register The 8051 microcontroller consists of two 16-bit timers and counters such as timer 0 and timer 1. Both the timers consist of a 16-bit register in which the lower byte is stored in the TL and the higher byte is stored in the TH. The Timer can be used as a counter as well as for timing operation that depends on the source of the clock pulses to the counters. The Counters and Timers in 8051 microcontrollers contain two special function registers: TMOD (Timer Mode Register) and TCON (Timer Control Register), which are used for activating and configuring timers and counters.

Shift Register Shift registers are a type of sequential logic circuits that are mainly used for the storage of digital data. The shift registers are bit-addressable registers that store only one bit of data.

4. **Assume you have a fan at home. You wish to control the on off switch via the internet. Design a system for its control. Draw the system architecture?**
Design the circuit, use Nodemcu or Arduino with ESP 8266, use thinger.io or thinkspeak website. Try Yourself.

5. Draw the pin diagram of the MQ 02/05 sensor and Arduino board. Connect them. Write a program to sense presence of gas and beep a buzzer if gas is detected.

(a) The pin diagram of gas sensor is shown in figure 2.9.

(b) The schematic diagram of gas sensor with Arduino uno board is shown in figure 2.10.

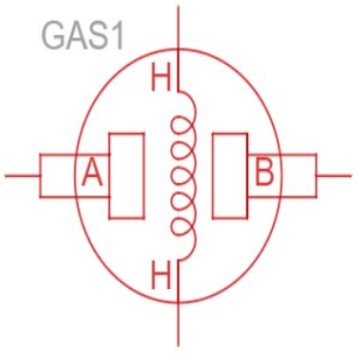


Figure 2.9: Pin diagram of gas sensor

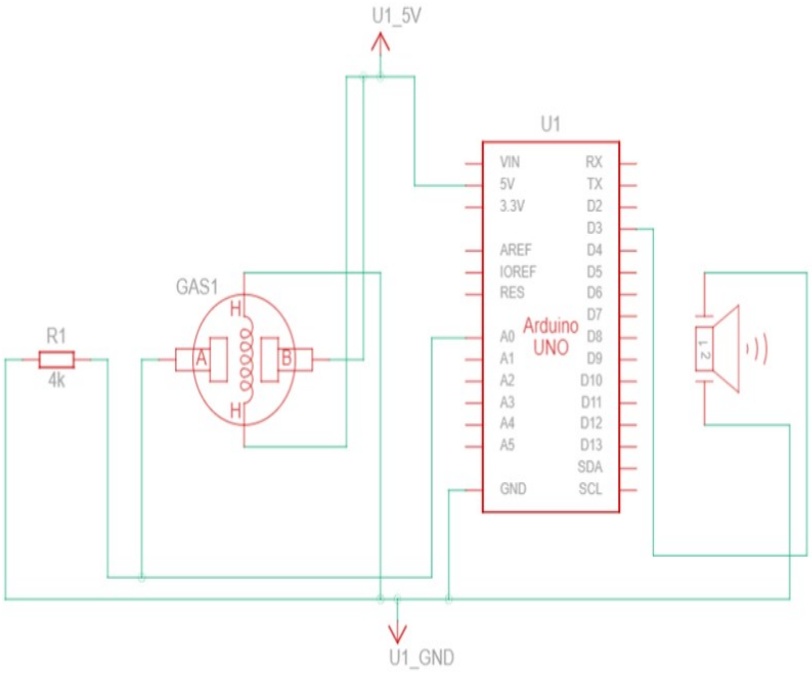


Figure 2.10: Schematic diagram of interfacing MQ 02/05 sensor and Arduino board with a buzzer

Program Code

```
int led=13;
int BUZZ=3;
```

```
const int gas =A0;
void setup() {
  pinMode(LED,OUTPUT);
  pinMode(BUZZ,OUTPUT);
}
void loop() {
  float sensorValue,MQ2pin;
  sensorValue=analogRead(MQ2pin);
  if(sensorValue<=470){
    digitalWrite(LED,HIGH);
    digitalWrite(BUZZ,HIGH);
}
else{
    digitalWrite(LED,LOW);
    digitalWrite(BUZZ,HIGH);
}
delay(500);
return (analogRead(pin));
}
```

6. **Draw the pin diagram of the Obstacle sensor and Arduino board. Connect them. Write a program to sense presence of obstacle and beep a buzzer if obstacle is detected**

Pin diagram of obstacle sensor

The pin diagram of obstacle sensor is shown in figure 2.11. **Schematic diagram**

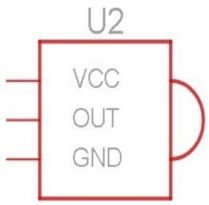


Figure 2.11: Pin diagram of obstacle sensor

The circuit schematic diagram of obstacle sensor is shown in figure 2.12.

Program Code

```
int pinir = 5;
int pinbuzz = 7;
```

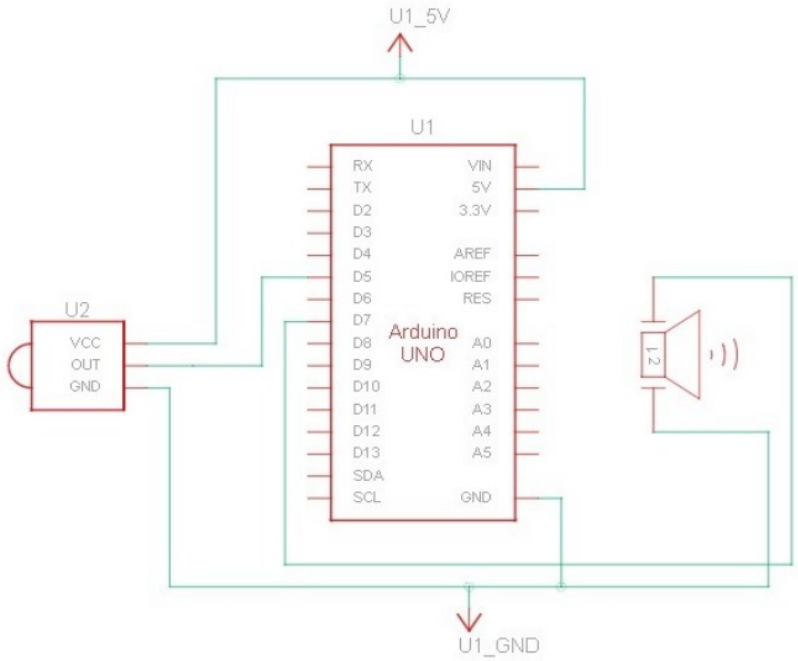


Figure 2.12: Schematic diagram of interfacing obstacle sensor and Arduino board with a buzzer

```
void setup() {
  pinMode(pinbuzz,OUTPUT);
  pinMode(pinir,INPUT);
}
void loop(){
  if(digitalRead(pinir)==1){
    tone(pinbuzz,1000);}
  else{
    noTone(pinbuzz);}
delay(1000);
}
```

7. Draw the pin diagram of the Ultrasonic sensor(HC SR 04) and Arduino board. Connect them. Write a program to sense distance of an obstacle and beep a buzzer if obstacle is too near.

Pin diagram of obstacle sensor

The pin diagram of ultrasonic sensor is shown in figure 2.13.

Schematic diagram

The schematic diagram of interfacing ultrasonic sensor with arduino uno board is shown in figure 2.14.

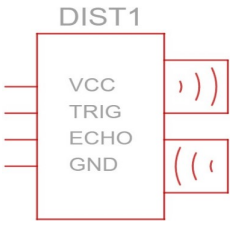


Figure 2.13: Pin diagram of ultrasonic sensor

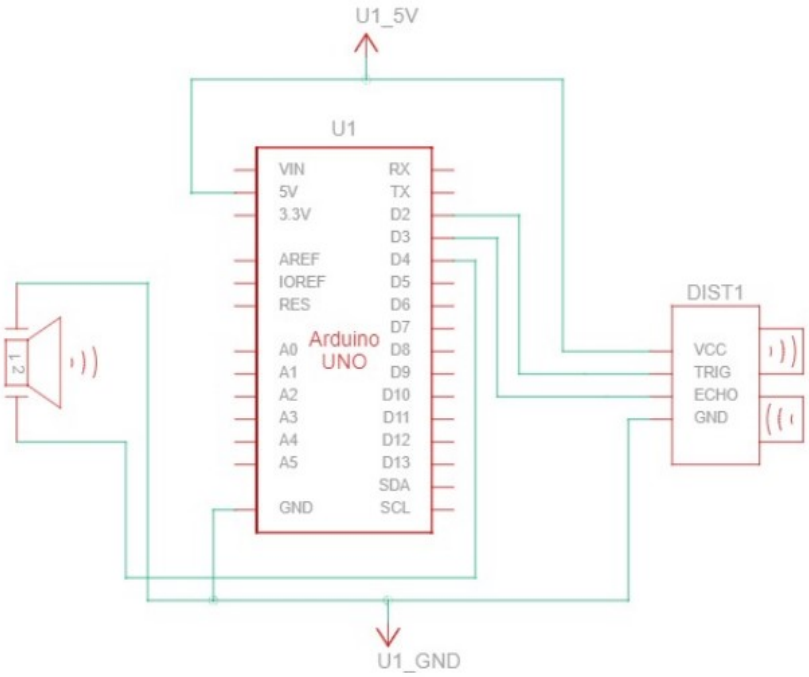


Figure 2.14: Schematic diagram of interfacing ultrasonic sensor and Arduino board with a buzzer

Program Code

```
int trigger = 2;
int echo = 3;
int buzzer = 4;
int time;
int distance;
void setup() {
  pinMode (trigger, OUTPUT);
  pinMode (echo, INPUT);
  pinMode (buzzer, OUTPUT);
  Serial.begin (9600);
}
void loop() {
```

```
  digitalWrite (trigger, HIGH);
  delayMicroseconds (10);
  digitalWrite (trigger, LOW);
  time = pulseIn (echo, HIGH);
  distance = (time * 0.034) / 2;
  if (distance <= 50){
    digitalWrite (buzzer, HIGH);
    Serial.println (" Obstruction is detected. ");
    print (" Distance= ");
    Serial.println (distance);
    delay (500);
}
  else {
    digitalWrite (buzzer, LOW);
    Serial.println (" There is no obstruction detected. ");
    Serial.print (" Distance= ");
    Serial.println (distance);
    delay (500);
}
}
```

8. **Draw the pin diagram of the LDR sensor and NODE mCU. Connect them. Write a program to sense Intensity of light and glow a LED if light intensity is too low. List the procedures that has to be followed for accessing these components using webpages (Assume thinger.io is used).**

   (a) The circuit diagram of nodemcu with LDR sensor and LED is shown in figure 2.15.

   Procedure

   - create a new account in www.thinger.io
   - login with your account
   - connect NodeMcu in the usb port
   - click on devices and click on add device
   - Give the following information
     - Device Type: Generic Thinger Device
     - Device ID: MyNodeMcu(Note: you can give any name)
     - Device Description: LED control
     - Click on Generate random credentials

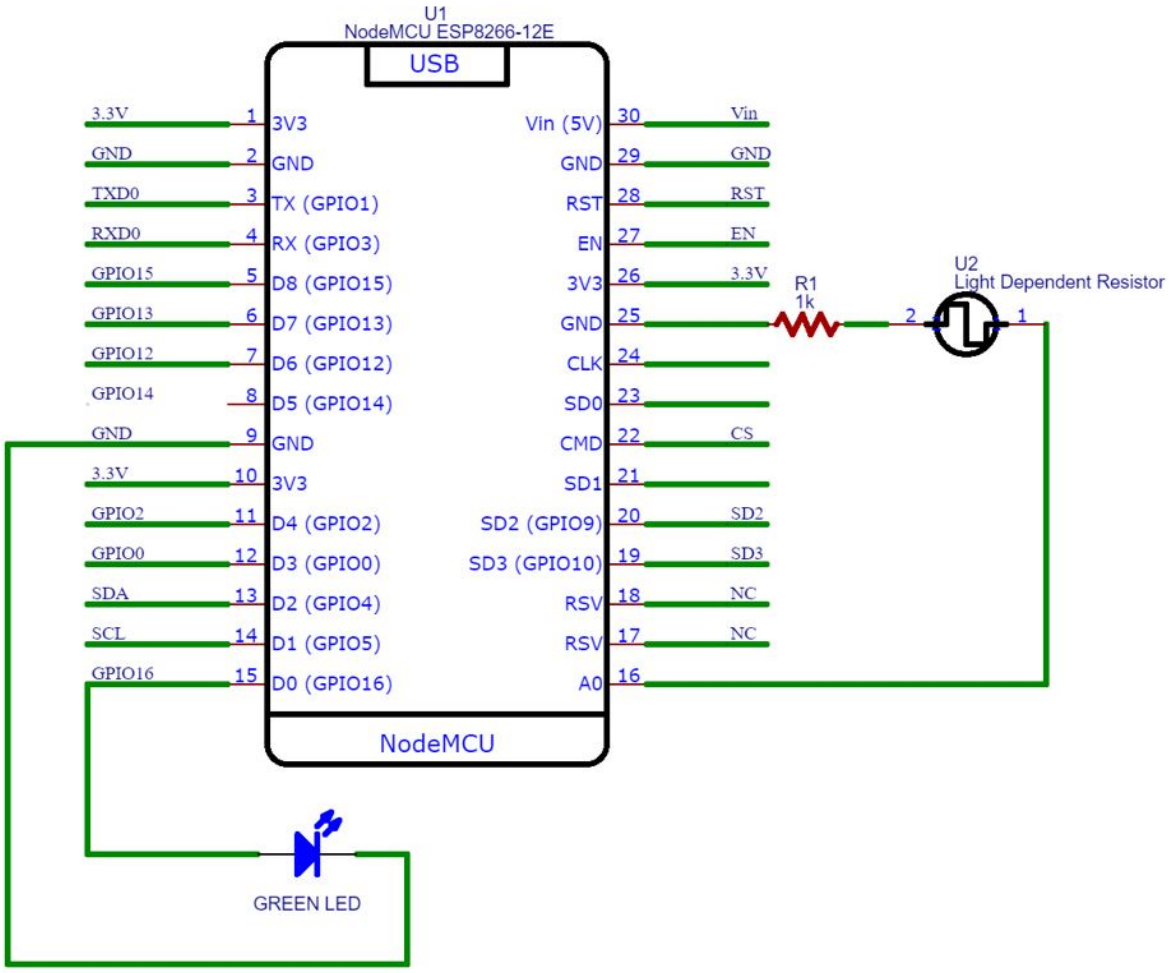


Figure 2.15: circuit diagram of interfacing ldr sensor with nodemcu

- Click add device Now your device is registered
- Open Arduino IDE
- Install thinger.io library
- Type thinger.io and install
- Once the library installed,go to NodeMcu
- Enter device id, device credentials from thinger.io and your Wi-Fi settings SSID(Wi-Fi name) and Wi-Fi password
- Select the board and select com, port and upload sketch.
- Press upload
- Press live transmission button
  You will be observing the transmission and received data and the device status online.
- go to device you can observe the device connected.

- Go to dashboard to create your controls with widgets
- Add dashboard
- Press led
- Press right corner switch to add widgets control
- Add widget and provide information
- Select type
- Press save

Program code

```
#include <ThingerESP8266.h>

#define USERNAME "DeviPrasad"
#define DEVICE_ID "DPNMCU"
#define DEVICE_CREDENTIAL "1556551"

#define SSID "Mi_A2"
#define SSID_PASSWORD "12344321"
ThingerESP8266 thing(USERNAME, DEVICE_ID, DEVICE_CREDENTIAL);

int value=0;
void setup()
{
Serial.begin(9600);
pinMode(D0, OUTPUT);
pinMode(A0, INPUT);

thing.add_wifi(SSID, SSID_PASSWORD);

thing["Darkness_status"] >> [](pson &out)
{
    int sensorValue = analogRead(A0);
    read the input on analog pin 0

        float voltage = sensorValue * (5.0 / 1023.0);
        Convert the analog reading (which goes from 0 - 1023)
        to a voltage (0 - 5V)
```

```
        if(voltage<2)
        {
                digitalWrite(D0, HIGH);
                Serial.println("Its Dark, Light ON");
                Serial.println(value);
        }
        else
        {
                digitalWrite(D0, LOW);
                Serial.println("Light OFF");
                Serial.println(value);
        }

        out["status"] = (bool)digitalRead(D0);

}
}

void loop()
{
thing.handle();
}
```

9. **Draw the pin diagram of the pH sensor and NODE mCU. Connect them. Write a program to sense acidity of water and glow a Red LED if water is acidic. List the procedures that has to be followed for accessing these components using webpages (Assume thinger.io is used).**

   (a) The circuit diagram of nodemcu with pH sensor and LED is shown in figure 2.16.

   Procedure

   - create a new account in www.thinger.io
   - login with your account
   - connect NodeMcu in the usb port
   - click on devices and click on add device
   - Give the following information
     - Device Type: Generic Thinger Device
     - Device ID: MyNodeMcu(Note: you can give any name)

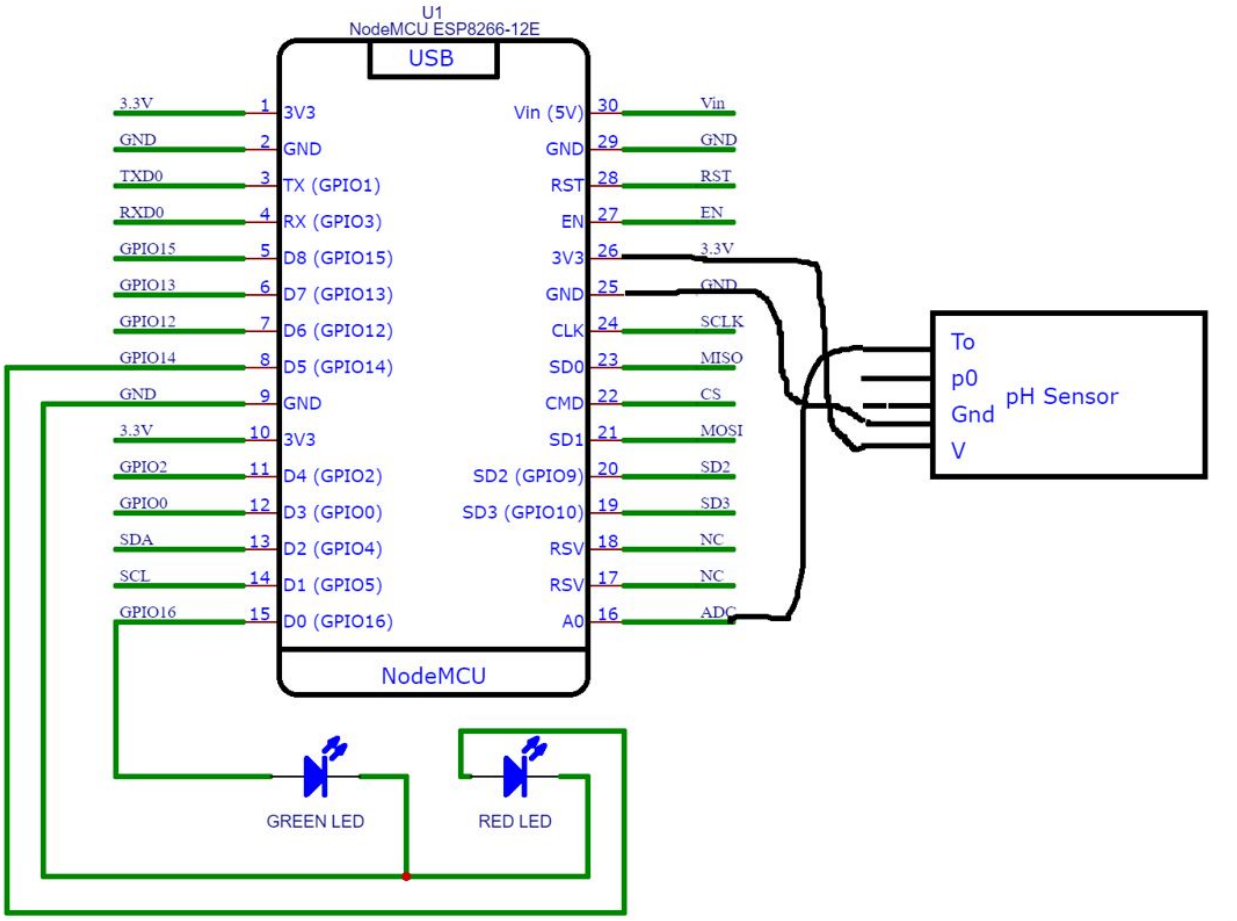


Figure 2.16: circuit diagram of interfacing pH sensor with nodemcu

  - Device Description: LED control
  - Click on Generate random credentials
- Click add device Now your device is registered
- Open Arduino IDE
- Install thinger.io library
- Type thinger.io and install
- Once the library installed,go to NodeMcu
- Enter device id, device credentials from thinger.io and your Wi-Fi settings SSID(Wi-Fi name) and Wi-Fi password
- Select the board and select com, port and upload sketch.
- Press upload
- Press live transmission button
  You will be observing the transmission and received data and the device status online.

- go to device you can observe the device connected.
- Go to dashboard to create your controls with widgets
- Add dashboard
- Press led
- Press right corner switch to add widgets control
- Add widget and provide information
- Select type
- Press save

Program code

```
#include <ThingerESP8266.h>

#define USERNAME "DeviPrasad"
#define DEVICE_ID "DPNMCU"
#define DEVICE_CREDENTIAL "1556551"

#define SSID "Mi_A2"
#define SSID_PASSWORD "12344321"
ThingerESP8266 thing(USERNAME, DEVICE_ID, DEVICE_CREDENTIAL);

int value=0;
void setup()
{
Serial.begin(9600);
pinMode(D0, OUTPUT);
pinMode(D5, OUTPUT);
pinMode(A0, INPUT);

thing.add_wifi(SSID, SSID_PASSWORD);

thing["Darkness_status"] >> [](pson &out)
{
    int sensorValue = analogRead(A0);
    read the input on analog pin 0

        float voltage = sensorValue * (5.0 / 1023.0);
        Convert the analog reading (which goes from 0 - 1023)
```

```
        to a voltage (0 - 5V)

        if(voltage>=2.5)
        {
                digitalWrite(D5, HIGH);
                Serial.println("ACIDIC");
                Serial.println(value);
        }
        else
        {
                digitalWrite(D0, LOW);
                Serial.println("ALKALINE");
                Serial.println(value);
        }

        out["status"] = (bool)digitalRead(D0);
        out["status1"] = (bool)digitalRead(D5);

}
}

void loop()
{
thing.handle();
}
```

10. **Draw the pin diagram of the PIR sensor and NODE mCU. Connect them. Write a program to sense motion of an object and beep a buzzer if object in motion is found. List the procedures that has to be followed for accessing these components using webpages (Assume thinger.io is used).**

    (a) The circuit diagram of nodemcu with pIR sensor and LED is shown in figure 2.17.

    Procedure

    - create a new account in www.thinger.io
    - login with your account
    - connect NodeMcu in the usb port
    - click on devices and click on add device
    - Give the following information

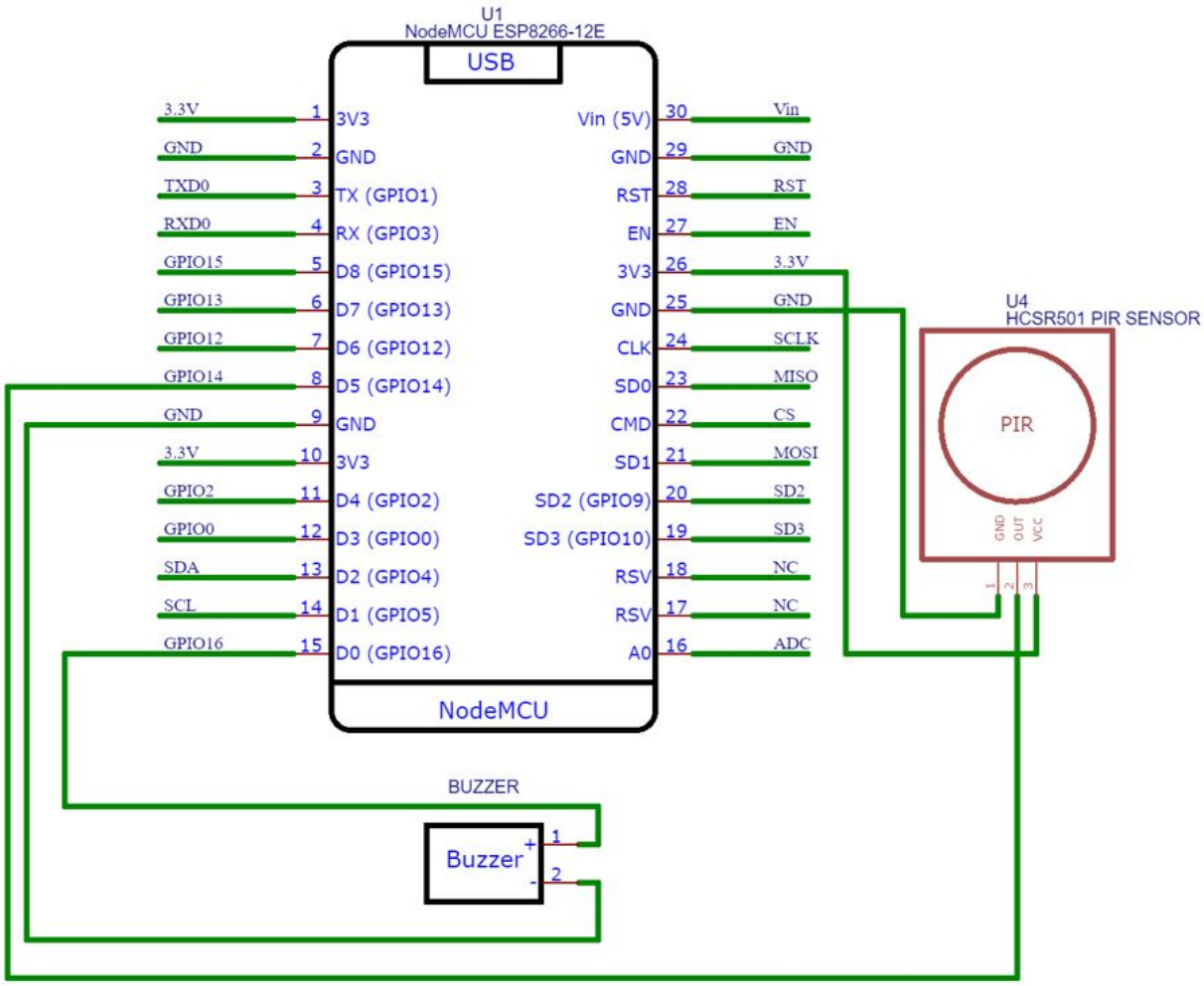


Figure 2.17: circuit diagram of interfacing PIR sensor with nodemcu

  - Device Type: Generic Thinger Device
  - Device ID: MyNodeMcu(Note: you can give any name)
  - Device Description: LED control
  - Click on Generate random credentials
- Click add device Now your device is registered
- Open Arduino IDE
- Install thinger.io library
- Type thinger.io and install
- Once the library installed,go to NodeMcu
- Enter device id, device credentials from thinger.io and your Wi-Fi settings SSID(Wi-Fi name) and Wi-Fi password
- Select the board and select com, port and upload sketch.

- Press upload
- Press live transmission button
  You will be observing the transmission and received data and the device status online.
- go to device you can observe the device connected.
- Go to dashboard to create your controls with widgets
- Add dashboard
- Press led
- Press right corner switch to add widgets control
- Add widget and provide information
- Select type
- Press save

Program code

```
#include <ThingerESP8266.h>

#define USERNAME "DeviPrasad"
#define DEVICE_ID "DPNMCU"
#define DEVICE_CREDENTIAL "1556551"

#define SSID "Mi_A2"
#define SSID_PASSWORD "12344321"
ThingerESP8266 thing(USERNAME, DEVICE_ID, DEVICE_CREDENTIAL);

int value=0;
void setup()
{
Serial.begin(9600);
pinMode(D0, OUTPUT);
pinMode(D5, OUTPUT);

thing.add_wifi(SSID, SSID_PASSWORD);

thing["Darkness_status"] >> [](pson &out)
{
    int sensorValue = digitalRead(D5);
    read the input on DIGITAL pin D5
```

```
        if(sensorValue==1)
        {
                digitalWrite(D0, HIGH);
                Serial.println("MOVEMENT_DETECTED");
                Serial.println(value);
        }
        else
        {
                digitalWrite(D0, LOW);
                Serial.println("NO_MOVEMENT");
                Serial.println(value);
        }

        out["status"] = (bool)digitalRead(D0);

}
}

void loop()
{
thing.handle();
}
```

3. IOT Protocols

3.1 Syallabus

3.1.1 Protocols for IOT

1. Messaging Protocols
    - Message Queuing Telemetry Transport(MQTT)
        - MQTT client, MQTT Broker
        - MQTT Publishing process
    - Constrained Application Protocol (CoAP)
        - Layers of CoAP
        - Request response layer messages
2. Transport Protocols
    - Bluetooth Low Energy (BLE)
        - Features of BLE
        - Components of BLE
        - BLE Protocol Stack
        - BLE Topology
        - Classic Bluetooth Vs BLE
    - Light Fidelity(Li Fi)
        - Functioning of Li Fi
        - Advantages of Li Fi
        - Disadvantages of Li Fi

3.1.2 Addressing and Identification:

1. Internet Protocol Version 4 (IPv4)
2. Internet Protocol Version 6 (IPv6)

3. Uniform Resource Identifier (URI)

3.2 Short Answer Questions

1. **Explain the importance of MQTT protocol with respect to IoT infrastructure?**
   Message Queuing Telemetry Transport(MQTT) is a lightweight protocol ,which makes it exceptionally useful.Lightweight means that it demands minimal resources for its functioning and doesn't require any additional resources from its working environment .IoT prefers this type of lightweight protocol due to resource constraints.

2. **How is IPv4 inferior to IPv6.**
   IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. IPv4 is a 32 bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4

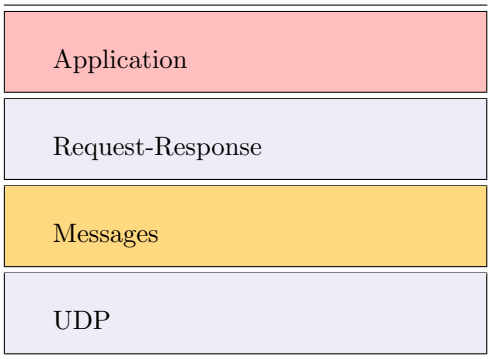
3. **How will you identify an IP class with a given IP address?**
   You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

   - Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.
   - Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.
   - Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

4. **What is the difference between URN and URL? Explain the differences with an example.**
   A URL also known as a eb address, identifies a web resource as well as its location on a computer network and how to access it A URN is a formal naming scheme that identifies a resource, but does not indicate its location or how to access it

5. **What are the layers of CoAP and explain them in brief?**
   The bottom layer is a message layer that has been designed to deal with UDp and asynchronous switching. The request/response layer concerns communication methods and deals with request /response messages.Message Layer supports 4 types message they are

- CON(confirmable)
- NON(non-confirmable)
- ACK(acknowledgement)
- RST(reset)



6. List the differences between MQTT and CoAP.

The difference between MQTT and CoAP are listed in table 3.1

Table 3.1: Difference between MQTT and CoAP

Comparison Aspect	**MQTT**	**COAP**
Underlying protocol	TCP(Connection oriented)	UDP(Connectionless)
Communication	M:N (Many to many)	1:1 (One to one)
Power	Higher than CoAP , Lesser than other protocols	Lowest ,Consumes less power than MQTT , making it the best
Model	Publisher/Subscriber	Request - response(Restful and not SOAPful)

7. List the advantages and disadvantages of LiFi.

Advantages:

- Since it is light weight it cannot penetrate through walls, it is extremely safe and no data hijacking will happen , which is a shortcoming with wifi.

- Efficient
- Fastest and has broken previous records.
- Effective alternative to RF.

Disadvantages:

- It could be short range due to the presence of a wall which could be a real interruption and range limiter.
- The infrastructure setup could take more time , so as to make it practically viable.
- There is no clarity on how the receiving device will transmit data back to the transmitter.

8. **Give a brief description of the URL.**
   URL stands for Uniform Resource Locator. A URL is nothing more than the address of a given unique resource on the web. In theory, each valid URL points to a unique resource. Such resources can be an HTML page, a CSS document, an image, etc. URLs consist of multiple parts – including a protocol and domain name – that tell a web browser how and where to retrieve a resource. URLs can only be sent over the internet using the ASCII character-set. Because URLs often contain non-ASCII characters, the URL must be converted into a valid ASCII format.

9. **List 4 types of messages that are supported by CoAP.**

   - CON(confirmable)
   - NON(non-confirmable)
   - ACK(acknowledgement)
   - RST(reset)

10. **List three levels of QOS supported by MQTT protocol.**

    - 0 - at most once.
    - 1 - at least once.
    - 2 - exactly once.

3.3 Long Answer Questions

1. **Differentiate URN and URL. Cite an example and explain your views.**
   Uniform Resource Locator(URL)- A URL is nothing more than the address of a given unique resource on the web. In theory, each valid URL points to a unique resource. Such

resources can be an HTML page, a CSS document, an image, etc. URLs consist of multiple parts – including a protocol and domain name – that tell a web browser how and where to retrieve a resource. URLs can only be sent over the internet using the ASCII character-set. Because URLs often contain non-ASCII characters, the URL must be converted into a valid ASCII format.

Uniform Resource Name(URN) is a string of characters that gives the name of the resource. lIke real life, two objects on the internet also can have the same name. URN gives a unique identity of a resource within a defined area or namespace. The combination of URL and URN gives the resource a unique identity

The main difference is-

Uniform Resource Locator (URL) establishes the identity of the object by giving the location and the protocol or the mechanism to retrieve it. Uniform Resource Name (URN) identifies the object by name. Hence URN and URL are subsets of URI and help in retrieving the objects on the Internet easily.

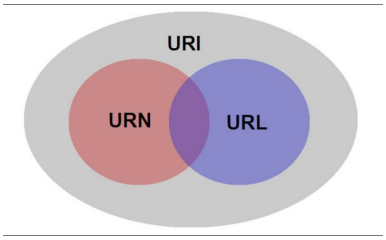


Figure 3.1: Relationship between URL, URN and URI

2. **Explain publish- subscribe pattern of MQTT protocol in detail.**

A component called central broker plays a key role in the entire system. This message broker helps to dispatch messages to the nodes that have subscribed for the same. The publisher (node) sends the message to the broker and the broker takes the responsibility of dispatching the message to the subscribed destinations. In the figure we can see that a publisher (node) can send the data (message) to the MQTT broker. Based on the subscription from the nodes connected, the broker sends the messages accordingly. In this example, only subscribers 1 and 3 have subscriptions for the humidity data. Hence, the data is captured by the nodes that have expressed interest through subscription. The data (message) reaches the node that really wants it and not to all the nodes present in the network.

Another important aspect is that the messages are published as topics and the publisher publishes the messages with a topic. In the above figure, the topic of the published message is "humidity". Clients subscribe to the topics and they get the messages based on their subscription.

In this approach, clients do not have any address. When there is no address available, the messages cannot be routed appropriately. In a typical networking schema, it is well-known

that addressing connects the source to the destination.

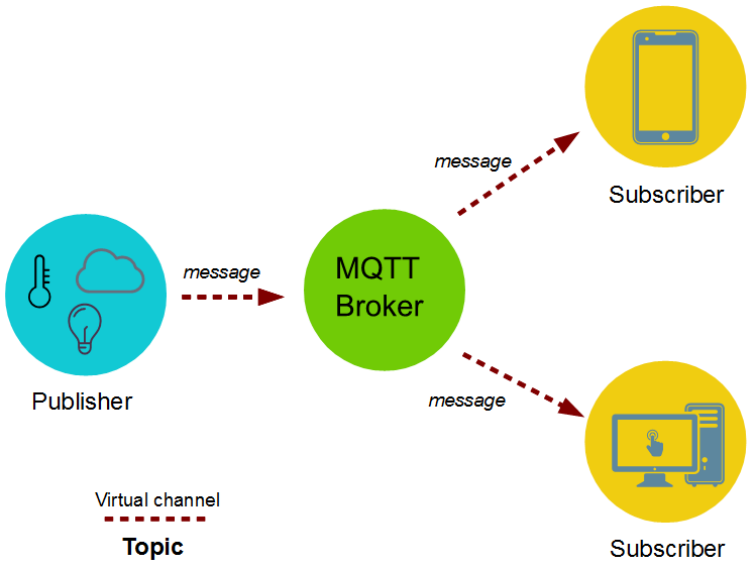


Figure 3.2: MQTT Architecture

3. Explain the importance of URI in networking

A uniform resource identifier (URI) is a character sequence that identifies a logical (abstract) or physical resource - usually, but nor always, connected to the internet. A URI distinguishes one resource from another. URIs enable internet protocols to facilitate interactions between and among these resources. The strings of characters incorporated in a URI serve as identifiers, such as a scheme name and a file path. In the URI, the file path may be empty. A Uniform Resource Locator (URL), or web address, is the most common form of URI. It is used for unambiguously identifying and locating websites or other web-connected resources.

URIs can identify different types of resources, including:

- electronic documents
- webpages
- images
- information sources with a consistent purpose

The generic form of any URI scheme is

`[//[user:password@]host[:port]][/]path[?query][fragment]`

A URI may consist of the following elements:

Scheme

Within the URI, the first element is the scheme name. Schemes are case-insensitive and separated from the rest of the object by a colon. The scheme establishes the concrete

syntax and associated protocols for the URI. Ideally, URI schemes should be registered with the Internet Assigned Numbers Authority (IANA) although non registered schemes can also be used.
Example
If the URI is **telnet://192.0.2.16:80**, the scheme name is **"telnet."**

Authority
The URI's authority component is made up of multiple parts: a host consisting of either a registered name or an IP address, an optional authentication section and an optional port number.
The authentication section contains the username and password, separated by a colon, and followed by the symbol for at (@). After the @ comes the hostname, followed by a colon and then a port number. IPv4 addresses are commonly in a dot-decimal notation, and IPv6 addresses, which need to be in brackets, are typically in hexadecimal form.
The path containing data is notated by a sequence of segments separated by slashes. These slashes imply a hierarchical structure. The path begins with a single slash, whether or not an authority is present. However, the path cannot start with a double slash. This part of the syntax may closely resemble a particular file path but does not always imply a relation to that file system path. In the previous URI example **(telnet://192.0.2.16:80)**, a scheme name is present. The numbers after the double slash constitute the authority. Because no characters come after the slash, it indicates that the path is empty.

Query (optional)
The query contains a string of non-hierarchical data. It is often a sequence of attribute-value pairs separated by a delimiter, such as an ampersand or semicolon. A question mark separates the query from the part that comes before it. The string represents some operation applied to a "iqueryable" object by the URI.
Example
In the URI
`foo://techtarget.com:8042/over/there?name=parrotbeak`
the query is name=parrotbeak.
However, because this part of the syntax is optional, it may not always be present.

Fragment (optional)
The fragment contains an identifier that provides direction to a secondary resource. It is separated from the preceding part of the URI by a hash . If the primary resource is an HTML document or article, the fragment may be an ID attribute of a specific element of that resource. In this case, a web browser will scroll this particular element into view.

However, if the fragment ID is void, it indicates that the URI refers to the whole object. In this case, the hash sign may be omitted.

4. **Explain client and broker of MQTT protocol in detail with a neat figure and List three levels of QOS supported by MQTT protocol.** An MQTT client is any device (from a micro controller up to a full-fledged server) that runs an MQTT library and connects to an MQTT broker over a network. The MQTT client can also be a typical computer running a graphical MQTT client for testing purposes. Basically, any device that speaks MQTT over a TCP/IP stack can be called an MQTT client. The client implementation of the MQTT protocol is very straight forward and streamlined. The ease of implementation is one of the reasons why MQTT is ideally suited for small devices.
MQTT Client:

   - Collects information from sensors (telemetry devices)
   - Connects it to the messaging server (broker)
   - Topic is used to publish this message to let other clients understand
   - Can also be a subscriber

   The broker is responsible for receiving all messages, filtering the messages, determining who is subscribed to each message, and sending the message to these subscribed clients. The broker also holds the session data of all clients that have persistent sessions, including subscriptions and missed messages. Another responsibility of the broker is the authentication and authorization of clients.
   Usually, the broker is extensible, which facilitates custom authentication, authorization, and integration into backend systems. Integration is particularly important because the broker is frequently the component that is directly exposed on the internet, handles a lot of clients, and needs to pass messages to downstream analyzing and processing systems.
   MQTT Broker:

   - Protocol is implemented in this case
   - Mediates and facilitates the data based on interest of the subscriber

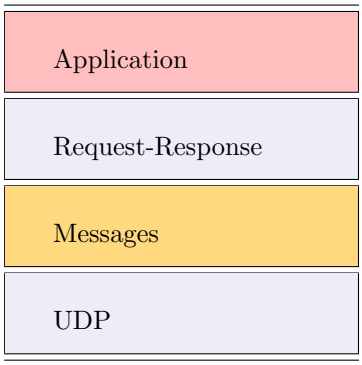
   MQTT also supports quality of service (QoS) levels. The three levels of QoS supported by MQTT are as follows:

   - 0=At most once (Best effort, No Ack)
   - 1=Atleast once (Acked,retransmitted if ack not received)
   - 2=Exactly once (Request to send(Publish), clear to send)

5. **List the layers of CoAP protocol. Discuss four types of messages that are supported by CoAP**

a. CoAP is a two layered protocol. The lower layer is the message layer and the upper layer owns the request-response process. The upper layer is dependent on UDP.

Table 3.2: CoAP Layers



CoAP supports four types of messages:

Confirmable (CON) - Reliable messaging: this is a reliable approach, wherein mission occurs until the acknowledgement is received with the same message ID as seen in the request. When there is a timeout or fail, there would be a RST message sent from the server as a response. This approach is referred to as a reliable messaging approach since re transmission is resolved. refer figure 3.3.

Non-Confirmable (NON) - Non Reliable Messaging: there is no reliability ensured in this message transmission style. No acknowledgement will be issued in the message. The message ID is also part of the transaction and this enables supervision. In case no processing is carried out by the receiver, an RST message is sent. refer figure 3.3.

Acknowledgement (ACK): this is a traditional acknowledgement message sent in any sort of protocol. We can connect it to the regular handshaking scheme (A handshake is an automated process of negotiation between two participants through the exchange of information that establishes the protocols of a communication link at the beginning before full communication begins.

Reset (RST): if no processing has happened at the receiver end even after a specific amount of time, there should be a mechanism to inform the sender of the situation. For this purpose, there is a message option called reser (RST). it will inform the sender that there is a problem or trouble in the transmission.

6. **Discuss CoAP request – response layer messages**

CoAP - Request - Response Layer Messages:

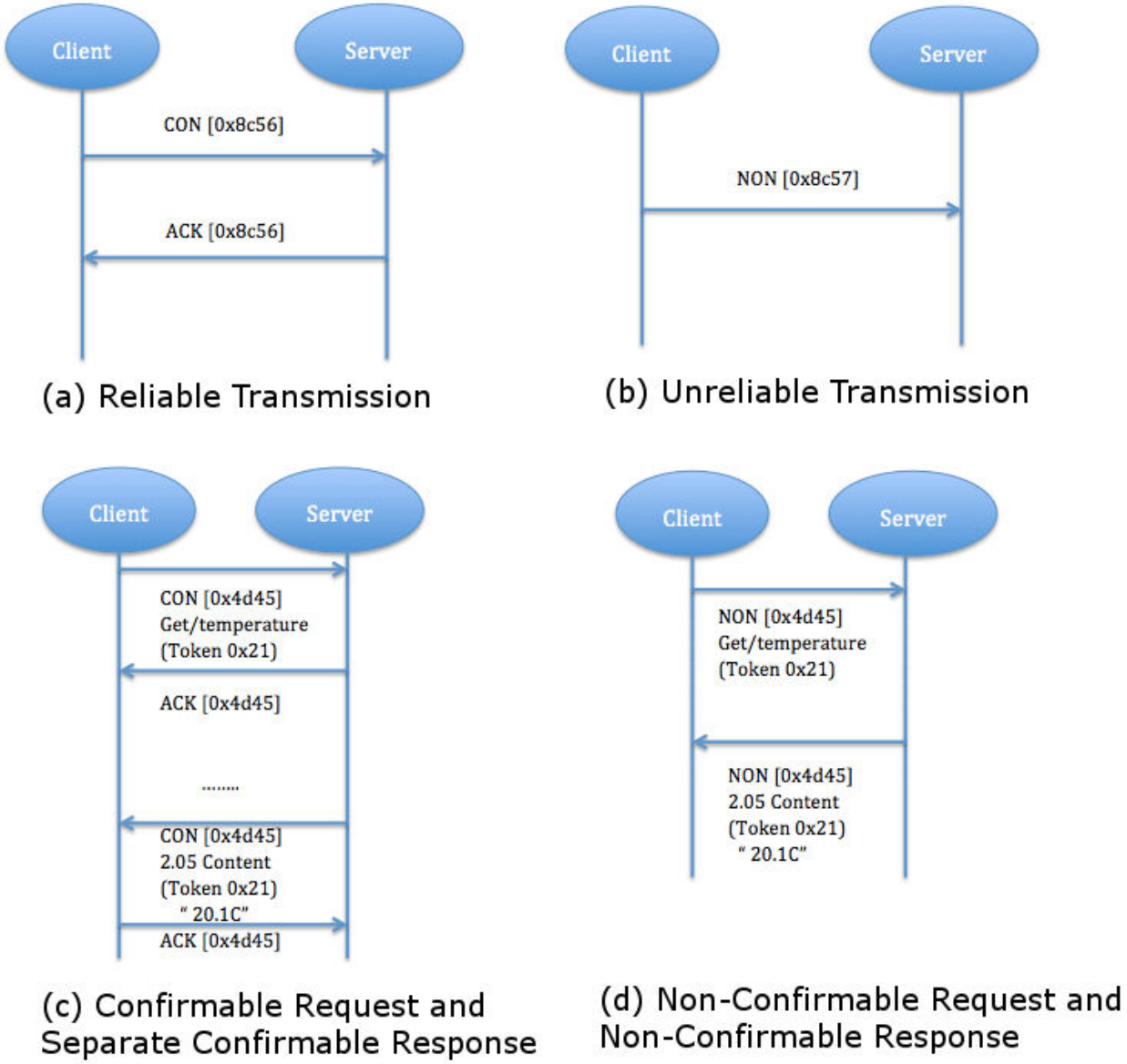


Figure 3.3: CON and NON

- Piggy - Backed: in this mode of request - response approach, the client sends a request through the CON/NON-messaging method. ACK is received immediately with corresponding token number and message. In the figure, the message is humidity. If humidity data is not available, the failure code is embedded as a part of the ACK
- Separate response: when a CON type message is sent to the server and in case the server is unable to respond immediately, an Empty ACK will be reverted. After some time, when the server is able to send the response, it sends a CON message with data. ACK is sent back from the client.
- Non - Confirmable Request and Response: here, NON type message is sent from the client to the server. The server does not need to give ACK and it can send a NON

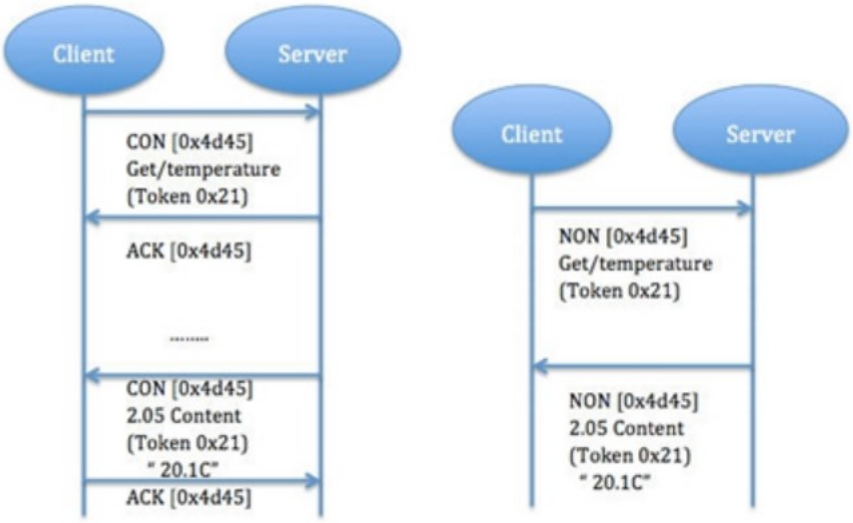


Figure 3.4: Piggy Backed Messages

type response request.

- Ver: it is a 2-bit unsigned integer and refers to CoAP version. In this case it is one.
- T: it is a 2-bit unsigned integer and refers to the message type. The message can be one of the following:
  - Confirmable (0)
  - Non - confirmable (1)
  - ACK (2)
  - RESET (3)
- TKL: it is a 4-bit unsigned integer and refers to the token length. It normally ranges from 0 to 8 bytes.
- Code: it refers to the response code
- Message ID: it is the identifier of the message.

7. **How does Li-Fi work? Explain its functioning.**

Li-Fi is a wireless communication technology which utilizes light to transmit data and position between devices. It has the high speed and is bi-directional and it is also used for communication of data

Working of Li-Fi: Li-Fi is constructed with many components which start with a modified LED bulb. The entire work-flow and component details are presented below

- Data is transmitted over Li-Fi by modulating the intensity of light; that is essentially dimming the light or turning it on and off at a very high speed
- The modulation happens real quick and human eyes cannot really fell or captured it

- The light is received by the photodetector and demodulation(processing) happens to generate the data stream sent by the transmitter
- All the LED lamps need an LED lamp driver RESET
- The lamp driver gets information from the server and encoding occurs here
- After this led illumination(flicker) takes place
- The photodetector will be able to read this and convert it into data(after amplification/processing)

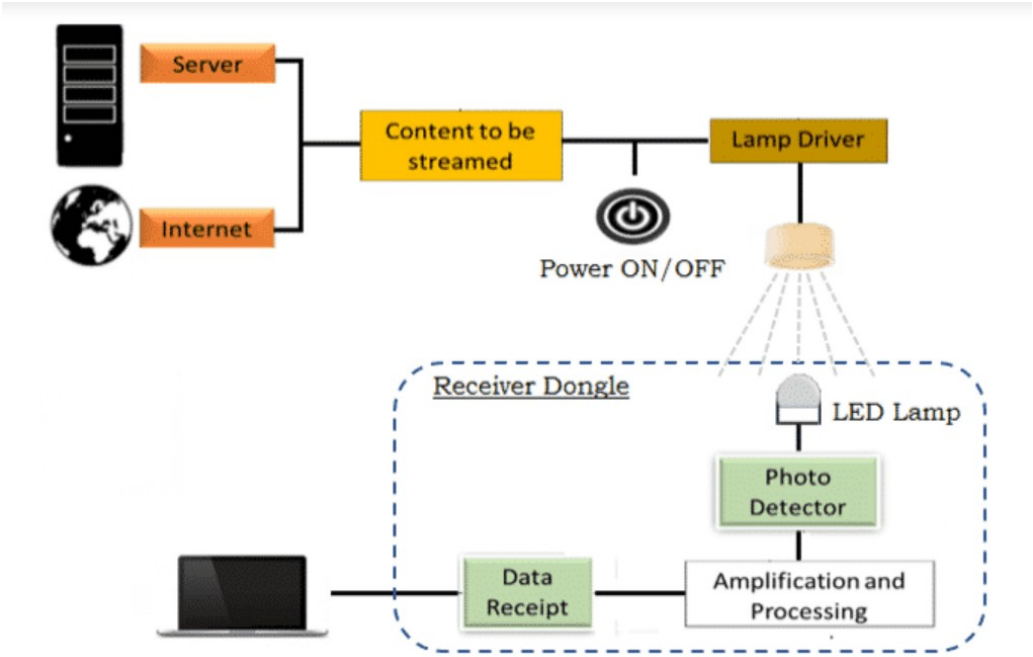


Figure 3.5: Working of Lifi

Advantages of Li-Fi: Some of the advantages of Li-Fi are listed below:

- Since light cannot penetrate through walls it is extremely safe and no data hijacking will happen which is a shortcoming with Wi-fi.
- Efficient
- LI-Fi is the fastest and is expected to break all precious records
- It is an effective alternative to RF

Disadvantages of Li-Fi: Some of the Disadvantages of Li-Fi are listed below:

- It could be short range due to the presence of walls which could be real interrupt and range limite
- The infrastructure setup could take more time so as to make it practically viable
- There is no clarity on how to receiving device will transmit data back to the transmitter

8. Compare the packet format of IPv4 and IPv6. Explain all the fields in detail.
Fields of IPv4:

- IP Version Number: it is a half a byte field (4 bits), which indicates the version of IP being utilized. This field has value 4 in binary (0100). The basic idea of using this version field is to ensure compatibility between the versions of IP that might be used in the network. One device may have IPv4 and another device may support IPv6. The backward compatibility will fail and the device using the older version will not be compatible with the newer one
- Internet Header Length: This length specifies Internet header length in 32-bit words and points to the beginning of the data. The minimum value for a correct header is 5 (0101)
- Type of Service: This is an 8-bit field, which indicates the quality of service (QoS). the QoS can be precedence, delay, and reliability. The 8-bits are framed as
  - Precedence: bits 0 to 2 represent precedence, which has further options as shown in the figure.
  - Delay: this is the 4th bit and it indicates the delay. Here "0" indicates a normal delay and "1" indicates a lower delay.
  - Throughput: "0" indicates normal delay and "1" indicates high throughput
  - Reliability: "0" indicates normal reliability and "1" indicates high reliability
- Total Length this is a 16 - bit field which defines the length of the IPv4 datagram. This length includes header and data. The minimum length of the IP datagram is 20 bytes and the maximum can be 65,535
- Identification: this is a 16-bit field added by the sender to help in assembling the fragments. It helps in organizing data. If the message sent is too large to fit in one packet, it will be split to multiple child packets. The unique identifier for all the split packets is provided to identify them. This makes the receiver's job of rebuilding the receiving data easy.
- Flags: this field is composed of three bits. The first bit is always 0 and it is kept unused. The second bit is called Don't Fragment (DF) flag. If DF is set to "0", the IP datagram can be fragmented and if set to "1" it cannot be fragmented. The next bit is called more fragments (MF) which if set will indicate that more fragments are on the way.:
- Fragment Offset: when fragmentation of a message occurs, this field specifies the offset or position in the overall message where the data in this fragment is present. It is specified in units of 8 bytes (64 bits). The first fragment has an offset of 0.
- Time to Live: this is an 8-bit field and indicates the time that IP datagram will survive.

There will be a time set that will be decremented by 1; the router keeps an eye on it. When it reaches zero, the datagram can be discarded

- Protocol: this serves as an identifier for the higher layer protocol carried in the IP datagram. The protocols can be ICMP, IGMP, TCP or UDP
- Header Checksum: this is a 16-bit checksum computed over the header to provide basic protection against corruption in transmission. It is calculated by dividing the header bytes into words and then adding them together. The data is not check summed, only the header. At each hop, the device receiving the datagram does the same checksum calculation and on a mismatch, discards the datagram as damaged
- Source Address: This is the 32-bit IP address of the source (originator) of the datagram.
- Destination Address: This is the 32-bit IP address of the destination which receives the IP datagram
- Options: There are a lot of optional header settings available and they are used for the debugging/testing and security purposes
- Padding: IP options field may vary in length. So, the padding field provides additional 0 bits so that the total header length is an exact multiple of 32 bits.

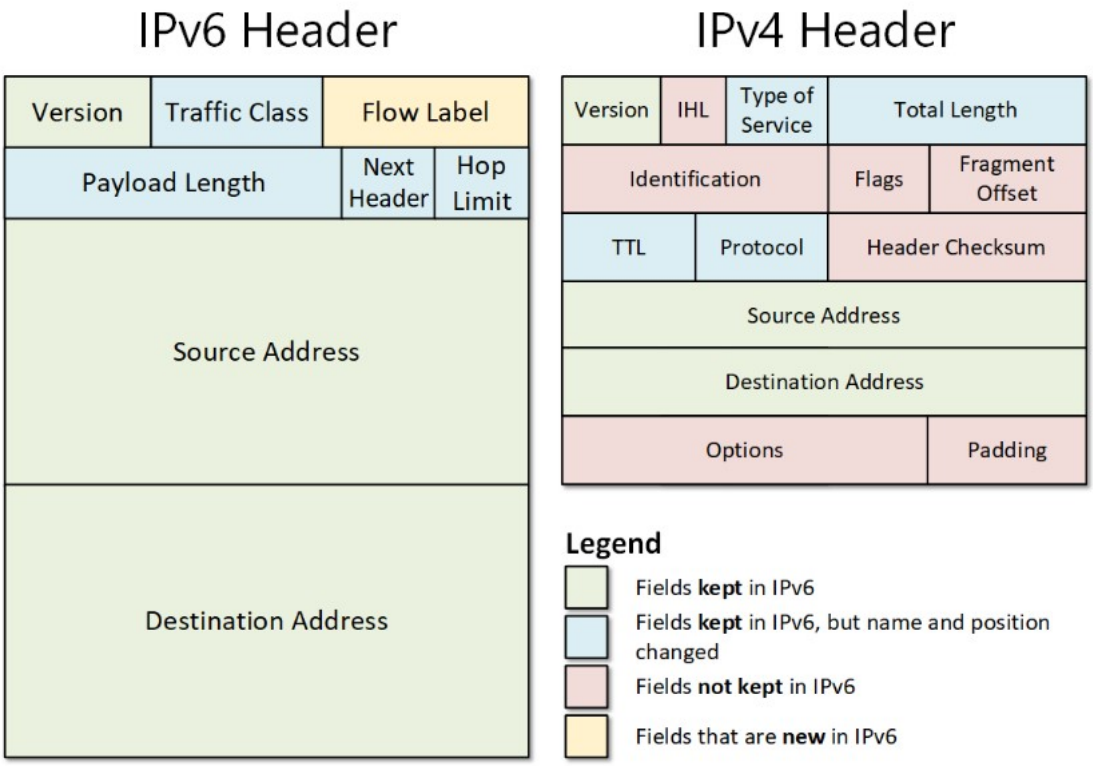


Figure 3.6: Piggybacked Messages

Fields of IPv6:

- Version (4 bits): This is used to represent the version of IP being used. In IPv4, it is 4 and in IPv6, it is 6.
- Traffic Class (8 bits): This is an 8-bit field that provides the means of identifying different classes or priorities of IPv6 packets. It replaces the ToS field of IPv4, MSB 6 bits are used for ToS to let the router know what services should be provided to this packet. LSB 2 bits are used for Explicit Congestion Notification.
- Flow Label (20 bits): This is used to identify the sequence of packets. It helps in prioritizing packet delivery and providing real time service. The vital packets can be delivered ahead of the lower priority packets
- Payload Length (16 bits): This identifies the length of IPv6 payload (the rest of the packet following the IPv6 header). It is used in place of the total length of IPv4.
- Next Header (8 bits): This is similar to the protocol field in IPv4 header. It represents the type of extension header that follows the primary IPv6 header.
- Hop Limit (8 bits): Time to Live (TTL) is replaced by Hop Limit in IPv6 header. The value in this field is decremented by 1 every time the packet passes through a host that forwards the packet. When the value reaches 0, the packet will be discarded.
- Source Address: As in IPv4, this specifies the sender's IP 128-bit address
- Destination Address: Similar to IPv4, the destination's IP address is denoted here,

9. Classify IPv4 addressing. If you are asked to identify a class of IP for your university campus, which class would you select and why?

a. An ip address is a unique identification for a node connected to a network. An IP address comprises two halves-networks host ID. addresses are categorized into classes based on network id and host id. In this section, a complete and comprehensive analysis of IPv4 classes is presented. The IP addresses are classified into ClassA,ClassB,ClassC,ClassD and ClassE as shown in figure 3.7

CLASSS A

The IP address belonging to Class A uses only the first octet to identify the network and the last three octets are used to identify the host

The network ID has 8 bits.

The host ID has 24 bits.

The first bit of the first octet is always set to 0

The default subnet mask for class A IP address is 225.0.0.0. Subnet masks are u;sed to tell hosts on the network which part is the network address and which part is the host address of an IP address The IP address belonging to Class A ranges from 1.a.a.a to 126.a.a.a.(where a ranges from 0 to 255)

Class B:

The IP address belonging to class B uses the first two octets to identify the network and

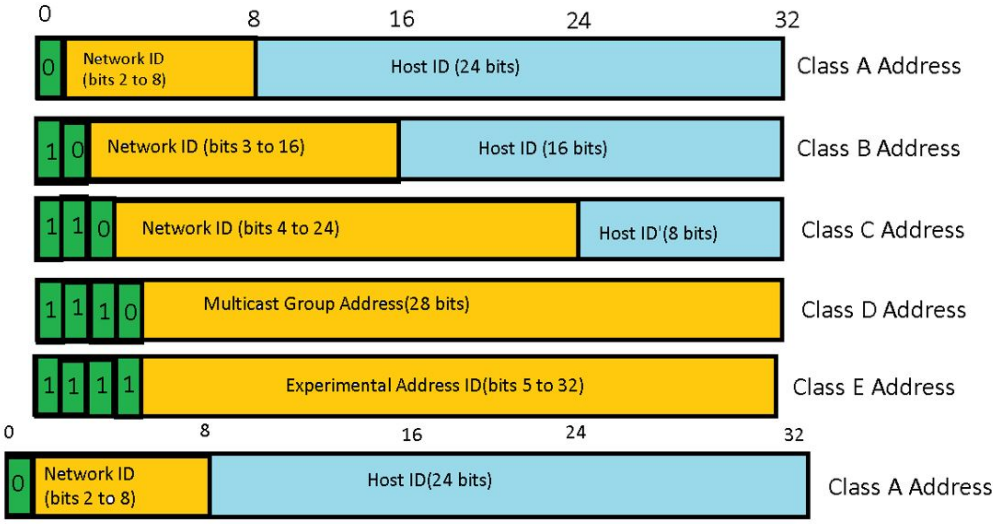


Figure 3.7: IPv4 Addressing

the last two octets are used to identify the host.
The network ID has 14 bits.
The host ID had 16 bits.
The first two bbit of the first octet is always set to 10
The subnet mask for class B is 225.255.0.0. The IP address belonging to Class B ranges from 128.0.a.a to 191.255.a.a.(where a ranges from 0 to 255)

Class C:

The IP address belonging to class c uses the first three octets to identify the network and the last octet is used to identify the host // The network ID has 24 bits.
The host ID had 8bits.
The first two bits of the first octet are always set to 110.
The IP address belonging to Class C ranges from 192.0.0.a to 223.255.255.a.(where a ranges from 0 to 255)

Class D:

The ip address belonging to Class D has the first four bits of the first octet set as 1110. The remaining bits are the host bits The IP address belonging to Class D ranges from 224.0.0.0 to 239.255.255.255. This class does not have any subnet mask

Class E:

The ip address belonging to Class E has the first four bits of the first octet set as 1111. The remaining bits are the host bits
The IP address belonging to Class D range form 240.0.0.0 to 225.225.225.254. This class does not have any subnet
To identify the IP class of a given IP address we can actually look into the first octet of the IP address. Convert the dotted decimal IP address to its binary equivalent.

10. Compare IPV4 and IPV6 addressing.

Table 3.3: Comparision of IPv4 & IPv6

IPv4	IPv6
IPv4 is a 32-Bit IP Address.	IPv6 is 128 Bit IP Address. IPv4 is a numeric address, and its binary bits are separated by a dot (.)
IPv6 is an alphanumeric address whose binary bits are separated by a colon (:). It also contains hexadecimal. IPv4 is a numeric addressing method	IPv6 is an alphanumeric addressing method. IPv4 offers 12 header fields
IPv6 offers 8 header fields. IPv4 has checksum fields	IPv6 doesn't have checksum fields IPv4 supports VLSM (Virtual Length Subnet Mask)
IPv6 doesn't support VLSM. IPv4 uses ARP (Address Resolution Protocol) to map to MAC address	IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC address. Fragmentation is done by sending and forwarding routes.
Fragmentation is done by the sender. IPv4 uses ARP (Address Resolution Protocol) to map to MAC address	IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC address.

4. Cloud for IoT

4.1 Syallabus

4.1.1 Introduction to Cloud

1. Cloud Services
    - Software-as-a-Service(SaaS)
    - Platform-as-a-Service(PaaS)
    - Infrastructure-as-aService(IaaS)
    - Constrained Application Protocol (CoAP)

4.1.2 Addressing and Identification

1. Internet Protocol Version 4 (IPv4)
2. Internet Protocol Version 6 (IPv6)
3. Uniform Resource Identifier (URI)

4.2 Short Answer Questions

1. **List three deployment models for cloud computing?**
   There are 3 main types of cloud computing services :
    - Infrastructure-as-a-Service (IaaS)
    - Platforms-as-a-Service (PaaS)
    - Software-as-a-Service (SaaS)
2. **Explain SaaS in cloud computing?**
   Software-as-a-Service, or SaaS for short, is a cloud-based method of providing software to users. SaaS users subscribe to an application rather than purchasing it once and installing it. Users can log into and use a SaaS application from any compatible device over the Internet.

3. **Explain PaaS in cloud computing?**

Platform as a service (PaaS) is a cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. so end users do not need to worry about managing the infrastructure.

Example: Google App Engine, Force.com, Joyent, Azure.

PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools:

- Programming languages

  PaaS providers provide various programming languages for the developers to develop the applications. Some popular programming languages provided by PaaS providers are Java, PHP, Ruby, Perl, and Go.

- Application frameworks

  PaaS providers provide application frameworks to easily understand the application development. Some popular application frameworks provided by PaaS providers are Node.js, Drupal, Joomla, WordPress, Spring, Play, Rack, and Zend.

- Databases

  PaaS providers provide various databases such as ClearDB, PostgreSQL, MongoDB, and Redis to communicate with the applications.

- Other tools

  PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

4. **Explain Iaas in cloud computing ?.**

Infrastructure as a service (IaaS) is a type of cloud computing service that offers essential compute, storage and networking resources on demand, on a pay-as-you-go basis. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model.

IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure.

IaaS is offered in three models: public, private, and hybrid cloud. The private cloud implies that the infrastructure resides at the customer-premise. In the case of public cloud, it is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which the customer selects the best of both public cloud or private cloud.

IaaS provider provides the following services -

- Compute: Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.
- Storage: IaaS provider provides back-end storage for storing files.
- Network: Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
- Load balancers: It provides load balancing capability at the infrastructure layer.

5. **List the reasons for private cloud deployment?**.
Using the private cloud is the best choice for such situations:

- Data storage for strictly regulated industries like government or healthcare
- Handling sensitive data
- Data processing in companies that execute strict control over their IT infrastructure and workloads to ensure regulatory compliance, like banking
- Global enterprises with geographically dispersed data storage and processing operations, that need to optimize their workflows to ensure cost-efficiency
- Top-performing organizations that can afford to invest in innovative technologies to ensure data processing speed and high-availability

6. **When is public cloud deployment opted?.**
Below are the most popular public cloud use cases:

- Predictable workloads and cloud computing resource needs, like communication services for a known quantity of users
- Running apps and services required to conduct IT and business workflows
- Scaling up and down to meet periodic workload spikes
- Environments for software development and testing

7. **When is hybrid cloud deployment opted?.**
Organizations often adopt a hybrid cloud strategy to maintain proprietary or protected information in local data centers, while also enjoying the scale and pay-per-use benefits of public cloud infrastructure. For example, legal may wish to store and process all its data on-premises, while marketing wants to use public cloud services to interact with employees and customers, keeping web traffic off of the local corporate network. Hybrid cloud computing commonly utilizes consistent management operations across environments.

8. **List the migration challenges when data is to be moved from the cloud?**

- Lack of Strategy.
- Cost Management.

- Vendor Lock-In.
- Data Security and Compliance.
- Cloud Migration Planning.
- Migration Business Case.
- Cloud Data Migration Execution.
- Ongoing Upkeep

9. **List the advantages of using a private cloud**
   There are the following advantages of Private Cloud -
   - More Control Private clouds have more control over their resources and hardware than public clouds because it is only accessed by selected users.
   - Improved performance Private cloud offers better performance with improved speed and space capacity.
   - Security and privacy Security and privacy are one of the big advantages of cloud computing. Private cloud improved the security level as compared to the public cloud.

10. **List the migration challenges when data is to be moved to cloud?.**
    Cloud migrations can be complex and risky. Here are some of the major challenges facing many organizations as they transition resources to the cloud.
    - Lack of Strategy

      Many organizations start migrating to the cloud without devoting sufficient time and attention to their strategy. Successful cloud adoption and implementation requires rigorous end-to-end cloud migration planning. Each application and dataset may have different requirements and considerations, and may require a different approach to cloud migration. The organization must have a clear business case for each workload it migrates to the cloud.
    - Cost Management

      When migrating to the cloud, many organizations have not set clear KPIs to understand what they plan to spend or save after migration. This makes it difficult to understand if migration was successful, from an economic point of view. In addition, cloud environments are dynamic and costs can change rapidly as new services are adopted and application usage grows. Vendor Lock-In
    - Vendor lock-in is a common problem for adopters of cloud technology. Cloud providers offer a large variety of services, but many of them cannot be extended to other cloud platforms. Migrating workloads from one cloud to another is a lengthy and costly process. Many organizations start using cloud services, and later find it difficult to switch providers if the current provider doesn't suit their requirements.

- Data Security and Compliance

  One of the major obstacles to cloud migration is data security and compliance. Cloud services use a shared responsibility model, where they take responsibility for securing the infrastructure, and the customer is responsible for securing data and workloads.

  So while the cloud provider may provide robust security measures, it is your organization's responsibility to configure them correctly and ensure that all services and applications have the appropriate security controls.

  The migration process itself presents security risks. Transferring large volumes of data, which may be sensitive, and configuring access controls for applications across different environments, creates significant exposure.

4.3 Long Answer Questions

1. Differentiate between edge and fog computing?

Table 4.1: Difference between edge and fog computing

Edge Computing	Fog Computing
Less scalable than fog computing	Highly scalable when compared to edge computing
Billions of nodes are present	Millions of nodes are present
Nodes are installed for away from the cloud	Nodes in this computing are installed close to the cloud (remote database where data is stored)
Edge computing is a subdivision of fog computing	Fog computing is a subdivision of cloud computing
The bandwidth requirement is very low. Because data comes orm the edge nodes themselves	The bandwidth requirement is high data originated from edge nodes is transferred to the cloud.
Operational cost is higher	Operational cost is comparatively lower
High privacy. Attacks on data are very low	The probability of data attacks is higher
Edge devices are the inclusion of the IoT devices or client's network	Fog is an extended layer of cloud.
The power consumption of nodes is low	The power consumption of nodes filter important information from the massive amount of data collected from the device and saves it in the fitter high.
Edge computing helps devices to get faster results by processing the data simultaneously received from devices.	Fog computing helps in filtering important information for the massive amount of data collected from the device and saves it in the cloud by sending the filtered data.

2. Summarize the concepts of fog nodes and cloud computing?

Fog nodes:

Consider the fog environment as represented sensors/devices generate data and transmit it to the middle layer. Which is very close to the data source, the se nodes in the middle layer are capable of handling the data. This requires minimum power and lesser resources. The idea is that all data need not go to the cloud at the instant it is generated. Also sensitive data gets processed very fast which results in an instant response. Fog is not meant for hefty storage. It is still the cloud that does the task of storing big data. Fog is just an intermediary layer that enables faster data processing thereby facilitating faster response time

- It receives the data feed form the sensors in real time
- Response time is minimal ideally in milliseconds
- Fog computing is transit, where data is stored for a limited time only
- Data is then sent to the cloud as a summary. It is important to note that all data goes to the cloud

Cloud computing

Cloud computing is the delivery of computing resources, including storage, processing power, databases, networking, analytics, artificial intelligence, and software applications – over the internet.

Characteristics of cloud computing

- On demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Types of cloud deployments

- Public cloud – public clouds deliver computing resources
- Private cloud – a private cloud is computing resources dedicated exclusively to an organization
- Hybrid cloud – they are combination of public and private clouds example IBM hybrid cloud

Cloud computing services

- Infrastructure as a service – it is a foundational cloud service layer that allows organizations to rent IT infrastructure

- Platform as a service – it is a cloud infrastructure built on laaS that provides resources to build user-level tools and applications
- Software as a service – this delivers software applications over the internet
- Function as a service – it is a cloud computing service that offers a platform where customers can develop, run, and manage applications

Benefits of cloud computing

- Reduced cost
- Increased scalability
- Better performance
- Improved execution speed
- Increased security
- Continuous integration and delivery
- Comprehensive monitoring and incident management

3. **Explain private cloud deployment models and list its advantages and disadvantages**

Private cloud deployment: This is one of the best models where the data generated is safeguarded without any flaw. This particular deployment model can be opted wherever confidentiality matters the most, this model can be chosen wherever and whenever the intellectual property needs to be protected when this model is chosen the complete control of everything is well within the organization for which the deployment is carried out In this approach the cloud services are typically in the data centers inside the organization hence everything has to be taken care of by the organization that owns this deployment. This model demands that the hardware,software,data center personnel,infrastructure,etc.

Be maintained,monitored,and installed by the organization, which makes this model expensive, however this model offers the organization complete flexibility in terms of deciding and managing the resources also, data security can be ensured in the best possible way through this model as per the organization's data security guidelines.
The main **advantages** of private cloud deployment include the following:

- Data security is paramount in this model and is ensured
- This model is seen as a flexible model compared

The main **disadvantages** of private cloud deployment include the following:

- Cloud prove expensive

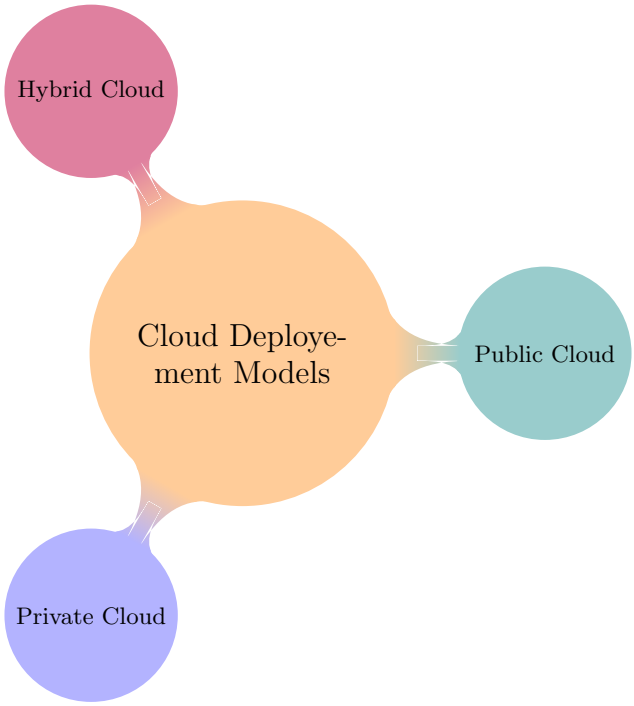


Figure 4.1: Various cloud deployment models

- Maintenance, periodic upgradation, etc. . . , could be difficult
- Politics and other related things are to be framed carefully to make sure that the data is safe

4. **Draw and explain the architecture and working of the fog computing model?**
The fog computing architecture consists of physical and logical elements in the form of hardware and software to implement IoT networks. It is composed of IoT devices, fog nodes, fog aggregation nodes with the help of fog data services, remote cloud storage and local data storage server/cloud. Let us understand go computing architecture components.

IoT devices:

These are devices connected to the IoT network using various wired and wireless technologies. These devices produce data regularly in huge amounts. There are numerous wired technologies used in IoT which include Z Wave,NFC etc.

Fog nodes:

Any device with computing, storage and networking connectivity is known as fog node. Multiple fog nodes are spread across larger regions to provide support to end devices fog nodes are connected using different topologies. The fog nodes are installed at various locations as per different applications such as on floor of a factory, on top of power pole along side of railways track , in vehicles and etc.

Fog aggregate nodes:

Each fog node has their aggregate fog node, it analyzes data in seconds to minutes. IoT

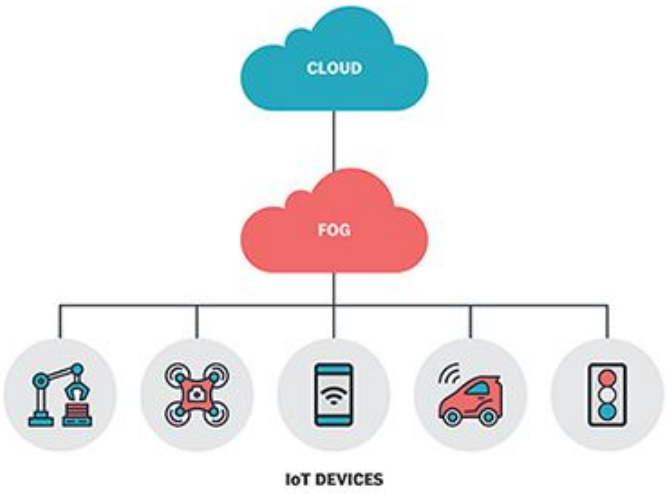


Figure 4.2: Fog Computing Model

data storage at these nodes can be of duration in hours or days. Its geographical coverage is wider. Fog data services are implemented to implement such aggregate node points they are used to address average sensitive data.

Remote cloud:
All the aggregate fog nodes are connected with the cloud, time insensitive data or less sensitive data are processed analyzed and stored at the cloud.

Local server and cloud:
Often fog computing architecture uses a private server/cloud to store the confidential data of the firm. These local storage is also useful to provide data security and data privacy

Fog computing model working:
Fog computing architecture works based on the type of data it receives; nearest fog nodes take data input from the devices. Let us understand working of fog computing architecture

- Most time sensitive data is handled by the nearest fog node to end device which has generated the data. After the received data is analyzed, division or action is transmitted to the device after this fog node sends and stores summary to the cloud for future analysis.
- Less time sensitive data are sent to aggregate nodes for analysis. After analysis is performed, the aggregate node sends a decision or action to the device through the nearest node. aggregate fog node takes seconds or minutes to complete the analysis. the aggregate node later sends the report to cloud for future analysis purpose.
- The time insensitive data can wait for a longer duration. The data is sent to cloud for storage and future analysis.

5. Explain public cloud deployment model and list its advantages and disadvan-

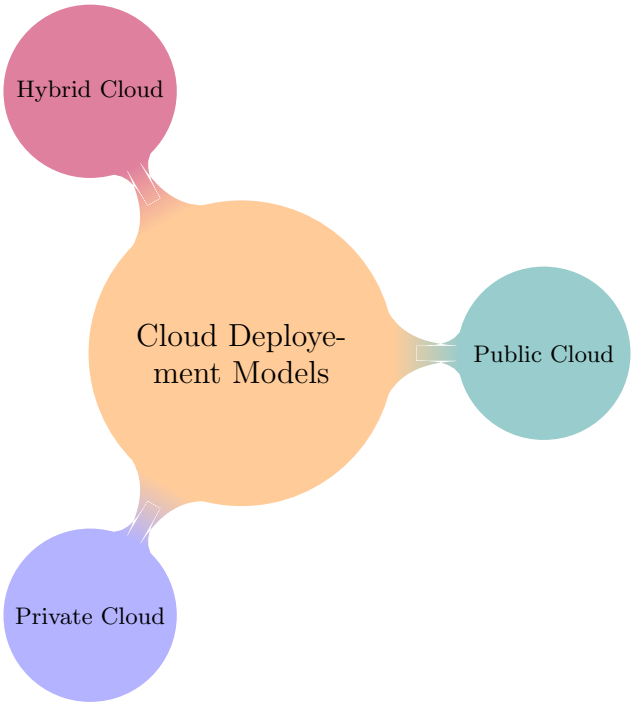


Figure 4.3: Various cloud deployment models

tages.

- Public Cloud Deployment is meant for general purpose or a large group.
- The cloud service provider owns all the resources which include hardware or infrastructure and software.
- Cloud service provider (eg.,Amazon,Microsoft)will take care of all the resource management such as Installation, maintenance,upgradation and monitoring.
- Access to this cloud service happens via the Internet.
- The biggest advantage of this approach is the ease of usage and it being inexpensive compared to private cloud deployment.
- The pay and use approach makes it easier for the cloud service consumer. Moreover you will get 24x7 customer support for technical and other related clarifications when you opt for this deployment .
- However, security and privacy issues are the major challenges.

Advantages:

- A simple approach where user needs to pay for what he has used (pay and use system).
- No investment in hardware or infrastructure is required.
- Customer support team can be reached on demand and team tries to resolve the challenges.

- It can be easily scaled up or scaled down based on requirements.

Disadvantages:

- Data is not within the walls of the organisation or user.
- Securing the data while ensuring privacy.

6. **Explain the procedure of generating an AIO key?**
The Adafruit IO key (AIO) key is used to authenticate one's client connection with the Adafruit IO system. To understand this we need to understand we should first understand the insights of Adafruit cloud service.

Creation of Account:

- The very first step to access the cloud service is to create an account.
- Visit `https://io.adafruit.com`, which is the homepage of Adafruit.
- On the homepage at the top right corner, find the button *"Get Started for free"*.
- Click on the webpage and your details need to be filled.
- After filling the details ,click on the *"Create Account "* tab to create your own account.
- Come back to the home page to sign in to your own account.

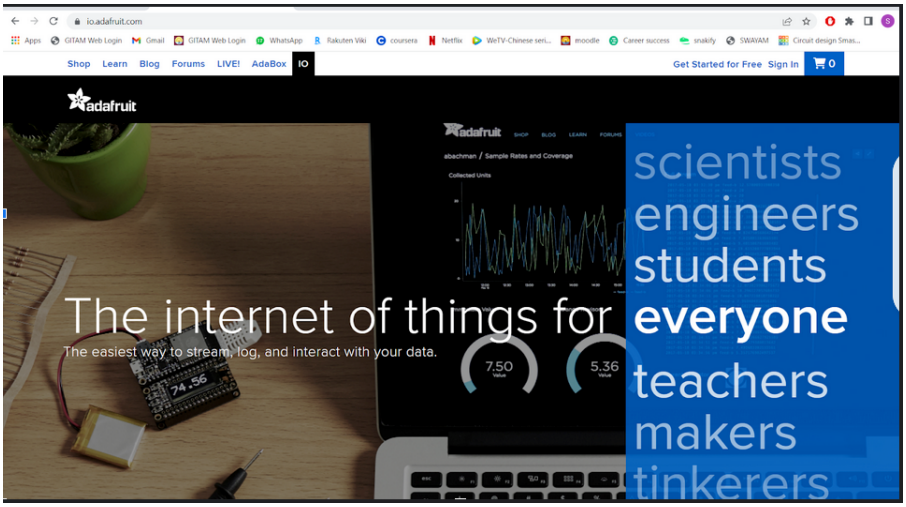


Figure 4.4: Signup an account in Adafruit

Generation of AIO key:

- For every account created there will be a unique asynchronous input output (AIO) key that is used by the program to identify the account without any error.
- The AIO key is a prerequisite for every code and leaving this field empty may lead to misidentification of the account.
- By clicking on the "view AIO key" it can be viewed.

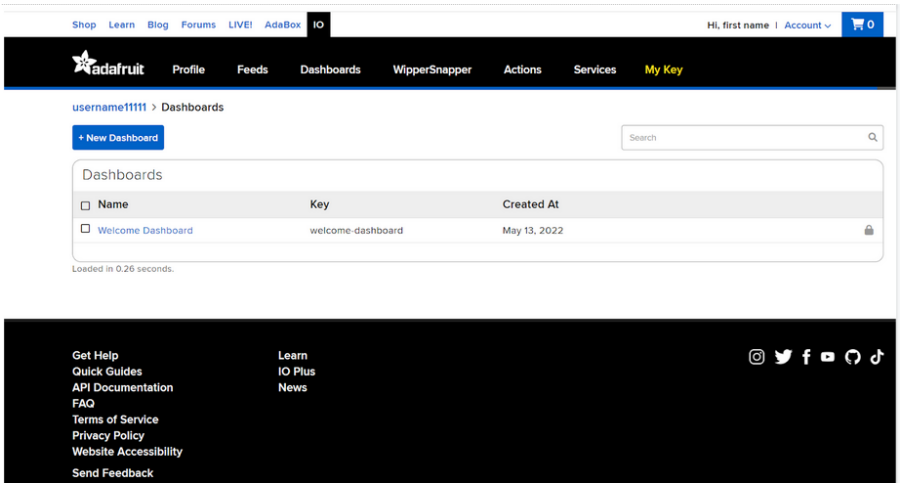


Figure 4.5: Dashboard of Adafruit

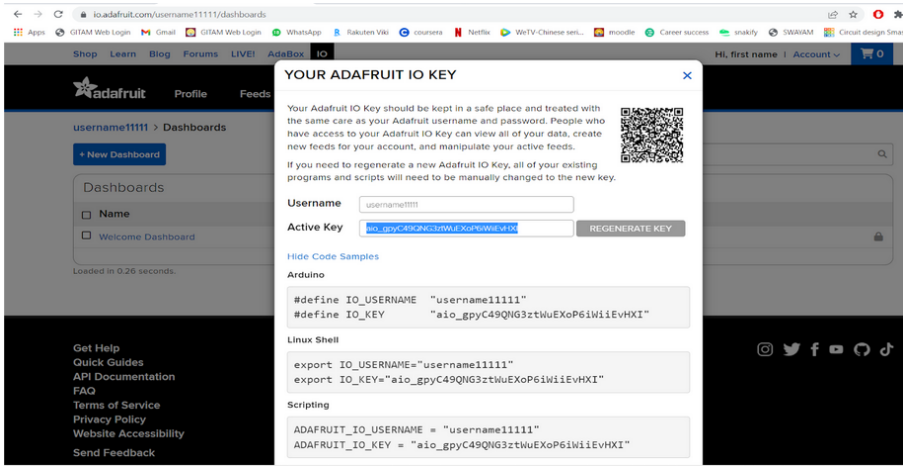


Figure 4.6: Adafruit IO Key

- The AIO key must be copied and preserved for future use.However, it can be regenerated for future use.

7. List the benefits and limitations of using fog computing models? <u>Benefits:</u>

- **Privacy**

  Fog computing can be used to control the extent of privacy. Any sensitive data of the user can be analyzed locally instead of sending them to a centralized cloud infrastructure. Through this way the team of IT will be able to track and control the respective device. Furthermore if any subset of data needs to be analyzed it can be sent to the cloud.

- **Productivity**

  If customer needs to make the machine function according to the way they want, they can utilize fog applications. These fog applications can be easily made by the developers with the right set of tools. After the development has taken place it can

be deployed whenever they want.

- **Security**
  Fog computing has the capability to connect multiple devices to the same network. Because of this the operations take place at various end points in a complex distributed environment rather than a centralized location. This makes it easier to identify potential threats before it effects the whole network.
- **Bandwidth**
  The bandwidth required for transmitting data can be expensive depending upon the resources. Due to the fact that the selected data can be processed locally instead of sending it to the cloud, there are very less number of bandwidth requirements. This bandwidth savings will be specially beneficial when increasing the number of IoT devices.
- **Latency**
  Another benefit of processing selected data locally is the latency savings. The data can be processed at the nearest data source geographically closer to the user. This can produce instant responses especially for the time sensitive services.

Limitations:

- **Complexity**
  Due to its complexity, the concept of Fog computing can be difficult to understand. There are many devices located at different locations storing and analyzing their own set of data. This could add more complexity to the network. In addition to that there are more sophisticated fog nodes present in a fog infrastructure.
- **Security**
  As mentioned earlier there are numerous devices and different fog nodes be present in a fog computing architecture. There are chances for these fog nodes to be in a less secure environment. Hackers can easily impose fake IP address in them gaining access to the respective fog node. Or else they increase the risk of corrupted files infiltrating the main data stream infecting both the device and the company. This makes them vulnerable to Man-in-the-middle attacks.
- **Authentication**
  Service offered by a fog computing is of large scale. The fog computing is comprised of end users, internet service providers and cloud providers. This can often rise trust and authentication issues in the fog.
- **Maintenance**
  Unlike cloud architecture, where maintenance is made seamless, it is not so in fog. Since controllers and storages are distributed across various locations in the network it needs more maintenance. The fog architecture is decentralized for processing.

- **Power Consumption**
  The number of fog nodes present in a fog environment is directly proportional to the energy consumption of them. Which means that these fog nodes require high amount of energy for them to function. As there are more fog nodes in a fog infrastructure there are more power consumption as well. Most companies often try to lower their cost using these fog nodes.

8. **List the criteria for selection of cloud service provider and explain at least four criteria.**

- **Certification and Standards compliance:**
  When a product adheres to the standard that is accepted widely, it is considered a reliable product . Similarly , cloud service providers(CSP)are also expected to comply with standards. This compliance with industry accepted standards is the first criteria to select CSP. Though there are many standards framed and followed by the industry, some main standards for cloud are ISO,OCC,IEEE,SNIA etc.
- **Financial Status of Service Provider:**
  The service provider should hold sufficient money/funding to operate for a long period.If the service provider has healthy financial status and history of sustenance, then it is most likely to shut down.
- **Business and Technology skills:**
  Having the technical expertise to sustain and adapt to a client's requirements is a key factor in selecting a CSP. Having just the technical skill and strength does not help; the CSP needs business as well to sustain.Business skills include growth planning,financial planning,and other factors that are required to sustain in the market.Hence, Sustenance = Technology + Business Skills
- **Compliance Audit:**
  The CSP must validate compliance with the client's requirement , which should be done through a proper third party audit.This will enable transparency and perfect validation.
- **Service level agreements:**
  SLA's provide details and information about the service provided and the real value that a customer get out of them. They serve as a contract between the 2 parties. They define terms and conditions and also the legal aspects of the contract relationship between the two parties.
- **Reporting/Tracking:**
  The service provider should be capable of issuing a comprehensive performance report also highlights the shortfalls . this will enable the customer to understand the complete situation.

- **Costing and Billing:**
  The cost and billing should be transparent and should provide the complete details for usage. Also ,it is expected to be automated with details of the complete resource utilization. It should not come as a shock to a customer to see the bill with a huge amount mentioned, without having clarity on the breakup. This means the billing should be transparent and for the usage only. This is a major factor in selecting the CSP.
- **Maintenance monitoring and Upgrade:**
  It should be easy and less expensive to migrate to CSP's environment . Also, when there is an upgrade , it should be done with ease. Any maintenance should be easy and affordable. In short, it should be easier to install,manage,maintain,and upgrade. This upgrade includes migration from private to public cloud to hybrid cloud if needed.
- **Support:**
  Help and assistance should be provided when required. Support should be available based on the agreements as a dedicated resource may be needed based on the complexity of the problem. Also, onsite support may be needed when clarifications cannot be offered over phone. Thus,support is a major deciding factor for selection of a service provider.
- **Security:**
  The infrastructure, both software and hardware should be secured. There should be defined politics about the security that should also be shared with a customer. This includes everything from access restrictions to customer data. The data should be safe in case of a breakdown/ failure. The recovery and backup options should be sound. The physical infrastructure has to be safeguarded as well. All these factors would require audit which should be carried out by a third party . Security is the prime concern and cannot be ignored . evaluation should start from this point.

9. Briefly discuss the security aspects of cloud computing

4 Must Have Cloud Computing Security Features.

- **Software Security:** Software is the core component and plays a vital role in presenting and ensuring a secure environment. If there are defects created/generated during the development phase, it is a software security threat. Defects such as simple software implementation defects , memory allocation,design issues, and exception handling all contribute to security issues. Care should be taken to write software for IoT without error/defects. This can be ensured by complete and comprehensive testing carried out at all stages.
- **Infrastructure security:** Making sure that the infrastructure provided by the CSP is safe is a must. The entire data is stored and is dependent on this infrastructure.

Since a third party could also contribute to the infrastructure, it is extremely important to check the security vulnerabilities with the infrastructure. All infrastructure related guidelines should be mentioned clearly in the agreements and should be made transparent to the customer. If data is damaged everything is damaged and lost. Hence, care should be taken to protect the infrastructure.

- **Storage security:** It is important to be informed of who owns the data and location where it is stored. Data leak, snooping,malware attacks, etc, are all threats to the stored data and can be listed under storage security . Appropriate antivirus software and periodic monitoring, should help protect the data.
- **Network security:** Data is stored in the cloud via the Internet, and hence all network threats become a possibility.

10. List the challenges that are faced when iot and clouds are integrated and explain them?

(a) **Privacy and security:** Security is a major concern in the field of IoT. valuable and confidential data goes into the cloud,outside the firewall. The moment the firewall is crossed, this data becomes hackable. There is a possibility that this data could be monitored without informing the user.

Solutions to it

- Periodic monitoring of the network activities, tracking unusual events in the network, opting for private cloud if the data is confidential, and using the recognised antivirus solutions could certainly reduce the risk of being exposed.
- Before signing the contract with a CSP , it is necessary to read and understand the regulations involved in the service being provided.
- The data received is from multiple sensor nodes. It is important to interpret this data in the correct sequence. This will safeguard the data and ensure that it is not stolen.

(b) **Bandwidth cost:** If the IoT application is on a small scale demanding lesser resources , then the requirement for investment in bandwidth would not be too much. In case the application is data-intensive, then investment would be huge. However, IoT is all about data , and in most cases, this would be big data.Hence, there is always a necessity for huge investment.

(c) **Migration and Portability:** The challenges like how safe it is to move the data?, how much downtime would this process require?, how easy is it to move the data? ,etc are the challenges doubled with IoT as the data comes from the sensory nodes at a very high speed.

(d) **Availability,Reliability and Robustness:** In IoT, there is continuous monitoring and reading of the data , so data generation and storage have to be spontaneous.

This forces the need of 24x7 cloud service availability.Also if there is downtime it could miss critical data. Hence , reliability of the process has to be monitored, which decides the effectiveness of the service. Also, the process should be robust towards handling data at different rates. IoT could flood data at any time , while it could slow down sometimes. Both these situations should be handled effortlessly.

(e) **Costing :** One of the main advantages of cloud is that it can scale up with rising demand. While it is scalable and flexible, an organization should plan its budget carefully.if someone opts for subscription without having clear vision and planning, it may lead to unnecessary cost

(f) **Data ownerships:** The data stored by the user on the cloud is owned by the user. This means that the data is under the ownership of the person who generates it. However , when opting for cloud storage(i.e,,public/hybrid/deployment model), the data is under the custody of the cloud service provider. Then it appears that the service provider owns the data. There are still challenges surrounding this debate of data ownership. When it comes to IoT , the data is generated at multiple points and ownership could lie with multiple participating parties. Hence, in IoT the ownership-related challenges are multiplied.

(g) **Expertise:** To use the cloud with IoT requires a special skill set. The cloud platform gets updated every now and then and so experts have to constantly upgrade themselves. This is a definite challenge. When it comes to IoT, the challenge lies with understanding the sensors and at the same time , getting updated on cloud development.

5. Data Analytics and Application Building with IoT

5.1 Syllabus

5.1.1 Data Analytics

1. visualising the Power of Data from IoT
2. Data Analysis
3. Machine Learning
    - supervised learning
        - semi-supervised learning
        - Active learning
        - Reinforcement learning
    - unsupervised learning
4. Types of Machine Learning Models
    - Classification
    - Regression
    - Clustering
5. Model Building Process.
    - Training the model
    - Testing the model
    - validation of the model
6. Modelling Algorithms
    - Decision Tree
    - Linear Regression

- Logistic Regression
- K-Means

7. Model Performance.

5.1.2 Application Building with IoT

1. Smart Perishable Tracking with IoT and Sensors
2. Smart Healthcare – Elderly Fall Detection with IoT and Sensors
3. IoT–Based Application to Monitor Water Quality
4. Smart Warehouse Monitoring, Smart Retail

5.2 Short Answer Questions

1. **List the reasons why data analysis is important in IoT?**
   data analysis aims at extracting valuable insights from a given data. Even though there is a huge abundance of data nowadays, it is present in inconsistent form. Data analysis helps to clean and transform all this data into a consistent form, a easily digestible format so it can be effectively studied, (i.e) it becomes ready to use.

2. **List the types of exploratory data analysis?**
   There are four types of EDA:
   (a) Uni variate Non-graphical
   (b) Multivariate Non-graphical
   (c) Uni variate graphical
   (d) Multivariate graphical

3. **Mathematically how to calculate precision from TP and FP during model performance evaluation?**
   Precision calculation in terms of TP and FP:

$$Precision = \frac{TP}{TP + FP} \tag{5.1}$$

4. **What is Gini impurity in a decision tree?**
   Gini impurity is the measure of the level of impurity at the node. It is a measure of probability of correctly labelling a random data point based on the distribution of data point within the node. It is calculated by the sum of square of probability of every output class value subtracted from one.

$$Gini(node) = 1 - \sum_{j=1}^{c} p(j)^2 \tag{5.2}$$

5. **Explain reinforcement learning.**
   reinforcement learning is a feedback-based learning process. Here, the input does not need to have labelled date. Instead, the model learns by interacting with the environment and getting feedback from it. It learns if each of it's decision is right or wrong based on the feedback. Reinforcement learning is commonly used in robots and computer games.

6. **Explain Data analysis in IOT & List few examples of data analysis**
   Data analysis in IoT is called IoT analytics. It is the application of data analysis tools and procedures to realize value from the huge volumes of data generated by connected Internet of Things devices. some common applications of IoT analytics are:

   - Predictive Maintenance
   - Vehicle Telematics
   - Smart Buildings
   - Product Monitoring
   - Smart Devices and Wearable
   - Smart Metering

7. **What is exploratory data analysis?**
   Exploratory Data Analysis refers to the critical process of performing initial investigations on data so as to discover patterns,to spot anomalies,to test hypothesis and to check assumptions with the help of summary statistics and graphical representations. It is achieved using Descriptive statistical methods. EDA is performed on clean data.

8. **Draw the sample confusion matrix for a Yes No class value.**

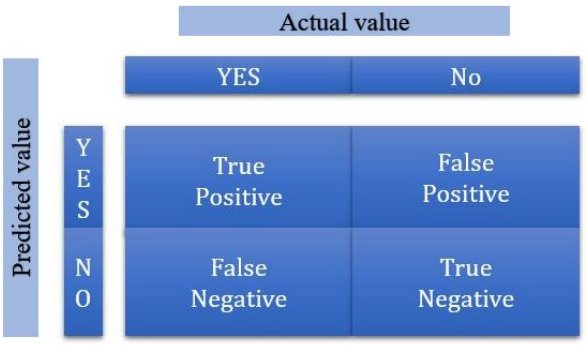


Figure 5.1: Confusion matrix for a Yes or No class value

9. **Mathematically how to calculate sensitivity from TN and FP during model performance evaluation?**

   sensitivity also called as recall is given by:

$$Recall = \frac{TP}{TP + FN} \tag{5.3}$$

   where TP=True Positive, the no.of observations that were real and the model predicts them to be true FN=False Negative, the no.of observations that were real but, the model predicts them to be false

   It is the ratio of correctly predicted out of the actually positive class.

10. **List three modelling techniques used for machine learning in IOT.**
    The three modelling techniques for machine learning in IoT are:

    (a) Classification (supervised)

    (b) Regression (supervised)

    (c) Clustering (unsupvervised)

5.3 Long Answer Questions

1. **What are two types of machine learning algorithm Explain and elaborate.?**
   These are three types of machine learning:

   (a) Supervised learning

   (b) Unsupervised learning

   Supervised learning, as the name indicates, has the presence of a supervisor as a teacher. Basically supervised learning is when we teach or train the machine using data that is well labelled. Which means some data is already tagged with the correct answer. After that, the machine is provided with a new set of examples(data) so that the supervised learning algorithm analyses the training data(set of training examples) and produces a correct outcome from labelled data.

   Supervised learning is classified into two categories of algorithms:

   (a) **Classification:** A classification problem is when the output variable is a category, such as “Red” or “blue” , “disease” or “no disease”.

   (b) **Regression:** A regression problem is when the output variable is a real value, such as “dollars” or “weight”.

   Supervised learning is also classified into three categories.

(a) Semi supervised learning

(b) Active learning

(c) Reinforcement learning

Advantages:

- Supervised learning allows collecting data and produces data output from previous experiences.
- Helps to optimize performance criteria with the help of experience.
- Supervised machine learning helps to solve various types of real-world computation problems.

Disadvantages:

- Classifying big data can be challenging.
- Training for supervised learning needs a lot of computation time. So, it requires a lot of time.

Unsupervised learning is the training of a machine using information that is neither classified nor labeled and allowing the algorithm to act on that information without guidance. Here the task of the machine is to group unsorted information according to similarities, patterns, and differences without any prior training of data.

Unlike supervised learning, no teacher is provided that means no training will be given to the machine. Therefore the machine is restricted to find the hidden structure in unlabeled data by itself.

It allows the model to work on its own to discover patterns and information that was previously undetected. It mainly deals with unlabelled data.

Unsupervised learning is classified into two categories of algorithms:

(a) **Clustering:** A clustering problem is where you want to discover the inherent groupings in the data, such as grouping customers by purchasing behavior.

(b) **Association:** An association rule learning problem is where you want to discover rules that describe large portions of your data, such as people that buy X also tend to buy Y.

Advantages:

- Labeling of data demands a lot of manual work and expenses. Unsupervised learning solves the problem by learning the data and classifying it without any labels.

- The labels can be added after the data has been classified which is much easier.
- It is very helpful in finding patterns in data, which are not possible to find using normal methods.

Disadvantages:

- The result might be less accurate as we do not have any input data to train from.
- The model is learning from raw data without any prior knowledge.
- The more the features, the more the complexity increases.

2. Explain step by step process of building a machine learning model.

Although different types of machine learning will have different approaches to training the model, there are basic steps that are utilised by most models. The steps in building a supervised learning based model are

(a) **Training the model** : Majority of learning takes place in the training phase. The model takes the key-value pair and trains based on the algorithm. The algorithm will change from model to model. How much more data is used to train, the more accurate will be the model.

(b) **Testing the model** : In machine learning, model testing is referred to as the process where the performance of a fully trained model is evaluated on a testing set.The testing set consisting of a set of testing samples should be separated from the both training and validation sets, but it should follow the same probability distribution as the training set. Once a model has been trained, performance is gauged according to a confusion matrix and precision/accuracy metrics.

(c) **Validation of the model** : This step estimates the accuracy of the model built in. The output of the previous step is the final model built from the training data. For calculating the model's performance, few data points are fed in and the prediction accuracy of the model is observed. Usually this step is done on 30 percent of available training data. In this phase "key" is not exposed and the "value" is fed and the model is allowed to predict. The prediction is compared with the actual values of the dependent variables. If model predicts 80 percent correctly, the accuracy is 80 percent and so on. The validation data set should not be used for training and testing phase. Few modelling algorithms are

- Logistic regression
- Linear regression
- Decision tree

3. List the matrices that help to assess the performance of machine learning model and explain them.

A confusion matrix is a tabular way of visualizing the performance of the prediction model. Each entry in a confusion matrix denotes the number of predictions made by the model where it classified the classes correctly or incorrectly.

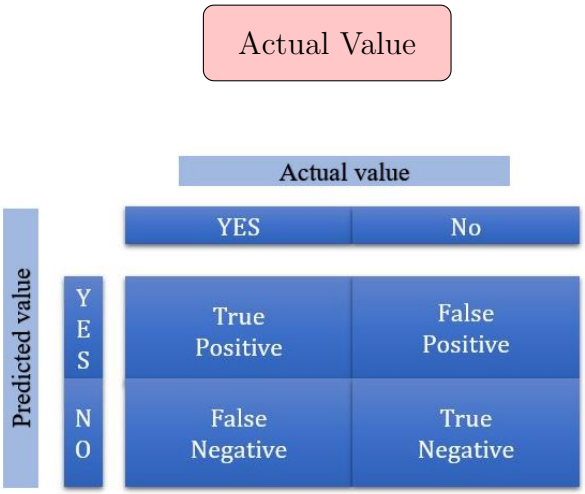


Figure 5.2: Confusion matrix for a Yes or No class value

this figure shows a sample confusion matrix for a model whose distinct class values are "Yes" and "No". the columns of the matrix are the actual class values, the rows of the matrix are the possivle class values. In an ideal case, the confusion matrix is a square matrix. On the contrary, models which couldn't perform properly either create a new class of objects and classify a few observations under this, or clubs together two or more actual classes leading to fewer predicted classes.

Every data point is placed in M[Actual Class][Predicted Class]. Whenever a data point is predicted correctly, it means that Predicted Class=Actual Class, which means that they lie on the diagonal of the confusion matrix.

the four entries of the given matrix are defined as follows:

(a) **True Positive (TP):**
Data points that are actually "Yes" and are predicted to be under class "Yes".

(b) **True Negative(TN):**
Data points that are actually "No" and predicted "No". These are negatives rightly identified.

(c) **False Positive(FP):**
Data points that are actually "No" but predicted "Yes" These are false predictions giving alert for non-exixting things. This is an error, but of less severity.

(d) **False Negative(FN):**
Data points that are actually "Yes" but predicted "No". These are missing problems.

This is more severe error compared to FP.

Of all these entries, TP and TN are the right predictions. From this confusion matrix entries, the following metrics have beend developed to assess the performance of a Machine Learning Model.

(a) **Accuracy**
Accuracy of the model is the ratio of the number of right predictions to the total number of predictions.

$$Accuracy = \frac{TP + TN}{N} \tag{5.4}$$

where N=TP+TN+FP+FN

(b) **Precision**
Precision of a model is defined as the ratio of correctly predicted data out of the positively predicted data. precision can also be seen as the accuracy of positive predictions. Precision should be as high as possible. Precision can be low if there is insufficient data in the training data set. Mathematically,

$$Precision = \frac{TP}{TP + FP} \tag{5.5}$$

the lower the value of FP, the better the model's performance is said to be.

(c) **Recall or Sensitivity**
it is the ratio of correctly predicted out of the positively predicted. Recall should be as high as possible.

$$Recall = \frac{TP}{TP + FN} \tag{5.6}$$

it also called sensitivity of the model.

(d) **Specificity** it is the ratio of correctly predicted class from the actual negative class.

$$Specificity = \frac{TN}{TN + FP} \tag{5.7}$$

this metric is used in evaluating the bias of data in the training data set.

by taking into account the values of all these metrics, the model can be better fine-tuned to produce reliable prediction values.

4. **How does classification algorithm handles continuous features.**

(i) Decision tree is a classification algorithm that handles continuous features.

(ii) It takes in a set of features(dependent variable) and predicts the value of the output(independent variable).

(iii) The input features may be continuous, but the output variable will always be categorical.

(iv) The main logic behind building a decision tree is that data can be iteratively split into two at each node.

(v) All the data points with one answer to a question are segregated and passed to the left child, and the ones with another answer are passed to the right child.

(vi) Thus it becomes imperative to identify the appropriate question at every node.

(vii) The question in the node should not be repeated in its direct child, but can be repeated in in any of it's descendants.

(viii) There can be multiple options for questions at each node. The question is identified with help of two metrics.

- Gini Impurity
- Gain Value

(ix) Gini is a measure of probability of correctly labelling a random data point based on the distribution of data point within the node.

(x) It is calculated by the sum of square of probability of every output class value subtracted from one. Gini Impurity is defined as

$$Gini(node) = 1 - \sum_{j=1}^{c} p(j)^2 \tag{5.8}$$

It means the data points in the node have j different values for the output class variable.

(xi) There can be multiple options for questions at each node, out of which we can select one based on Gini.

(xii) Similarly Impurity level at the leaf node can also be calculated. This loop should continue till the impurity at a leaf node gets zero.

(xiii) It should be noted that the impurity level at the node must always be higher than impurity at the children, as the decision tree continuously segregates data into individual class values.

(xiv) For every possible question at a node there is an information gain value. The question with maximum information gain value is best question for the node.

(xv) The gain formula is

$$Gini(question) = Gini(currentnode) - [p(left) * Gini(left) + p(right) * Gini(right)] \tag{5.9}$$

(xvi) This gives the difference of impurity at the current node to the weighted average of impurity at the child nodes.

(xvii) These metrics are used in the classification and regression algorithm.

5. **Propose a system for retail business to manage customer relationship in a smart manner. Draw the workflow of proposed system and explain each step.**

The role of IoT is important in two aspects: First making the entire retail infrastructure smart and second making the customer relationship smart.

Key tools for enhancing customer relationship:-

Feedback is very important for any business to sustain. A customer can be retained by listening tohis/her feedback. If taken care of properly a customer can bring many other customers. Getting proper customer feedback is essential to understand where and how the business stands. Feedback is also helpful in understanding and predicting the market.

We can improve the feedback collection process by connecting it directly to the customer. A comprehensive IoT based real-time feedback collection with data analytics is the choice

The app and Web interface for easier access can be provided. One can understand the trend/fall of business in detail.

Since Sensors and IoT components are not expensive the approach is quite commercial.

The system uses Iot, sensors and data analytics to receive and understand customer feedback to accelerate business .The system of collecting feedback through simple equipment which has buttons to reflect the service quality should be deployed at all important points. It should be an easy and intuitive device, and not requiring customer to spend much time to give his/her feedback. The feedback system should have HAPPY, OKAY, UNHAPPY, TERRIBLE buttons which could be connected to the sensors. The input would be recorded and then sent to the cloud, which could be analysed immediately. Also if a customer presses the UNHAPPY or TERRIBLE button, immediate attention can be paid to customer at his/her current location in the retail store,

Feedback customer feedback is very important for any business to sustain. getting proper feedback is helpful in understanding and predicting the market. A comprehensive IoT-based real-time feedback collection with data analytics is an effective choice. An app and web infrastructure can be used for easier access. This is quite an economical setup since IoT sensors are not very expensive. the workflow of the proposed system is presented in the following figure. the system consists of collecting feedback through simple equipment with buttons to reflect the service quality and should be deployed at all the important points. The device should be easy and intuitive to use. The inputs and data will be sent to the could which an be analysed immediately.

Insights from this data can prove to be helpful in understanding the customer's latent needs

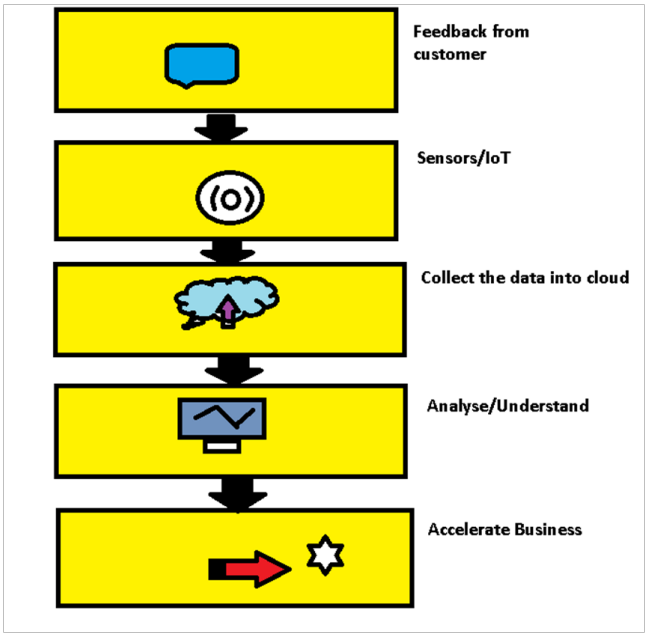


Figure 5.3: Workflow of the proposed system for retail business

and make the appropriate improvements. this kind of system ensures that no feedback either positive or negative would go unnoticed. everything is recorded and uploaded in real-time.

6. **List the areas in a retail business store where IoT can make retail smarter. Proposed a system and explain each areas.**
The areas where IoT can help in making retail smarter are listed below and shown in figure 5.4

   (a) surveillance and security having human security and surveillance system is expensive and may not be perfectly reliable. So, we can have an IoT ecosystem with smart cameras that upload their feed directly to a display unit, which can be monitored over by a human.

   (b) Alert and Alarms in case of fire accidents or circuit-shorting, a IoT based smart alert system can be installed which can alert the people inside of the danger and get them to safety in time. Since the whole process is automated, no person will have to take up the responsibility of manually turning on the alarm systems

   (c) Energy saving In modern retail stores, energy saving is of prime importance as it can take up a chunk of the store's expenditure. so, we can have a smart human & motion detection system which can turn on/off lighting equipment in a store based on the human activity.

   (d) Hygiene and parking In malls, where the number of customer is usually high, maintaining hygiene at restrooms becomes a tedious task. This can be made easier by

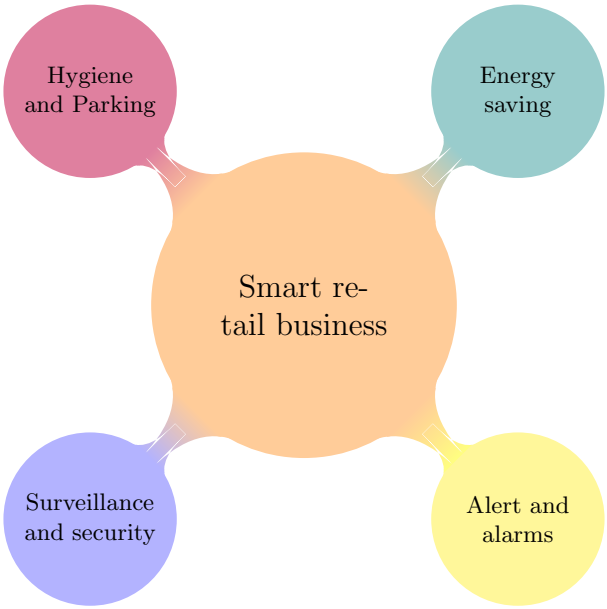


Figure 5.4: The areas in retail store where IoT can make retail smarter

installing smart flushing and sanitation systems which periodically clean the commode(of course, in the absence of humans). Parking and ticket allotment can also be made smart, thus reducing the expenditure of having human valets.

7. **Design a confusion matrix model whose output variable can have three different values "CAT", "DOG" and "RAT".**

A confusion matrix is a tabular way of visualizing the performance of your prediction model. Each entry in a confusion matrix denotes the number of predictions made by the model where it classified the classes correctly or incorrectly.

Given that we have three classes. and Ideal confusion matrix would have three classes both for the actual and predicted values, thus forming a 3X3 square matrix

the performance metrics are given by:

(a) **Total True Positive** ‘

$$TP_{Cat} = CC \tag{5.10}$$

$$TP_{Dog} = DD \tag{5.11}$$

$$TP_{Rat} = RR \tag{5.12}$$

$$TP_{Overall} = TP_{Cat} + TP_{Dog} + TP_{Rat} = CC + DD + RR \tag{5.13}$$

(b) **Total False Positive** ‘

$$FP_{Cat} = CD + CR \tag{5.14}$$

$$FP_{Dog} = DC + DR \tag{5.15}$$

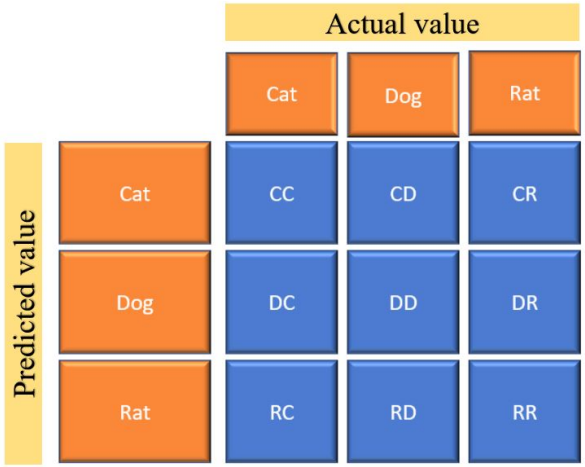


Figure 5.5: confusion matrix for given three classes

$$FP_{Rat} = RC + RD \tag{5.16}$$

$$FP_{Overall} = FP_{Cat} + FP_{Dog} + FP_{Rat} = CD + CR + DC + DR + RC + RD \tag{5.17}$$

(c) **Total False Negative** ‘

$$FN_{Cat} = DC + RC \tag{5.18}$$

$$FN_{Dog} = CD + RD \tag{5.19}$$

$$FN_{Rat} = CR + DR \tag{5.20}$$

$$FN_{Overall} = FN_{Cat} + FN_{Dog} + FN_{Rat} = DC + RC + CD + RD + CR + DR \tag{5.21}$$

(d) **Total True Negetive** ‘

$$TN_{Cat} = DD + DR + RD + RR \tag{5.22}$$

$$TN_{Dog} = CC + CR + RC + RR \tag{5.23}$$

$$TN_{Rat} = CC + CD + DC + DD \tag{5.24}$$

$$TN_{Overall} = 0 \tag{5.25}$$

(e) **Accuracy**

Accuracy of the model is the ratio of the number of right predictions to the total number of predictions.

$$Accuracy = \frac{CC + DD + RR}{N} \tag{5.26}$$

where N=CC+CD+CR+DC+DD+DR+RC+RD+RR

(f) **Precision**

Precision of a model is defined as the ratio of correctly predicted data out of the positively predicted data. precision can also be seen as the accuracy of positive predictions. Precision should be as high as possible. Precision can be low if there is insufficient data in the training dataset. Mathematically, we have 3 kind of precisions here.

$$Precision(Cat) = \frac{CC}{CC + CD + CR} \tag{5.27}$$

the lower the value of CD+CR, the better the model's performance is said to be. similarilty, the precisions for the other three observations are as f

$$Precision(Dog) = \frac{DD}{DD + DC + DR} \tag{5.28}$$

$$Precision(Rat) = \frac{RR}{RR + RC + RD} \tag{5.29}$$

(g) **Recall or Sensitivity**

it is the ratio of correctly predicted out of the positively predicted. Recall should be as high as possible.

$$Recall = \frac{TP}{TP + FN} \tag{5.30}$$

it also called sensitivity of the model.

(h) **Specificity** it is the ratio of correctly predicted class from the actual negative class.

$$Specificity = \frac{TN}{TN + FP} \tag{5.31}$$

this metric is used in evaluating the bias of data in the training dataset.

8. **Demonstrate a fall detection system that is smart enough to take care of elderly people using IoT, Sensors and data analytics.**

The national Council on Aging(NCOA) states that the rate of deaths in the elderly population has reached a critical state and that once every eleven seconds an elderly person is being treated fro a fall. Moreover and elderly person dies due to falling once every 90 minutes. Most of the elderly people suffer from back pain, joint pain, knee pain they are mostly other ones who can't walk properly. To reduce these types of risks in the elderly people, there is an economical and affordable system that could monitor their movement and detect their fall.

Immediately after a person falls, the system alerts his/her caretaker to take necessary

actions to save him/her. this system uses IoT, sensors and data analytics. This system detects the falls of the elderly, not only in the bedroom but aso in the restroom.

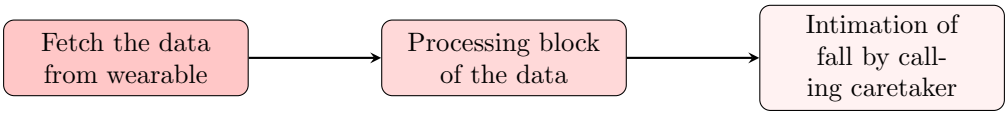


Figure 5.6: Workflow of fall detection system

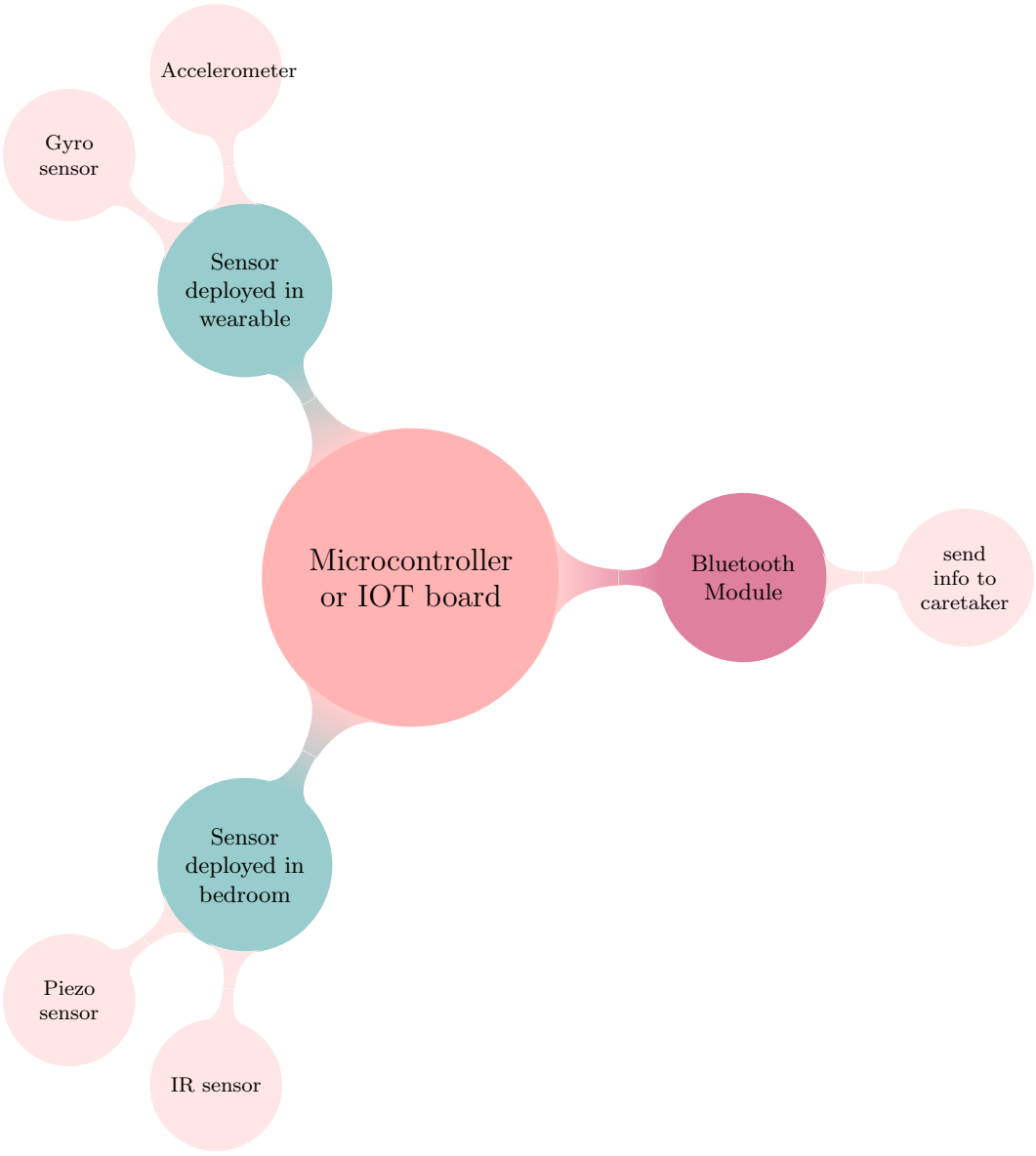


Figure 5.7: Transmitter of fall detection system

Design

(a) An accelerometer(GY-61) sensor and the gyro(MPU-6560) sensor are attached to the proposed wearable.

(b) The wearable has to work on both hands of the elderly person

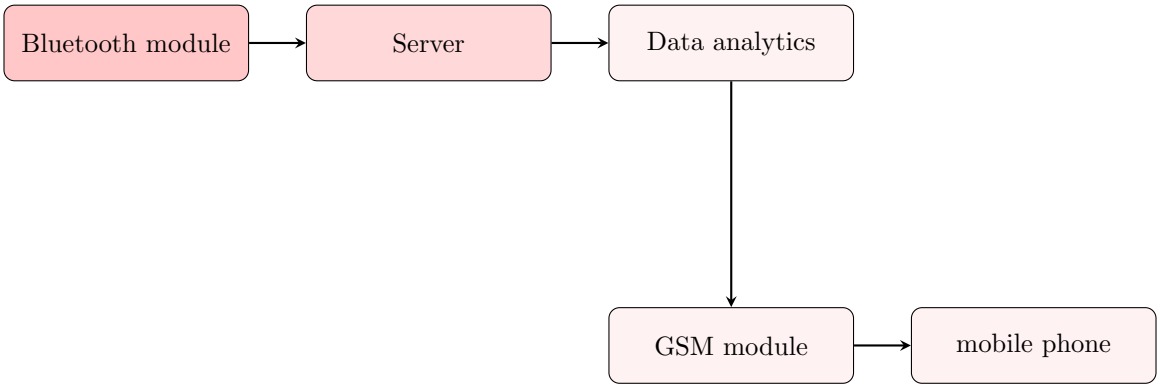


Figure 5.8: Receiver of fall detection system

(c) It can be worn similar to a watch

(d) Having measured the angle change of GY-61 and MPU-6050 with various deliberate falls, we have identified the threshold value for each of these sensors.

(e) The data acquired from these sensors is transmitted via Bluetooth node, which in turn is connected to the micro controller unit. Here we use Arduino Uno R3.

(f) The server receives the data and a graph is plotted for further analysis. the moment the threshold value is sensed, a call is triggered to the elderly person's caretaker calling with an alert message.

(g) A buzzer is also raised to get immediate attention.

(h) If the elderly person goes to the restroom he or she might have to remove the wearable, then the fall may go unnoticed.

(i) To avoid this two IR sensors placed at the entrance of the restroom.

(j) Also piezoelectric plates are implanted at different places of the restroom.

(k) The figure 5.6 shows the workflow of fall detection system.

(l) Transmitter of fall detection system is shown in figure 5.7

(m) receiver of fall detection system is shown in figure 5.8

9. List the limitations of a nodal network method that is helpful in monitoring water quality.

The nodal network method for monitoring water quality is expensive and is thus used selectively, only on certain waterbodies. In India it is used at certain points of Ganga and Yamuna. Sensors are placed at different points in the river and water quality data gathered by the sensors at regular intervals is uploaded in the internet. the nodal network method or the electronic sensor method address the short comings of the traditional method by collecting data in real time. So, this system with a usage of wireless sensor network helps

in constatn and remote monitoring of water quality. It is divided into four broad areas. Each area establishes a cluster containing numerous wireless sensor ndoes accountable for sensing, data collection, processing and communication. the nodal network method, despite doing real-time monitoring of water quality, has the following limitations.

(a) The sensors used in this method are very expensive. They are installed at deeper levels in the river which makes the system less effective

(b) The sensors, which are driven by a power source, may need replacement if found to be malfunctioning. this may incur additional cost

(c) Monitoring the equipment and maintainence of the sensors are also challenging and expensive

(d) through the water sensor network can acquire and serve data in real item , most of the sensors will be lacking mobility as they are fixed in their positions

(e) Natural disasters like floods and movement of aquatic animals in waterbodies may damage the sensors.

10. Present an architecture of a nodal network method that is helpful in monitoring water quality.

The entire process of proposed nodal network system is accomplished through the following four modules:

- Data collection and communication
- Cloud and data analytics
- Data visualization and presentation
- Water status report generation

The working principle of proposed system is listed below.

(a) The multi-parameter water sensors are mounted on an autonomous boat.

(b) Selection of the sensors is based on parameters such as sensitivity, cost, accuracy, latency etc

(c) The points from where water samples are to be taken for quality analysis are chosen at random and their GPS co-ordinate positions are fed into the system. It is ensured that the sample points are selected to cover the entire stretch of the waterbody.

(d) To locate the sample points in the waterbody, a microcontroller unit in the boat interfaces with the GPS module for guidance to navigate to the desired location. To increase its sophistication and to reduce the number of peripherals, compact microcomputing units such as Arduino and Raspberry Pi are utilized.

(e) At various points along the waterbody, water parameters measured are acquired with the help of microcontroller and other sensors mounted on the boat.

The data collected during the course of navigation is sent to the cloud via Wi-Fi/GPRS GSM module for analysis and prediction. In the cloud, the geotagged sensor data is stored as a history of the corresponding waterbody. — To analyse the data in the cloud, machine learning techniques such as clustering and regression are used and a hypothesis is generated over the data log that was initially collected Using the analysed data, the algorithm plots the choropleth map of the waterbody. The generated choropleth maps are stored in the cloud. The map could be easily preted by any end user. The end user can get the updated information about the waterbody via the applications developed for mobile and web platforms. ,

11. Propose a smart, frugal, and feasible solution to perishable management using IoT, Sensors and data analytics.

Transportation and distribution (T&D) of fresh food products is a substantial and increasing part of the economic activities throughout the world. Unfortunately, fresh food T & D not only suffers from significant spoilage and waste, but also from dismal efficiency due to tight transit timing constraints between the availability of harvested food until its delivery to the retailer. Fresh food is also easily contaminated, and together with deteriorated fresh food is responsible for much of food-borne illnesses. There are many technologies coming together to enable substantial automation in logistics operations & real-time quality/contamination monitoring to reduce inefficiencies and food waste. These are the technologies that provide solutions, particularly relative to the cyber aspect. This includes

(a) Food quality sensing

(b) Robust low-power communications to report sensed data in a very challenging environment

(c) real-time monitoring and data collection

(d) Online analytics to drive logistics operations.

Assume that some sensing and communication modules are placed in some of the boxes and pallets that are in transit or stored in some warehouse/distribution/retailing centers.

These modules sense the quality/contamination parameters and deposit them in a local hub by forming a local communication network.

These local hubs send this information to an Analytics & Operations Center (AOC) via long-range cellular communication.

Electronic tagging : The automation crucially depends on the electronic tagging/identification of the items that it handles. In the logistics space, this means we need electronic

tags at all levels.

Environmental Factors : The decay rate is strongly influenced by the environmental parameters such as temperature, humidity, vibration, and so on. Hence suitable sensors are used.

Modeling The Perishability Metric : food quality deterioration as a function of time can be modeled as a function of some measurable parameters related to the reaction that determines the quality loss.

Food Sensing Technologies : Tiny quality sensors can be embedded in food containers for continuous monitoring purposes, such tiny sensors should communicate with each other and dynamically self-organize necessarily to build an online sensing infrastructure.

Communicating Sensed Data : The following technologies can be used

- Magnetic Induction (MI)-based communication
- Radio Frequency Communication (RF)
- Ultrasonic

The architecture is designed to relay all sensed data to the dual-interface anchors and then to the local hub, which in turn sends all data to an Analytics & Operations Center (AOC) via a cellular link for comprehensive analytics and control. The AOC could be hosted in a cloud.

Data Analytics For Proactive Decision Making : Assuming a ubiquitous deployment of the infrastructure in the T&D system, the AOC can collect a fine-grain view of all of the T&D operations including the status, location, and condition of every product in the T&D pipeline. This allows for online analytics of collected data from individual carriers and warehouses, system-wide analysis and optimization across the entire company, and derivation of insights and fine-tuning of the operations based on the offline analysis of historical data.