1. Relationship b/w IoT and Cloud Computing.

Internet of Things (IoT) refers to a system of connected physical objects via the internet. The ‘thing’ in IoT can refer to a person or any device which is assigned through an IP address. A ‘thing’ collects and transfers data over the internet without any manual intervention with the help of embedded technology. It helps them to interact with the external environment or internal states to take the decisions.

What is Cloud Computing?

Cloud Computing offers services to users on a pay-as-you-go model. Cloud providers offer three primary services. These services are outlined below:

- Infrastructure as a Service (IAAS)

Infrastructure as a service (IaaS) is a cloud computing offering in which a vendor provides users access to computing resources such as storage, networking, and servers. Organizations use their own platforms and applications within a service provider’s infrastructure.

- Platform as a Service (PAAS)

Platform as a service (PaaS) is a cloud computing offering that provides users with a cloud environment in which they can develop, manage, and deliver applications. In

addition to storage and other computing resources, users are able to use a suite of prebuilt tools to develop, customize, and test their own applications.

- Software as a Service (SAAS)

Software as a service (SaaS) is a cloud computing offering that provides users with access to a vendor's cloud-based software. Users do not install applications on their local devices. Instead, the applications reside on a remote cloud network accessed through the web or an API. Through the application, users can store and analyze data and collaborate on projects.

https://www.ibm.com/in-en/cloud/learn/iaas-paas-saas

https://www.geeksforgeeks.org/difference-between-iaas-paas-and-saas/

The Relationship between Internet of Things and Cloud Computing

The internet of things has evolved the new concept of the Internet network. This enables communication between several objects which include

- Smart devices
- Mobile devices
- Sensors and others.

The architecture of the Internet of Things provides effective communication between all elements of architecture. The elements could be

- Objects
- Gates
- Network infrastructure
- Cloud infrastructure

There are multiple benefits of using IoT and cloud computing together:

- In a cloud infrastructure, you can deploy applications to process and analyze data quickly and make decisions as soon as possible.
- It is estimated that almost 4.4 trillion GB data is going to generate by the year 2020. This is no doubt that it will put a massive strain on its infrastructure. Hence, there is a need to minimize this huge pressure and find a solution to transfer the data. Cloud computing, on the other hand, provides adequate performance and scalability to store and operate such a huge volume of data.
- IoT and cloud computing has a complementary relationship. While IoT generates large amounts of data, many cloud providers allow data transfer via the internet, that means it facilitates a way to navigate the data.
- Cloud comp uting helps to collaborate in IoT development. Using Cloud platform, IoT developers can store the data remotely and access easily.
- Cloud computing helps to advance analytics and monitoring of IoT devices.
- IoT devices which utilize common APIs and back-end infrastructure can receive important security updates instantly through Cloud as soon as any security breach happens in the infrastructure. This IoT and Cloud computing combined feature is a vital parameter for user security and privacy.

2. Differentiate b/w scalability and elasticity in cloud computing.

	Cloud Elasticity	Cloud Scalability
1	Elasticity is used just to meet the sudden up and down in the workload for a small period of time.	Scalability is used to meet the static increase in the workload.
2	Elasticity is used to meet dynamic changes, where the resources need can increase or decrease.	Scalability is always used to address the increase in workload in an organization.
3	Elasticity is commonly used by small companies whose workload and demand increases only for a specific period of time.	Scalability is used by giant companies whose customer circle persistently grows in order to do the operations efficiently.
4	It is a short term planning and adopted just to deal with an unexpected increase in demand or seasonal demands.	Scalability is a long term planning and adopted just to deal with an expected increase in demand.

Extra (no need to study) -

Cloud Elasticity :

The Elasticity refers to the ability of a cloud to automatically expand or compress the infrastructural resources on a sudden-up and down in the requirement so that the workload can be managed efficiently. This elasticity helps to minimize infrastructural cost. This is not applicable for all kind of environment, it is helpful to address only those scenarios where the resources requirements fluctuate up and down suddenly for a specific time interval. It is not quite practical to use where persistent resource infrastructure is required to handle the heavy workload.

It is most commonly used in pay-per-use, public cloud services. Where IT managers are willing to pay only for the duration to which they consumed the resources.

Example :

Consider an online shopping site whose transaction workload increases during festive season like Christmas. So for this specific period of time, the

resources need a spike up. In order to handle this kind of situation, we can go for Cloud-Elasticity service rather than Cloud Scalability. As soon as the season goes out, the deployed resources can then be requested for withdrawal.

Cloud Scalability :

Cloud scalability is used to handle the growing workload where good performance is also needed to work efficiently with software or applications. Scalability is commonly used where the persistent deployment of resources is required to handle the workload statically.

Example :

Consider you are the owner of a company whose database size was small in earlier days but as time passed your business does grow and the size of your database also increases, so in this case you just need to request your cloud service vendor to scale up your database capacity to handle a heavy workload.

It is totally different from what you have read above in Cloud Elasticity. Scalability is used to fulfill the static needs while elasticity is used to fulfill the dynamic need of the organization. Scalability is a similar kind of service provided by the cloud where the customers have to pay-per-use. So, in conclusion, we can say that Scalability is useful where the workload remains high and increases statically.

3. How is fog computing different from cloud computing.

   https://www.geeksforgeeks.org/difference-between-cloud-computing-and-fog-computing/

Feature	Cloud Computing	Fog Computing
Latency	Cloud computing has high latency compared to fog computing	Fog computing has low latency
Capacity	Cloud Computing does not provide any reduction in data while sending or transforming data	Fog Computing reduces the amount of data sent to cloud computing.
Responsiveness	Response time of the system is low.	Response time of the system is high.
Security	Cloud computing has less security compared to Fog Computing	Fog computing has high Security.
Speed	Access speed is high depending on the VM connectivity.	High even more compared to Cloud Computing.
Data Integration	Multiple data sources can be integrated.	Multiple Data sources and devices can be integrated.
Mobility	In cloud computing mobility is Limited.	Mobility is supported in fog computing.
Location Awareness	Partially Supported in Cloud computing.	Supported in fog computing.
Number of Server Nodes	Cloud computing has Few number of server nodes.	Fog computing has Large number of server nodes.
Geographical Distribution	It is centralized.	It is decentralized and distributed.
Location of service	Services provided within the internet.	Services provided at the edge of the local network.
Working environment	Specific data center building with air conditioning systems	Outdoor (streets,base stations, etc.) or indoor (houses, cafes, etc.)
Communication mode	IP network	Wireless communication: WLAN, WiFi, 3G, 4G, ZigBee, etc. or wired communication (part of the IP networks)

4. Difference b/w cyber-physical systems and machine-to-machine devices.

Technology

– Cyber-physical systems (CPS) are intelligent engineered systems that seamlessly integrate computation, networking and physical processes. It is a system that combines physical with cyber components, potentially networked and tightly interconnected, providing the foundation for IoT. Internet of Things (IoT) is a catch-all term for the growing number of physical devices around the world that are connected to the internet and eventually to each other. IoT is a networked world of interconnected devices, objects, and people.

Focus

– The concept of cyber-physical systems is a generalization of embedded systems. These systems are concerned with how physical systems can be controlled and monitored using the cyber space. In practical terms, this integration takes into account both the cyber part and the physical part working together. IoT, on the other hand, represents a more evolved

state where physical and digital worlds are blended into a single space. It is focused on how these physical objects can be connected to the internet to do something meaningful.

Mechanism

– Cyber-physical systems are smart embedded systems that integrate sensor networks with embedded computing to monitor the physical environment. The mechanism is controlled and monitored by computer-based algorithms. With human assistance, these systems can autonomously evaluate operational conditions and subsequently support decision-making. IoT, on the other hand, is purely automation meaning no human intervention is required.

Scope

– The IoT is on the level of physical objects and it is concerned with building Omnipresent connection in the physical space. The scope of IoT is not limited to just connecting things; it allows these things to communicate and exchange data, which can be analyzed and processes further into meaningful information. Cyber-physical systems integrate actuators or sensors with networking technologies. Sensors and actuators work in the feedback loop using human intervention so that their behavior could be changed based on user's requirements.

5. Differentiate b/w point to point and point to multipoint connection

BASIS FOR COMPARISON	POINT-TO-POINT	MULTIPOINT
Link	There is dedicated link between two devices.	The link is shared between more than two devices.
Channel Capacity	The channel's entire capacity is reserved for the two connected devices.	The channel's capacity is shared temporarily among the devices connected to the link.
Transmitter and Receiver	There is a single transmitter and a single receiver.	There is a single transmitter and multiple receivers.
Example	Frame relay, T-carrier, X.25, etc.	Frame relay, token ring, Ethernet, ATM, etc.

Sr. No.	Key	Point-to-Point Communication	Multi-point Communication
1	Definition	Point-to-point communication is the communication in which the channel of communication is shared only between two devices or nodes.	On other hand Multi-point communication is the communication is which the channel of communication is shared not only between two devices or nodes but it is shared between multiple devices or nodes which are taking part in it.
2	Load sharing	As mentioned above in case of Point-to-point communication the channel is only between two nodes so the load and capacity of the channel is divided or available only to two nodes.	On other hand in case of Multi-point communication the channel capacity is divided between multiple participant nodes.
3	Parties involved	In case of Point-to-point communication only two parties get involved one as Sender and other as Receiver.	While on other hand in case of Multi-point communication there could be multiple parties however role of parties could either be sender or receiver and some parties may behave as like both.
4	Reliability	As Point-to-point communication involves only two parties and chances for information modulation is very less hence this type of communication is more reliable as compared to Multi-point communication.	On other hand due to multiple parties involvement the chances for information modulation is more and hence Multi-point communication is comparatively less reliable as compared to Point-to-point communication.
5	Error Prone	Point-to-point communication is more error prone as compared to Multi-point communication.	On other hand Multi-point communication is less error prone as compared to Point-to-point communication.
6	Security and Privacy	Due to less number of parties involvement the Point-to-point communication is more secure and private as compared to Multi-point communication.	On other hand due to more number of parties involvement the Multi-point communication is less secure and private as compared to Point-to-point communication.

6. Differentiate b/w structured and unstructured data.

On the basis of	Structured data	Unstructured data
Technology	It is based on a relational database.	It is based on character and binary data.
Flexibility	Structured data is less flexible and schema-dependent.	There is an absence of schema, so it is more flexible.
Scalability	It is hard to scale database schema.	It is more scalable.
Robustness	It is very robust.	It is less robust.
Performance	Here, we can perform a structured query that allows complex joining, so the performance is higher.	While in unstructured data, textual queries are possible, the performance is lower than semi-structured and structured data.
Nature	Structured data is quantitative, i.e., it consists of hard numbers or things that can be counted.	It is qualitative, as it cannot be processed and analyzed using conventional tools.
Format	It has a predefined format.	It has a variety of formats, i.e., it comes in a variety of shapes and sizes.
Analysis	It is easy to search.	Searching for unstructured data is more difficult.

1. Define IoT, explain evolution/genesis of IOT.

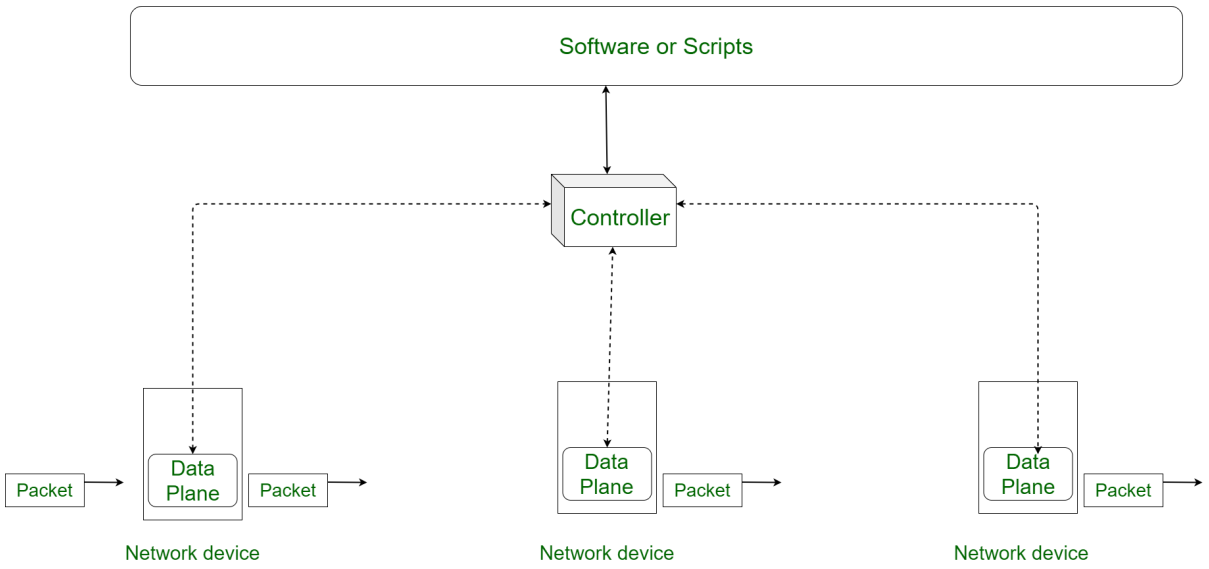
https://www.techaheadcorp.com/knowledge-center/evolution-of-iot/#:~:text=The%20evolution%20of%20IoT%20started,internet%20of%20things%20was%20paved.

2. Describe how SDN can be used for various levels of IOT

   Internet of Things (IoT) and Software Defined Network (SDN) are two emerging technologies. The IoT aims to connect objects over the Internet and the SDN provides orchestration for network management by decoupling the control plane and the data plane. The number of connected objects is in billions, and its management and control is a complex task for a large distributed network. The SDN provides flexibility and programmability in the IoT network without troubling underlying architecture of existing implementations. In this paper, we study different IoT application and domains, and the generalized IoT-SDN solutions over the period of 2012-2016. Furthermore, this paper provides a critical view of the IoT and the SDN technologies, current trends in research and the futuristic contributing factors. A comparative analysis of the existing solutions of SDN-based IoT implementations provides an easy and concise view of the emerging trends.
   https://www.researchgate.net/publication/319602888_Software_Defined_Network_SDN_Based_Internet_of_Things_IoT_A_Road_Ahead#:~:text=Internet%20of%20Things%20(IoT)%20and,plane%20and%20the%20data%20plane.

3. What is the function of central network controller of SDN

An SDN controller is the application that acts as a strategic control point in a software-defined network. Essentially, it is the “brains” of the network.



4. What are the common challenges associated with adoption of IOT in any new domain

   1.Scalability. Given the huge number of devices requiring simultaneous connectivity, scalability in IoT systems has become a concern. ...

   2.Security and Privacy. ...

   3.Self-Organization. ...

   4.Road and Transportation. ...

   5.Buildings. ...

   6.Healthcare. ...

   7.Supply Chain—Farm to Folks. ...

   8.Education and Training.

5. How is cloud based storage different from regular off site storage in IoT network

   The sole focus is to establish an ability to recover data should there be a loss of location. I see off-site backups as being purely storage-oriented. On the other hand, **cloud backups generally imply the addition of services to the basic "put your data somewhere else" model**.

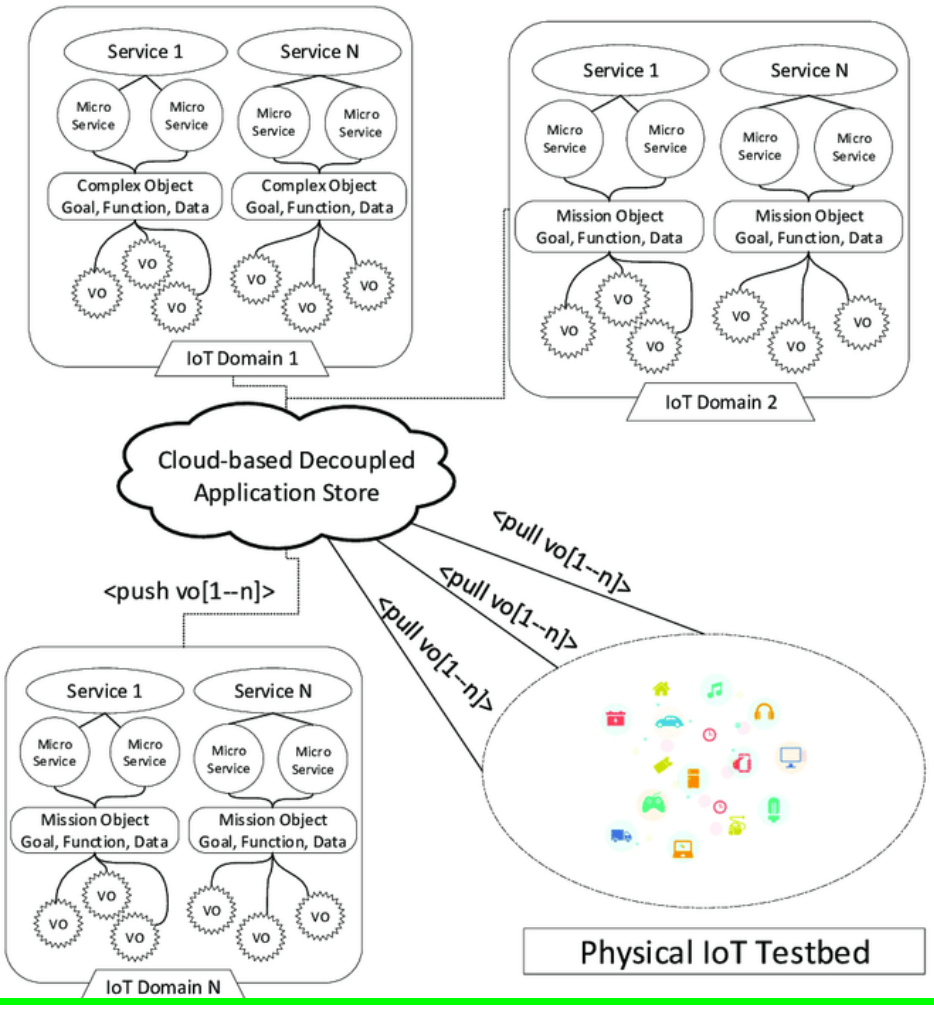
6. What is the role of fog and cloud computing in IoT? Elaborate on small physical and small virtual objects

When a device or application generates or collects huge amounts of information, data storage becomes increasingly complex and expensive.

When handling this data, network bandwidth also becomes expensive, requiring large data centers to store and share the information.

Fog computing has emerged as an alternative to the traditional method of handling data. Fog computing gathers and distributes resources and services of computing, storage, and network connectivity. It significantly reduces energy consumption, minimizes space and time complexity, and maximizes this data’s utility and performance.

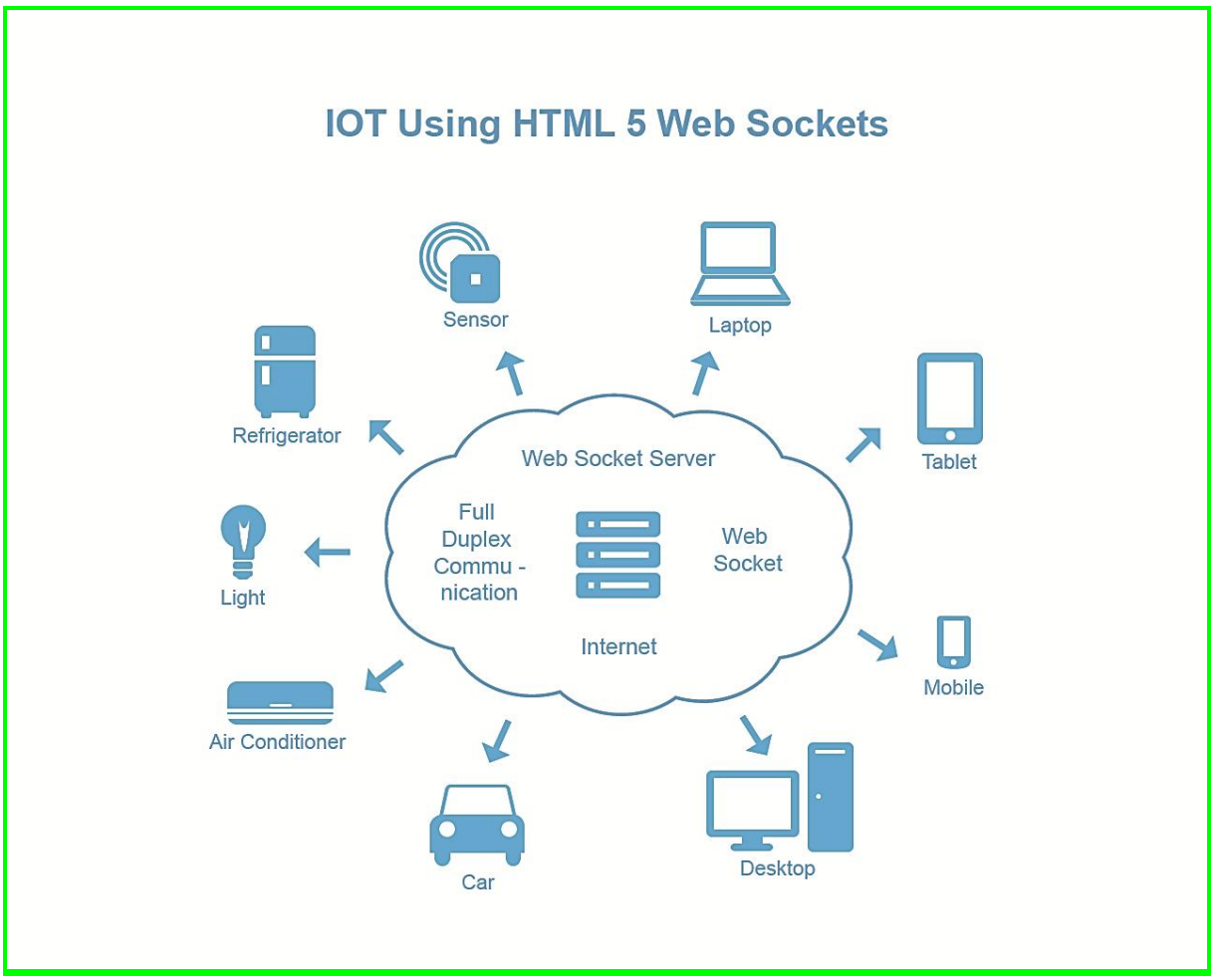
Virtual Object's Attributes	Physical Object Mapping	Relationship
Type	Sensors, Actuators, Hybrid	Type of virtual object limits it to be used in certain categories of devices for instance sensors.
Title	Name of Object	Title can help in correlating virtual object in similar things
Supported Protocol	Way of interacting physical objects	A sensor supporting only CoAP can't work with HTTP
Data Attributes	Size, duty cycle, resistance are data attributes	These enables the correct use of these attributes; For instance, a thing Person could have an attribute age
Methods	Potential tasks/operations a physical object perform	Sensing data, controlling fans, etc. can be mapped into methods in virtual domain
URI	Location	URI is where the object is located. With URI
Tags	Properties	Tags help in categorising virtual objects and efficiently searching relevant search
Metadata	Information like last access time	Metadata represents information about the physical object



7. What is virtualization and how does network function virtualization work for IoT communication

https://www.javatpoint.com/virtualization-in-cloud-computing

8. Describe an example of IoT service that uses web socket based communication



9. What are the protocol stacks using IEEE 802.15.4

https://www.geeksforgeeks.org/introduction-of-ieee-802-15-4-technology/

Layered Protocol Stack of IEEE 802.15.4:

The Physical layer defined by IEEE802.15.4 is responsible for activation and deactivation of the radio transceiver, link quality indication (LQI), channel selection, transmitting as well as receiving packets across the physical medium. Several channels in different frequency bands make it possible to relocate within the available spectrum.

The MAC layer.

The medium access control (MAC) enables the transmission of MAC frames through the use of the physical channel. Besides the data service, it offers a management interface and itself manages access to the physical channel and

network beaconing. It also controls frame validation, guarantees time slots and handles node associations. Finally, it offers hook points for secure services.
Higher layers: No higher-level layers and interoperability sublayers are defined in the standard. Other specifications - such as ZigBee, SNAP, and 6LoWPAN/Thread - build on this standard. RIOT, OpenWSN, TinyOS, Unison RTOS, DSPnano RTOS, nanoQplus, Contiki and Zephyr operating systems also use a few items of IEEE 802.15.4 hardware and software.

10. With an example explain SAAS differs from PAAS

https://www.geeksforgeeks.org/difference-between-iaas-paas-and-saas/

11. DIFFERENTIATE between low end and mid range IoT device

1) Low-End IoT Devices

Low-End IoT devices are devices that are constrained in terms of resources. The term constrained devices [5] was introduced to define a group of connected devices that are resource challenged. Low-end IoT devices are too constrained in terms of resources to run traditional OS such as Linux or Windows 10 IoT Core. Their Random Access Memory (RAM) and flash are of tens or hundreds of kilobytes and the processing unit is a 8-bit or 16-bit architecture with some state-of-the-art devices supporting 32-bit architecture. These devices are primary manufactured for basic sensing and actuating applications, and are programmed either by using low-level firmware or a very low functionality Wireless Sensor Networks (WSN) OS. An example of a low-end IoT device is the OpenMote-B and Atmel SAMR21 Xplained-Pro. These devices have been involved in various IoT applications [6], [7]. The Internet Engineering Task force (IETF) standardized the classification [5] of such devices into three subcategories.2 Table 1 shows the classes of low-end IoT devices.

2) Middle-End IoT Device

Middle-end IoT devices are devices with less constrained resources compared to a high-end IoT device described in Section I-.3, but providing more features with greater processing capabilities opposed to low-end IoT devices. There are some processing capabilities in the middle-end IoT device such as image recognition by running low-level computer vision algorithms. Furthermore, middle-end IoT devices can house more than one communication technologies unlike many of the low-end devices. The devices in this category usually have their clock speed and RAM in the range of hundreds of MHz and KB respectively compare to low-end devices that have their clock speed and RAM in tens of MHz and KB respectively. An example of the middle-end IoT devices are the Arduino Yun, Netduino devices etc. Interesting projects have been developed through middle-end IoT devices [8]–[9][10].

3) High-End IoT Device

High-end IoT devices are devices, mostly Single Board Computers (SBC) that have enough resources, such as a powerful processing unit, a lot of RAM and a possible high storage volume with a possible Graphical Processing Unit, to run a traditional OS such as Linux, Windows 10 IoT Core etc. In addition, these devices can perform tentative computations such as executing heavy Machine Learning algorithms. An example of such a device is the Raspberry Pi. These devices are well-known for their on-board connectivity including FastEthernet/GigaEthernet interfaces, Wi-Fi/BT chipset, HDMI out interface, more than one full USB 2.0 ports. Moreover, with the increasing usage of multimedia applications, majority of these devices come with camera interfaces such as Camera Serial Interface (CSI) and Display Serial Interface (DSI). Various interesting projects [11]–[12][13] demonstrate the usage of high-end IoT devices. These devices are often used as IoT gateways because of their high level of resources, making them to accommodate new services such as intelligent analytics at the edge of the network. We are only focusing on embedded systems and boards as smartphones are also regarded as high-end IoT devices.

12. What is the role of internet and things in IoT

Internet of Things (IoT) refers to a system of connected physical objects via the internet. The 'thing' in IoT can refer to a person or any device which is assigned through an IP address. A 'thing' collects and transfers data over the internet without any manual intervention with the help of embedded technology. It helps them to interact with the external environment or internal states to take the decisions.

13. What are the methods to ensure message integrity in IoT

https://www.practicalnetworking.net/series/cryptography/message-integrity/

14. Write 3 features of request response, publish subscribe, push pull

https://www.geeksforgeeks.org/communication-models-in-iot-internet-of-things/

15. List and explain key advantages of internet protocol

Advantages of TCP/IP
Its benefits are as follows:-

https://www.quora.com/What-are-the-advantages-of-Internet-Protocol-IP
https://www.tutorialspoint.com/Advantages-and-Disadvantages-of-the-TCP-IP-Model

- Provides scalability feature; this feature allows adding N number of networks without disturbing current services.
- It is interoperable, which means it allows two different systems to communicate over a heterogeneous network.
- It is open-source, i.e. free to use. Anyone can use it for communication.
- It is an industry-standard model which is developed to solve problems related to communication over a network.
- It assigns a unique IP address to each device across the network. So each device is identified uniquely over the network.

Disadvantages of TCP/IP
Its disadvantages are as follows:-

- It is a complicated model so it is a bit difficult to set up and manage.
- The transport layer does not guarantee the delivery of packets.
- It is not easy to replace protocols.
- It does not separate the concept of services, interfaces, and protocols, therefore it is not suitable to describe it in new technology.
- It was designed for a wide area network (WAN). It has not been optimized for LAN (local area network) and personal area network (PAN).

Final set 10 marks:

8. Determine the various communication models that can be used for weather monitoring system. What is more appropriate model for this system, describe the pros and cons. (3+4+3)

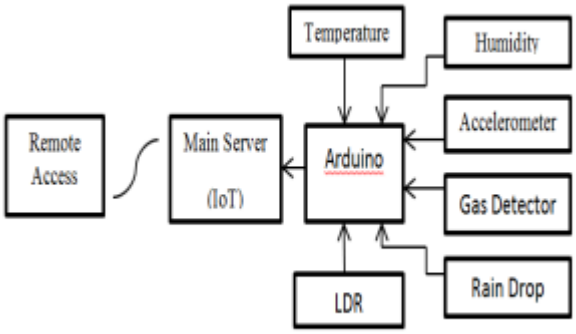
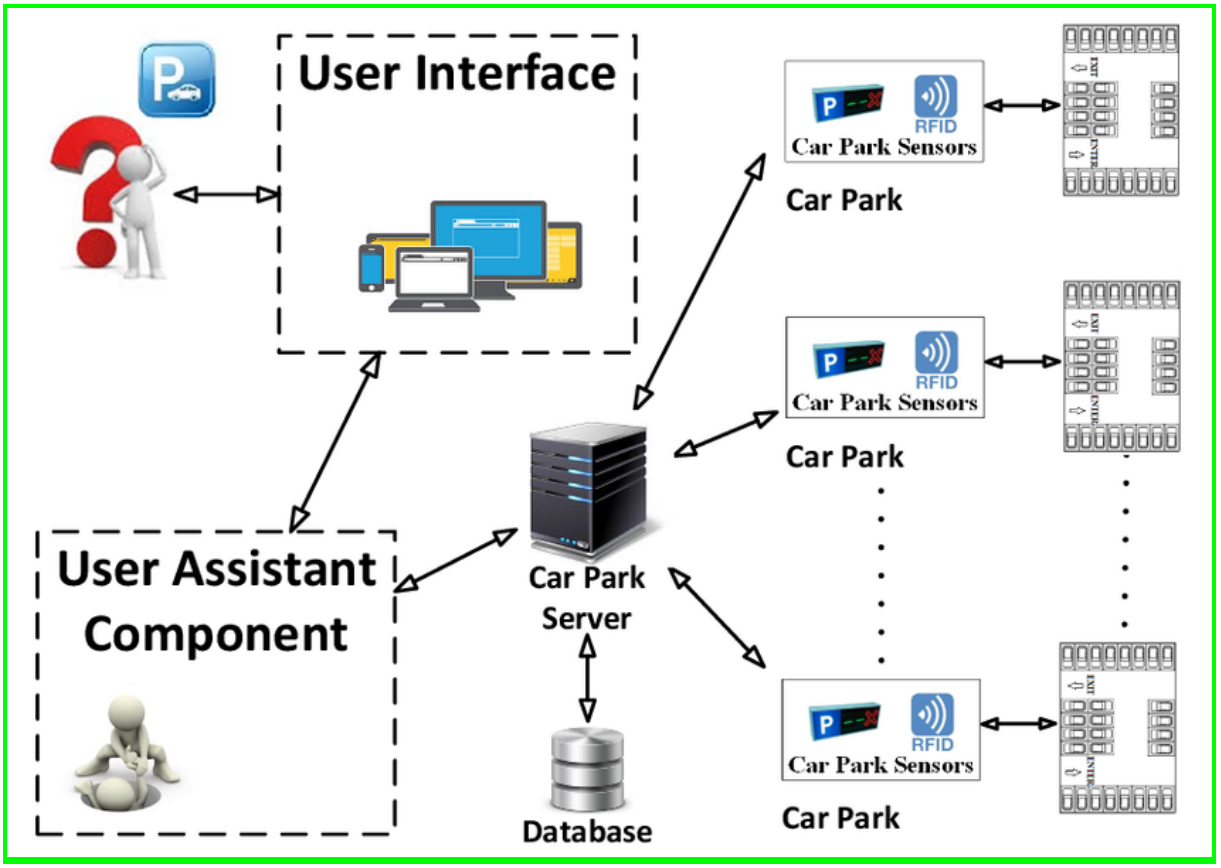
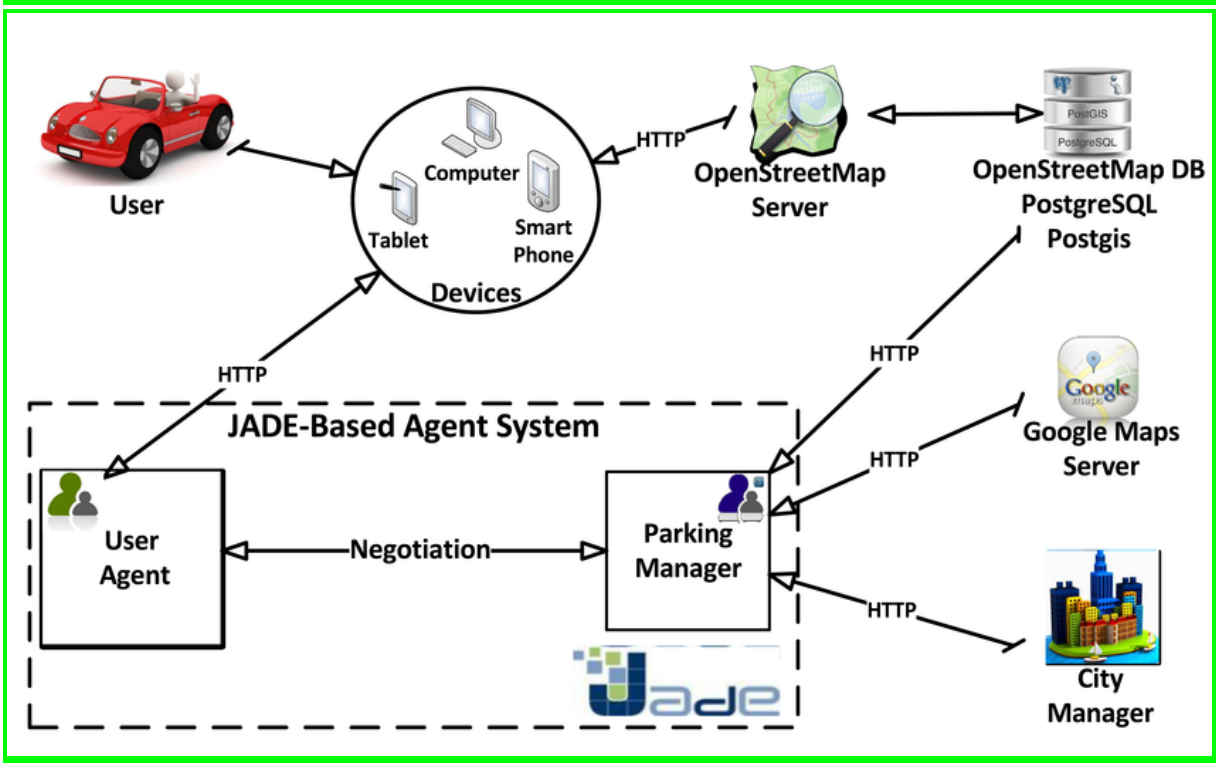
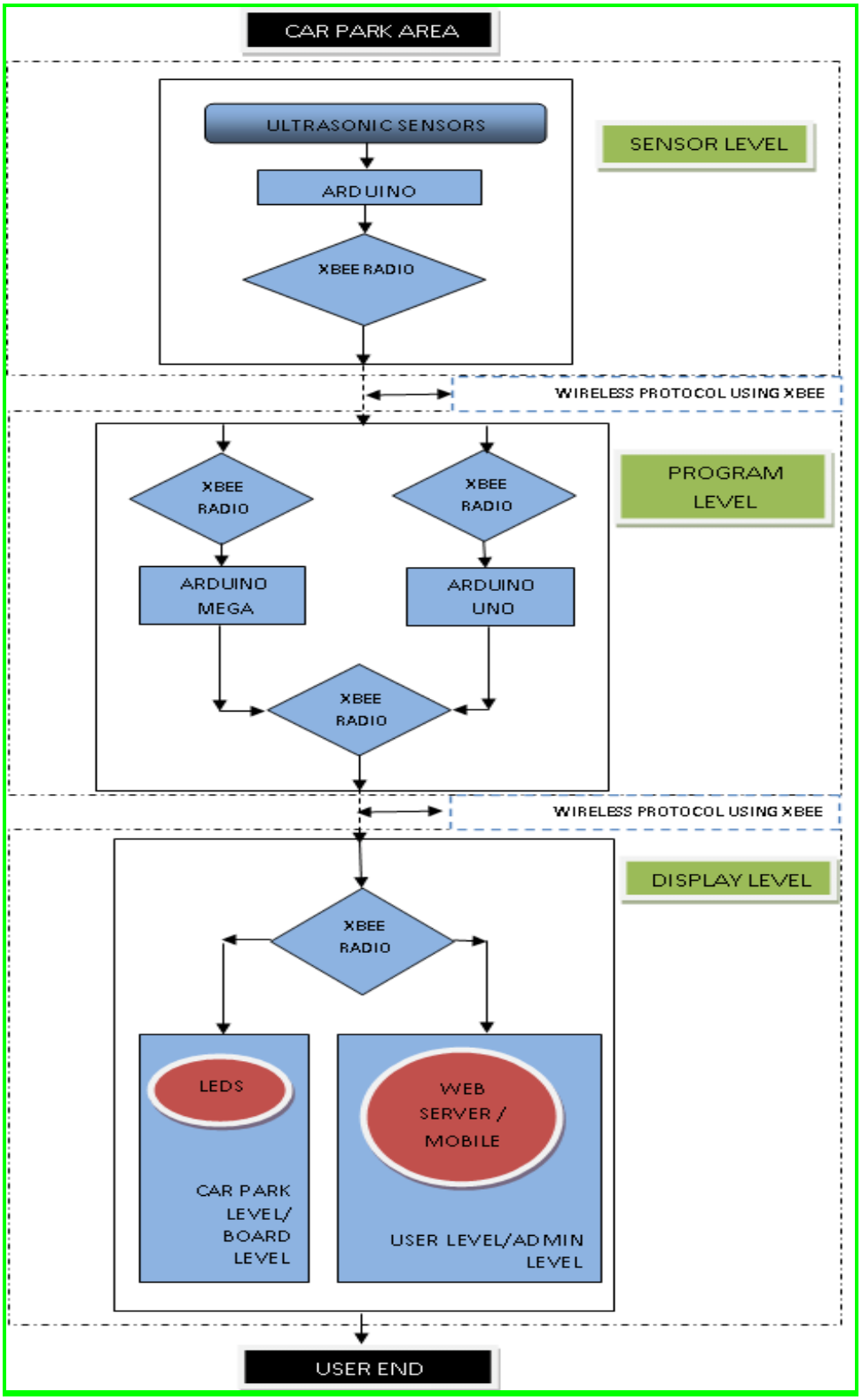


Figure1. Block Diagram of WMS

9. Why is network wide configuration important for IOT system with multiple nodes? Explain the service specification of a smart parking system (make a flowchart).


User Interface
Car Park Sensors
RFID
Car Park
Car Park Sensors
RFID
Car Park
User Assistant Component
Car Park Server
Database
Car Park Sensors
RFID
Car Park

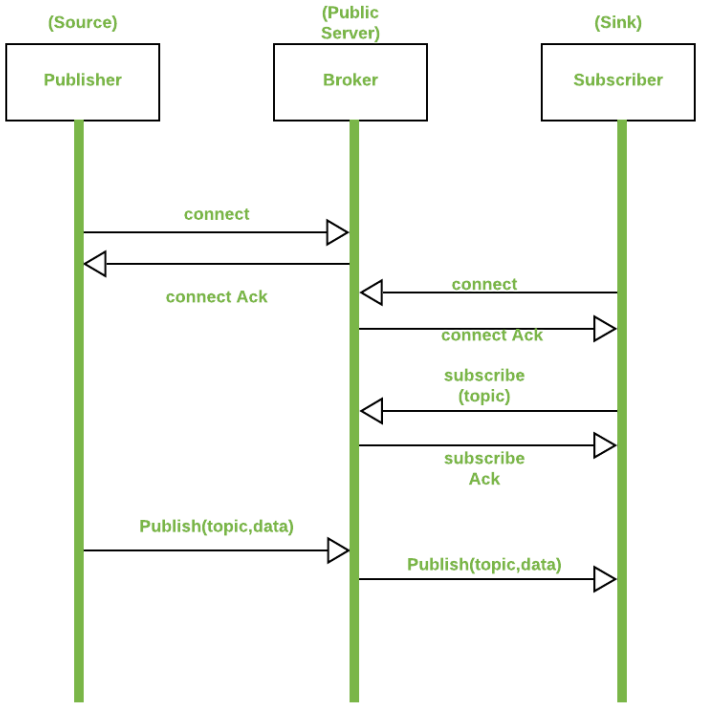

User
Computer
Tablet
Smart Phone
Devices
HTTP
OpenStreetMap Server
PostGIS
PostgreSQL
OpenStreetMap DB
PostgreSQL
Postgis
HTTP
HTTP
JADE-Based Agent System
Google
Google Maps Server
User Agent
Negotiation
Parking Manager
HTTP
Jade
City Manager



10. Explain the working principle of SNMP. Which limitation makes SNMP unsuitable for IOT networks?

https://www.javatpoint.com/simple-network-management-protocol

11. Explain MQTT and how is it a lightweight protocol? How is MQTT different from HTTP? (5+5) / How does MQTT work? What is an MQTT client? What does an MQTT broker do? What features separates MQTT-SN from MQTT? 20 marks



Broker Based MQTT Protocol

https://www.javatpoint.com/mqtt-protocol

The MQTT has some unique features which are hardly found in other protocols. Some of the features of an MQTT are given below:

- It is a machine to machine protocol, i.e., it provides communication between the devices.
- It is designed as a simple and lightweight messaging protocol that uses a publish/subscribe system to exchange the information between the client and the server.
- It does not require both the client and the server to establish a connection at the same time.
- It provides faster data transmission and a real-time messaging protocol.
- It allows the clients to subscribe to the narrow selection of topics so that they can receive the information they are looking for.

12. What is REST protocol? What are the architectural constraints of REST? What are the advantages of REST over regular web based service? (3+4+3)

REST stands for REpresentational State Transfer. REST is web standards based architecture and uses HTTP Protocol. It revolves around resource where every component is a resource and a resource is accessed by a common interface using HTTP standard methods. REST was first introduced by Roy Fielding in 2000.

In REST architecture, a REST Server simply provides access to resources and REST client accesses and modifies the resources. Here each resource is identified by URIs/ global IDs. REST uses various representation to represent a resource like text, JSON, XML. JSON is the most popular one.

HTTP methods
Following four HTTP methods are commonly used in REST based architecture.

- GET − Provides a read only access to a resource.
- POST − Used to create a new resource.
- DELETE − Used to remove a resource.
- PUT − Used to update a existing resource or create a new resource.

13. What is CoAP? Explain various messaging modes in CoAP. List the salient features of CoAP protocol.

CoAP and Features:
The constrained Application protocol (CoAP) is a web transfer protocol in constrained devices and low power, lossy networks. It follows request-response model to connect device across networks with high packet loss, high error rates and low bandwidth. CoAP implementations can act both as client and servers.

The various CoAP messaging modes are -

a. Confirmable (CCN): in the request-response paradigm, the requests are caried in confirmable type. (requires ack)

b. Non confirmable (NON): Both requests and responses are carried in this type. These message don't require acknowledgment from server.

c. Acknowledgement (ACK) - The acknowledgement mostly caries the response code included in the messages
Reset: It resets the connection b/w the 2 devices using COAP. it receiver of NON cannot process the message.

The salient features of CoAP are:

i. It is a web protocol for integrating. IOT with M2M services in a constrained environment.

ii. It enables UDP binding and provides reliability.

iii. Message transmission b/w end points is asynchronous.

iv. Limited packet header ensures low overhead thus less complexity.

14. List the characteristics of a fog node. What is the role of protocol abstraction layer?

- 1.Storage
- 2. computing
- 3.networking capability

In computer science, an abstraction layer is **a generalization of a conceptual model or algorithm, away from any specific implementation**. These generalizations arise from broad similarities that are best encapsulated by models that express similarities present in various specific implementations.
An abstraction layer **exposes an interface and hides the implementation details behind it**. The purpose of abstraction layers is to create abstractions. Methods and properties inside the layer should be the interface that's exposed, while the implementation inside those methods is everything in the detail layer.

15. Determine the IOT levels for designing the home automation IOT system including smart lighting and intrusion detection
https://www.geeksforgeeks.org/iot-home-automation/

By analyzing and sensing the human movements and environment, the light can be controlled by the smart lightening system. For example, a person enters a room, the light turns on automatically and it turns off when a person leaves the room. For this purpose, Solid State Lighting, IP enabled light are included.These can be controlled via mobile or web application. E.g. Philips Hue Lights Intrusion detection includes the sensors and cameras used to raise alerts and detect intrusions viaSMS, image, video, and email. This will improve security.

5. Write down a comprehensive short note of IOT impact in real world. Explain the steps that can process the algorithms involved in IOT and digitisation elaborating on this concept.How does SoAP enable communication between two syntactical different devices or machines.

Impact of IoT:
Smart Home has become the revolutionary ladder of success in the residential spaces and it is predicted Smart homes will become as common as smartphones.

The cost of owning a house is the biggest expense in a homeowner's life. Smart Home products are promised to save time, energy and money. With Smart home companies like Nest, Ecobee, Ring and August, to name a few, will become household brands and are planning to deliver a never seen before experience.

Wearable devices are installed with sensors and softwares which collect data and information about the users. This data is later pre-processed to extract essential insights about user.

These devices broadly cover fitness, health and entertainment requirements. The pre-requisite from internet of things technology for wearable applications is to be highly energy efficient or ultra-low power and small sized.

A connected car is a vehicle which is able to optimise it's own operation, maintenance as well as comfort of passengers using onboard sensors and internet connectivity.
Most large auto makers as well as some brave startups are working on connected car solutions. Major brands like Tesla, BMW, Apple, Google are working on bringing the next revolution in automobiles.

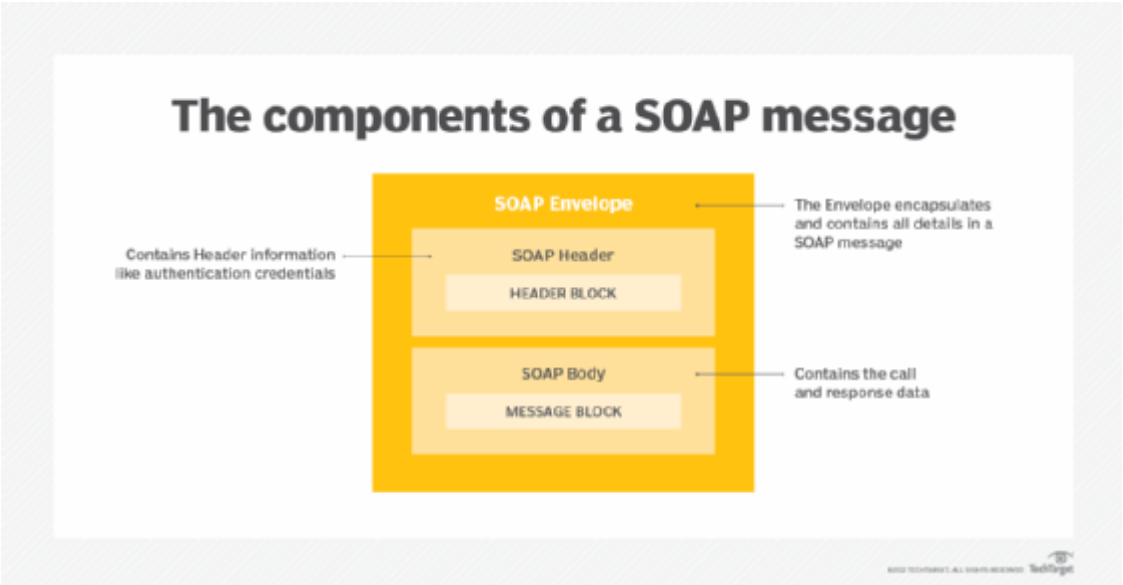
Industrial Internet is the new buzz in the industrial sector, also termed as Industrial Internet of Things (IIoT). It is empowering industrial engineering with sensors, software and big data analytics to create brilliant machines.
IIoT holds great potential for quality control and sustainability. Applications for tracking goods, real time information exchange about inventory among suppliers and retailers and automated delivery will increase the supply chain efficiency.

Smart city is another powerful application of IoT generating curiosity among world's population. Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security and environmental monitoring all are examples of internet of things applications for smart cities.
IoT will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies etc.

Smart farming is one of the fastest growing field in IoT.Farmers are using meaningful insights from the data to yield better return on investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertiliser are some simple uses of IoT.

https://www.cloudcredential.org/blog/the-ultimate-guide-to-implementing-iot/

https://www.techtarget.com/searchapparchitecture/definition/SOAP-Simple-Object-Access-Protocol



6. Differentiate between zigbee and 6lowpan. With diagram explain fog computing model with its defining characteristics.Elaborate the 2 type of model (service and deployment) associated with cloud computing methodology.

6LoWPAN

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), is a low power wireless mesh network where every node has its own IPv6 address. This allows the node to connect directly with the Internet using open standards.
6LoWPAN came to exist from the idea that the Internet Protocol could and should be applied even to the smallest devices, and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things.

S.NO	Bluetooth	Zigbee
1.	The frequency range supported in Bluetooth vary from 2.4 GHz to 2.483 GHz.	While the frequency range supported in Zigbee mostly 2.4 GHz worldwide.
2.	There are seventy nine RF channels in Bluetooth.	There are sixteen RF channels in zigbee.
3.	It uses GFSK modulation technique.	Whereas it also uses BPSK and QPSK modulation techniques like UWB.
4.	There is maximum of 8 cell nodes in Bluetooth.	While there is more than sixty five thousand (65000) cell nodes in zigbee.
5.	Bluetooth requires low bandwidth.	While zigbee also requires low bandwidth but greater than Bluetooth’s bandwidth most of time.
6.	The radio signal range of Bluetooth is ten meters.	While the radio signal range of zigbee is ten to hundred meters.

7.	Bluetooth was developed under IEEE 802.15.1.	Whereas it was developed under IEEE 802.15.4.

	ZigBee	Z-Wave	6LoWPAN
Operating Frequency	2.4 GHz, 915 MHz, 868 MHz	900 MHz	2.4 GHz
Max. Outdoor Range	~ 500 m	~ 100 m	~ 200 m
Max. Data Rate	250 Kbps	40 Kbps	200 Kbps
Max. Nodes	65,536	232	~ 100
Average Current Consumption	Tx: 25-35 mA; Rx: 20-30 mA;	Tx: 30-40 mA; Rx: 20-30 mA;	Tx: 20-35 mA; Rx: 12-25 mA;
Multi-hop Capabilities	Yes	Yes	Yes
Certification / Qualification Cost	Medium	Medium	Low
Development Community Adoption	High	High	Medium
Interoperability	High	High	Low
Reliability	Low	Low	Low
Suitable for Industrial / Military?	No	No	No

https://www.javatpoint.com/fog-computing-vs-cloud-computing

Cisco coined the term *fog computing* (***or fogging***) in 2014, so it is new to the general public. Fog and cloud computing are intertwined. In nature, Fog is closer to Earth than clouds; In the tech world, it's the same; Fog is closer to end-users, bringing cloud capabilities to the ground.

Fog is an extension of cloud computing that consists of multiple *edge nodes* directly connected to physical devices.

Such nodes tend to be much closer to devices than centralized data centers so that they can provide instant connections.

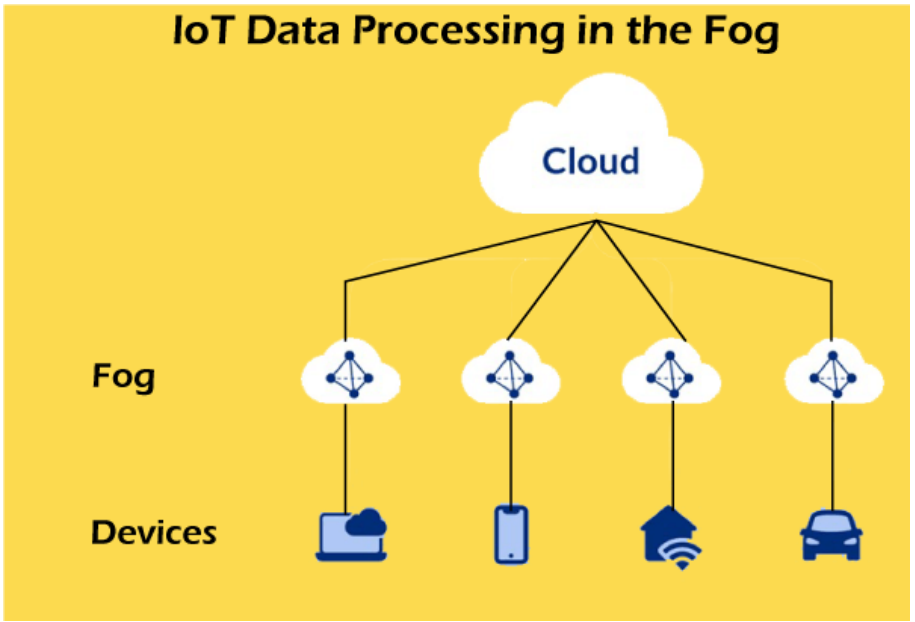
The considerable processing power of edge nodes allows them to compute large amounts of data without sending them to distant servers.

Fog can also include *cloudlets* - small-scale and rather powerful data centers located at the network's edge. They are intended to support resource-intensive IoT apps that require low latency.

The main difference between fog computing and cloud computing is that Cloud is a centralized system, whereas Fog is a distributed decentralized infrastructure.

Fog is an intermediary between computing hardware and a remote server. It controls what information should be sent to the server and can be processed locally. In this way, Fog is an intelligent gateway that dispels the clouds, enabling more efficient data storage, processing, and analysis.

It should be noted that fog networking is not a separate architecture. It does not replace cloud computing but complements it by getting as close as possible to the source of information.



Advantages of fog computing in IoT

The fogging approach has many benefits for the Internet of Things, Big Data, and real-time analytics. The main advantages of fog computing over cloud computing are as follows:

Low latency - Fog tends to be closer to users and can provide a quicker response.
There is no problem with bandwidth - pieces of information are aggregated at separate points rather than sent through a channel to a single hub.
Due to the many interconnected channels - loss of connection is impossible.

High Security - because the data is processed by multiple nodes in a complex distributed system.
Improved User Experience - Quick responses and no downtime make users satisfied.
Power-efficiency - Edge nodes run power-efficient protocols such as Bluetooth, Zigbee, or Z-Wave.

Disadvantages of fog computing in IoT

The technology has no obvious disadvantages, but some shortcomings can be named:

Fog is an additional layer in a more complex system - a data processing and storage system.
Additional expenses - companies must buy edge devices: routers, hubs, gateways.
Limited scalability - Fog is not scalable like a cloud.

Fog Computing is the term coined by Cisco that refers to extending cloud computing to an edge of the enterprise's network. Thus, it is also known as Edge Computing or Fogging. It facilitates the operation of computing, storage, and networking services between end devices and computing data centers.

Advantages of fog computing

- This approach reduces the amount of data that needs to be sent to the cloud.
- Since the distance to be travelled by the data is reduced, it results in saving network bandwidth.
- Reduces the response time of the system.
- It improves the overall security of the system as the data resides close to the host.
- It provides better privacy as industries can perform analysis on their data locally.

Deployment Models

The cloud deployment model identifies the specific type of cloud environment based on ownership, scale, and access, as well as the cloud's nature and purpose. The location of the servers you're utilizing and who controls them are defined by a cloud deployment model. It specifies how your cloud infrastructure will look, what you can change, and whether you will be given services or will have to create everything yourself. Relationships between the infrastructure and your users are also defined by cloud deployment types.

Different types of cloud computing deployment models are:

- Public cloud
- Private cloud

- Hybrid cloud
- Community cloud
- Multi-cloud

1. Public Cloud : The public cloud makes it possible for anybody to access systems and services. The public cloud may be less secure as it is open for everyone. The public cloud is one in which cloud infrastructure services are provided over the internet to the general people or major industry groups. The infrastructure in this cloud model is owned by the entity that delivers the cloud services, not by the consumer.

2. Private Cloud : The private cloud deployment model is the exact opposite of the public cloud deployment model. It's a one-on-one environment for a single user (customer). There is no need to share your hardware with anyone else. The distinction between private and public cloud is in how you handle all of the hardware.

3. Hybrid cloud : By bridging the public and private worlds with a layer of proprietary software, hybrid cloud computing gives the best of both worlds. With a hybrid solution, you may host the app in a safe environment while taking advantage of the public cloud's cost savings.

4. Community cloud: It allows systems and services to be accessible by a group of organizations. It is a distributed system that is created by integrating the services of different clouds to address the specific needs of a community, industry, or business.

Cloud Service Models

There are the following three types of cloud service models -

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

Software as a Service(SaaS)

Software-as-a-Service (SaaS) is a way of delivering services and applications over the Internet. Instead of installing and maintaining software, we simply access it via the Internet, freeing ourselves from the complex software and hardware management. It removes the need to install and run applications on our own computers or in the data centers eliminating the expenses of hardware as well as software maintenance.

Platform as a Service

PaaS is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser.

Infrastructure as a Service
Infrastructure as a service (IaaS) is a service model that delivers computer infrastructure on an outsourced basis to support various operations. Typically IaaS is a service where infrastructure is provided as outsourcing to enterprises such as networking equipment, devices, database, and web servers.

7. Explain process of detection of outliers on IoT using density based special clustering of applications . Write a python program to add two numbers in Raspberry Pi. Write a program to find the IP address of raspberry Pi (10 marks)

https://www.analyticsvidhya.com/blog/2020/09/how-dbscan-clustering-works/#:~:text=DBSCAN%20is%20a%20density%2Dbased,points%20into%20a%20single%20cluster.

It was proposed by Martin Ester et al. in 1996. DBSCAN is a density-based clustering algorithm that works on the assumption that clusters are dense regions in space separated by regions of lower density.

It groups ‘densely grouped’ data points into a single cluster. It can identify clusters in large spatial datasets by looking at the local density of the data points. The most exciting feature of DBSCAN clustering is that it is robust to outliers. It also does not require the number of clusters to be told beforehand, unlike K-Means, where we have to specify the number of centroids.

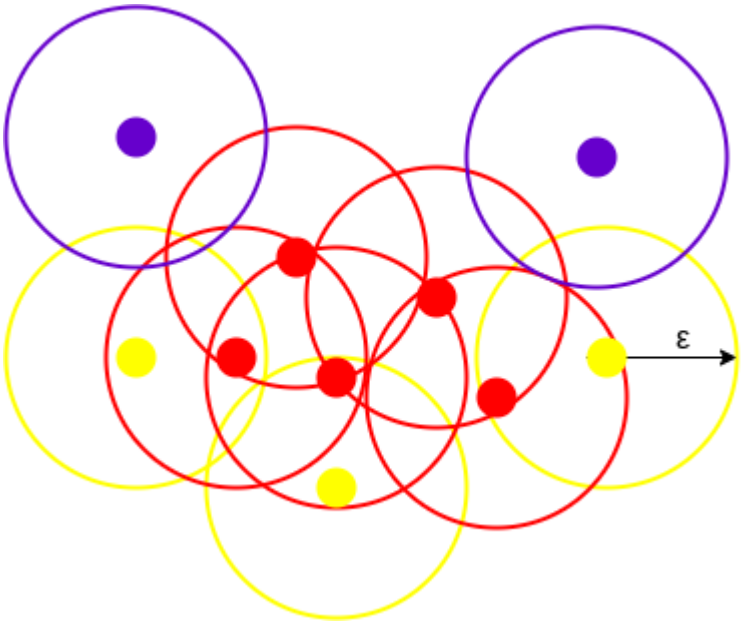
DBSCAN requires only two parameters: *epsilon* and *minPoints*. *Epsilon* is the radius of the circle to be created around each data point to check the density and *minPoints* is the minimum number of data points required inside that circle for that data point to be classified as a Core point.

In higher dimensions the circle becomes hypersphere, *epsilon* becomes the radius of that hypersphere, and *minPoints* is the minimum number of data points required inside that hypersphere.

Sounds confusing? Let's understand it with the help of an example.

Here, we have some data points represented by grey color. Let's see how DBSCAN clusters these data points.

DBSCAN creates a circle of *epsilon* radius around every data point and classifies them into Core point, Border point, and Noise. A data point is a Core point if the circle around it contains at least '*minPoints'* number of points. If the number of points is less than *minPoints*, then it is classified as Border Point, and if there are no other data points around any data point within *epsilon* radius, then it treated as Noise.



The above figure shows us a cluster created by DBCAN with *minPoints* = *3*. Here, we draw a circle of equal radius *epsilon* around every data point. These two parameters help in creating spatial clusters.

All the data points with at least 3 points in the circle including itself are considered as Core points represented by red color. All the data points with less than 3 but greater than 1 point in the circle including itself are considered as Border points. They are represented by yellow color. Finally, data points with no point other than itself present inside the circle are considered as Noise represented by the purple color.

For locating data points in space, DBSCAN uses Euclidean distance, although other methods can also be used (like great circle distance for geographical data). It also needs to scan through the entire dataset once, whereas in other algorithms we have to do it multiple times.

Reachability and Connectivity

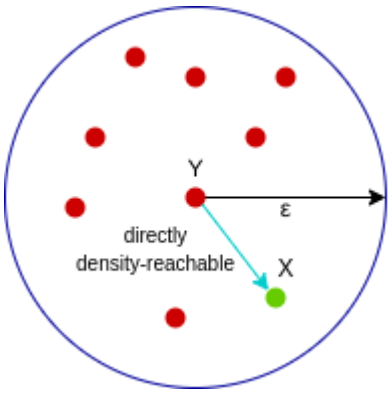
These are the two concepts that you need to understand before moving further. Reachability states if a data point can be accessed from another data point directly or indirectly, whereas Connectivity states whether two data points belong to the same cluster or not. In terms of reachability and connectivity, two points in DBSCAN can be referred to as:

- Directly Density-Reachable
- Density-Reachable
- Density-Connected

Let's understand what they are.

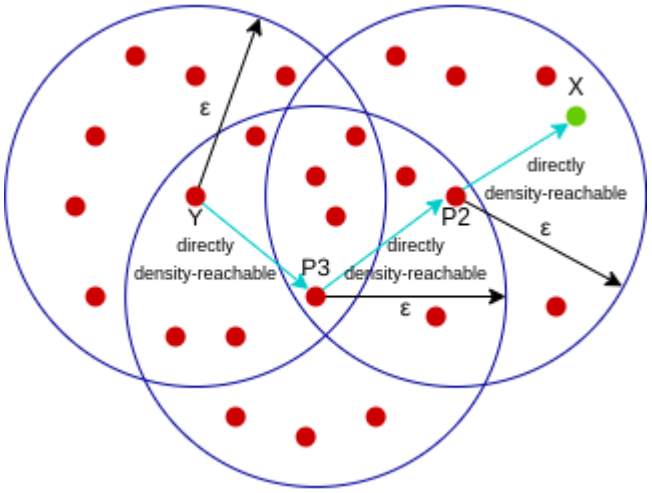
A point X is directly density-reachable from point Y w.r.t *epsilon, minPoints* if,

1. X belongs to the neighborhood of Y, i.e, *dist(X, Y)* <= *epsilon*
2. Y is a core point



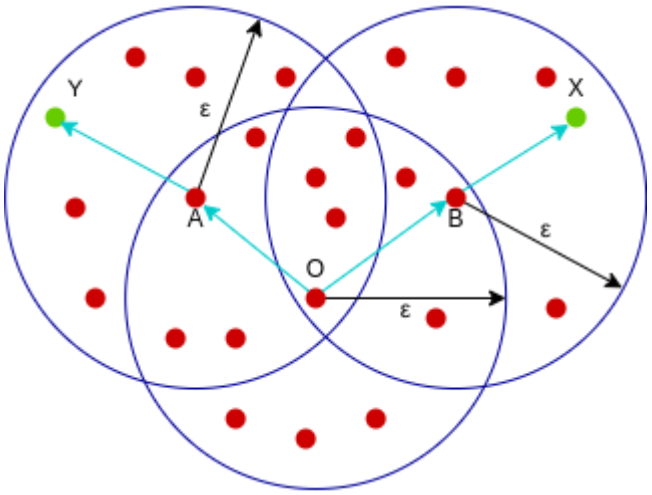
Here, X is directly density-reachable from Y, but vice versa is not valid.

A point X is density-reachable from point Y w.r.t *epsilon, minPoints* if there is a chain of points p1, p2, p3, …, pn and p1=X and pn=Y such that pi+1 is directly density-reachable from pi.



Here, X is density-reachable from Y with X being directly density-reachable from P2, P2 from P3, and P3 from Y. But, the inverse of this is not valid.

A point X is density-connected from point Y w.r.t *epsilon and minPoints* if there exists a point O such that both X and Y are density-reachable from O w.r.t to *epsilon and minPoints.*



Here, both X and Y are density-reachable from O, therefore, we can say that X is density-connected from Y.

Parameter Selection in DBSCAN Clustering

DBSCAN is very sensitive to the values of *epsilon* and *minPoints*. Therefore, it is very important to understand how to select the values of *epsilon* and *minPoints*. A slight variation in these values can significantly change the results produced by the DBSCAN algorithm.

The value of *minPoints* should be at least one greater than the number of dimensions of the dataset, i.e.,

$$minPoints >= Dimensions + 1.$$

It does not make sense to take *minPoints* as 1 because it will result in each point being a separate cluster. Therefore, it must be at least 3. Generally, it is twice the dimensions. But domain knowledge also decides its value.

The value of *epsilon* can be decided from the K-distance graph. The point of maximum curvature (elbow) in this graph tells us about the value of *epsilon*. If the value of *epsilon* chosen is too small then a higher number of clusters will be created, and more data points will be taken as noise. Whereas, if chosen too big then various small clusters will merge into a big cluster, and we will lose details.

https://pimylifeup.com/raspberry-pi-ip-address/

All you need to find out the IP address of your Raspberry Pi is to run the following command in the terminal.

hostname -I.

ping raspberrypi.

ping retropie.

sudo apt install nmap.

hostname -I.

sudo nmap -sn 192.168.1.0/24.