



SRI MUTHUKUMARAN INSTITUTE OF TECHNOLOGY

Chikkarayapuram, Near Mangadu, Chennai- 600 069.

Academic Year 2023 – 2024/ Odd Semester

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

(Regulation – 2021)

VI SEM/ III YEAR

UNIT I: IOT ARCHITECTURE AND PROTOCOLS

9

Internet – of – Things – Physical Design, Logical Design – IoT Enabling Technologies – Domain Specific IoTs – IoT and M2M – IoT System Management with NETCONF – YANG – IoT Platform Design – Methodology – IoT Reference Model – Domain Model – Communication Model – IoT Reference Architecture – IoT Protocols – MQTT, XMPP, Modbus, CANBUS and BACNet.

PART A

1. Define Internet of Things.

A dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual —things— have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into information n/w, often communicate data associated with users and their environments.

2. Mention the characteristics of IoT.

- **Dynamic & Self Adapting:** IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user's context or sensed environment.
Eg: the surveillance system is adapting itself based on context and changing conditions.
- **Self Configuring:** It allowing a large number of devices to work together to provide certain functionality.
- **Inter Operable Communication Protocols:** support a number of interoperable communication protocols and can communicate with other devices and also with infrastructure.
- **Unique Identity:** Each IoT device has a unique identity and a unique identifier (IP address).
- **Integrated into Information Network:** that allow them to communicate and exchange data with other devices and systems.

3. List out the key application functionalities of IoT systems.

The key application functionalities of IoT systems:

1. Information and analysis

- a. Tracking behavior
- b. Enhanced situational awareness
- c. Sensor-driven decision analytics

2. Automation and control

- Process optimization
- Optimized resource consumption
- Complex autonomous systems

4. List out the requirements of cloud computing in Iot system?

Minimizing latency: Milliseconds matter for many types of industrial systems, such as when you are trying to prevent manufacturing line shutdowns or restore electrical service. Analyzing data close to the device that collected the data can make a difference between averting disaster and a cascading system failure.

■ **Conserving network bandwidth:** Offshore oil rigs generate 500 GB of data weekly. Commercial jets generate 10 TB for every 30 minutes of flight. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud. Nor is it necessary because many critical analyses do not require cloud-scale processing and storage.

■ **Increasing local efficiency:** Collecting and securing data across a wide geographic area with different environmental conditions may not be useful. The environmental conditions in one area will trigger a local response independent from the conditions of another site hundreds of miles away. Analyzing both areas in the same cloud system may not be necessary for immediate efficiency.

5. Mention the data-related problems of fog computing

Bandwidth in last-mile IoT networks is very limited. When dealing with thousands/millions of devices, available bandwidth may be on order of tens of Kbps per device or even less.

■ Latency can be very high. Instead of dealing with latency in the milliseconds range, large IoT networks often introduce latency of hundreds to thousands of milliseconds.

■ Network backhaul from the gateway can be unreliable and often depends on 3G/LTE or even satellite links. Backhaul links can also be expensive if a per-byte data usage model is necessary.

■ The volume of data transmitted over the backhaul can be high, and much of the data may not really be that interesting (such as simple polling messages).

■ Big data is getting bigger. The concept of storing and analyzing all sensor data in the cloud is impractical.

The sheer volume of data generated makes real-time analysis and response to the data almost impossible.

6. Define fog computing.

The best-known embodiment of edge services in IoT is fog computing. Any device with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and IoT gateways. Analyzing IoT data close to where it is collected minimizes latency, offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the local network.

7. List out the characteristics of fog computing.

The defining characteristic of fog computing are as follows:

■ **Contextual location awareness and low latency:** The fog node sits as close to the IoT endpoint as possible to deliver distributed computing.

■ **Geographic distribution:** In sharp contrast to the more centralized cloud, these services and applications targeted by the fog nodes demand widely distributed deployments.

■ **Deployment near IoT endpoints:** Fog nodes are typically deployed in the presence of a large number of IoT endpoints. For example, typical metering deployments often see 3000 to 4000 nodes per gateway router, which also functions as the fog computing node.

8. What is edge computing?

Edge computing is also sometimes called “mist” computing. If clouds exist in the sky, and fog sits near the ground, then mist is what actually sits on the ground. Thus, the concept of mist is to extend fog to the furthest point possible, right into the IoT endpoint device itself.

9. Define sensor.

A sensor does exactly as its name indicates: It senses. More specifically, a sensor measures some physical quantity and converts that measurement reading into a digital representation. That digital representation is typically passed to another device for transformation into useful data that can be consumed by intelligent devices or humans.

10. List out the different categories of sensors.

Active or passive: Sensors can be categorized based on whether they produce an energy output and typically require an external power supply (active) or whether they simply receive energy and typically require no external power supply (passive).

■ **Invasive or non-invasive:** Sensors can be categorized based on whether a sensor is part of the environment it is measuring (invasive) or external to it (non-invasive).

- **Contact or no-contact:** Sensors can be categorized based on whether they require physical contact with what they are measuring (contact) or not (no-contact).
- **Absolute or relative:** Sensors can be categorized based on whether they measure on an absolute scale (absolute) or based on a difference with a fixed or variable reference value (relative).

11. Mention the different types of sensors.

1. Acoustic sensor- Acoustic sensors measure sound levels and convert that information into digital or analog data signals.

e.g. Microphone, geophone, hydrophone

2. Humidity sensor- Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and

so on. e.g. Hygrometer, humistor, soil moisture sensor

Light sensor- Light sensors detect the presence of light (visible or invisible).

e.g. Infrared sensor, photodetector, flame detector

Radiation sensor- Radiation sensors detect radiation in the environment. Radiation can be sensed by scintillating or ionization detection.

e.g. Geiger-Müller counter, scintillator, neutron detector

12. What is actuator?

Actuators are natural complements to sensors. Figure 3-4 demonstrates the symmetry and complementary nature of these two types of devices. As discussed in the previous section, sensors are designed to sense and measure practically any measurable variable in the physical world. They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human). Actuators, on the other hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.

13. How the actuators can be classified.

Type of motion: Actuators can be classified based on the type of motion they produce (for example, linear, rotary, one/two/three-axes).

- **Power:** Actuators can be classified based on their power output (for example, high power, low power, micro power)

- **Binary or continuous:** Actuators can be classified based on the number of stable-state outputs.

- **Area of application:** Actuators can be classified based on the specific industry or vertical where they are used.

- **Type of energy:** Actuators can be classified based on their energy type.

14. What is MEMS

Micro-electro-mechanical systems (MEMS), sometimes simply referred to as micro-machines, can integrate and combine electric and mechanical elements, such as sensors and actuators, on a very small (millimeter or less) scale. One of the keys to this technology is a microfabrication technique that is similar to what is used for microelectronic integrated circuits. This approach allows mass production at very low costs. The combination of tiny size, low cost, and the ability to mass produce makes MEMS an attractive option for a huge number of IoT applications.

15. Define smart objects.

Smart objects are, quite simply, the building blocks of IoT. They are what transform everyday objects into a network of intelligent objects that are able to learn from and interact with their environment in a meaningful way. It can't be stressed enough that the real power of smart objects in IoT comes from being networked together rather

than being isolated as standalone objects. This ability to communicate over a network has a multiplicative effect and allows for very sophisticated correlation and interaction between disparate smart objects.

16. Mention the characteristics of smart objects.

- Processing unit
- Sensors/actuators
- Communication device
- Power source

17. List out the trends in smart objects.

Size is decreasing: As discussed earlier, in reference to MEMS, there is a clear trend of ever-decreasing size.

Some smart objects are so small they are not even visible to the naked eye. This reduced size makes smart objects easier to embed in everyday objects.

■ **Power consumption is decreasing:** The different hardware components of a smart object continually consume less power. This is especially true for sensors, many of which are completely passive. Some battery-powered sensors last 10 or more years without battery replacement.

■ **Processing power is increasing:** Processors are continually getting more powerful and smaller. This is a key advancement for smart objects, as they become increasingly complex and connected.

■ **Communication capabilities are improving:** It's no big surprise that wireless speeds are continually increasing, but they are also increasing in range. IoT is driving the development of more and more specialized communication protocols covering a greater diversity of use cases and environments.

■ **Communication is being increasingly standardized:** There is a strong push in the industry to develop open standards for IoT communication protocols. In addition, there are more and more open source efforts to advance IoT.

18. List out the technologies used for connecting smart objects.

The following subsections cover technologies for connecting smart objects:

■ **IEEE 802.15.4:** This section highlights IEEE 802.15.4, an older but foundational wireless protocol for connecting smart objects.

■ **IEEE 802.15.4g and IEEE 802.15.4e:** This section discusses improvements to 802.15.4 that are targeted to utilities and smart cities deployments.

■ **IEEE 1901.2a:** This section discusses IEEE 1901.2a, which is a technology for connecting smart objects over power lines.

■ **IEEE 802.11ah:** This section discusses IEEE 802.11ah, a technology built on the well-known 802.11 Wi-Fi standards that is specifically for smart objects.

■ **LoRaWAN:** This section discusses LoRaWAN, a scalable technology designed for longer distances with low power requirements in the unlicensed spectrum.

■ **NB-IoT and Other LTE Variations:** This section discusses NB-IoT and other LTE variations, which are often the choice of mobile service providers looking to connect smart objects over longer distances in the licensed spectrum.

19. What is constrained network.

Constrained-node networks are often referred to as low-power and lossy networks (LLNs). *Low-power* in the context of LLNs refers to the fact that nodes must cope with the requirements from powered and battery-powered constrained nodes. *Lossy networks* indicates that network performance may suffer from interference and variability due to harsh radio environments. Layer 1 and Layer 2 protocols that can be used for constrained-node networks must be evaluated in the context of the following characteristics for use-case applicability: data rate and throughput, latency and determinism, and overhead and payload

20. List out the different forms of Cloud Computing.

1. Infrastructure-as-a-service (IaaS): provides users the ability to provision computing and storage resources. These resources are provided to the user as a virtual machine instances and virtual storage.

2. Platform-as-a-Service (PaaS): provides users the ability to develop and deploy application in cloud using the development tools, APIs, software libraries and services provided by the cloud service provider.

3. Software-as-a-Service (SaaS): provides the user a complete software application or the user interface to the application itself.

21. What is Wireless Sensor Network. Give example.

WSN Comprises of distributed devices with sensors which are used to monitor the environmental and physical conditions. Zig Bee is one of the most popular wireless technologies used by WSNs.

WSNs used in IoT systems are described as follows:

- Weather Monitoring System: in which nodes collect temp, humidity and other data, which is aggregated and analyzed.
- Indoor air quality monitoring systems: to collect data on the indoor air quality and concentration of various gases.
- Soil Moisture Monitoring Systems: to monitor soil moisture at various locations.
- Surveillance Systems: use WSNs for collecting surveillance data (motion data detection).

Smart Grids: use WSNs for monitoring grids at various points

22. Differentiate level 1 and level 2.

IoT Level 1: System has a single node that performs sensing and/or actuation, stores data, performs analysis and host the application as shown in fig. Suitable for modeling low cost and low complexity solutions where the data involved is not big and analysis requirement are not computationally intensive. An e.g., of IoT Level 1 is Home automation.

IoT Level 2: has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level 2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself. An e.g., of Level 2 IoT system for Smart Irrigation.

23. What is Embedded Systems?

It is a computer system that has computer hardware and software embedded to perform specific tasks. Embedded System range from low cost miniaturized devices such as digital watches to devices such as digital cameras, POS terminals, vending machines, appliances etc

24. Differentiate the class 0 and class 2 of constrained nodes.

Class 0

This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of Flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms.

An example of a Class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging

new unlicensed LPWA wireless technology.

Class 2

Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of Flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.

25. List out the parameter mainly used in connecting objects in IoT.

Range: This section examines the importance of signal propagation and distance.

■ **Frequency Bands:** This section describes licensed and unlicensed spectrum, including sub-GHz frequencies.

■ **Power Consumption:** This section discusses the considerations required for devices connected to a stable power source compared to those that are battery powered.

■ **Topology:** This section highlights the various layouts that may be supported for connecting multiple smart objects.

■ **Constrained Devices:** This section details the limitations of certain smart objects from a connectivity perspective.

■ **Constrained-Node Networks:** This section highlights the challenges that are often encountered with networks connecting smart objects.

26. Mention the home application of IoT device.

- a) **Smart Lighting:** helps in saving energy by adapting the lighting to the ambient conditions and switching on/off or dimming the light when needed.
- b) **Smart Appliances:** make the management easier and also provide status information to the users remotely.
- c) **Intrusion Detection:** use security cameras and sensors (PIR sensors and door sensors) to detect intrusion and raise alerts. Alerts can be in the form of SMS or email sent to the user.
- d) **Smoke/Gas Detectors:** Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of fire. Alerts raised by smoke detectors can be in the form of signals to a fire alarm system. Gas detectors can detect the presence of harmful gases such as CO, LPG etc.,

PART B

Internet-of-Things

The Internet of Things (IoT) is a network of connected devices that can communicate with each other, share data, and perform tasks without human intervention. The importance of communication in IoT cannot be overstated, as it is the foundation on which the entire system is built. The devices that make up the IoT ecosystem need to be able to communicate with each other in order to function properly and achieve their intended purpose.

Effective communication in IoT enables devices to share data, receive instructions, and respond to requests in a timely and accurate manner. This is critical for the successful implementation of IoT solutions across various industries, such as healthcare, manufacturing, transportation, and smart homes.

For example, in a smart home, the communication between the devices (such as lights, thermostats, and security systems) allows them to work together to create a more convenient and secure living environment for the occupants. Similarly, in a healthcare setting, IoT devices can be used to monitor patients remotely and alert healthcare providers in case of an emergency, ensuring that timely medical intervention is provided.

Physical Design, Logical Design

While talking about the **logical and physical design of IoT** we are talking about the physical devices and the protocols that take data from one device to another. All of them work together as a single unit. Each of the physical devices is called a node and each device has its own unique identity with the help of protocol they do things like monitoring, sensing and tracking. IoT today are becoming immensely popular. Companies today are implementing IoT technologies more so if you want to be relevant to the tech industry you have to know one or two things about IoT. Sadly very few do this.

Physical Design Of

IoT Physical Devices/Things

Devices are physical electronic components that are used to build a connection to process data, provide interfaces that offer storage, graphics and also power source sometimes in the IoT system. Most of these physical components collect data from the environment and send raw data to be processed and analyzed. After analyzing it sends the information to the actuator to act accordingly. Instead of collecting data from the environment some IoT also collects user data to provide more refined performance to the users.

For example, a small propeller sensor inside the tap of a wine barrel spins whenever the wine is poured from the tap. After that, the data of the number of times it spun gets sent to the analyzer and tells how much wine is spent and when to shut off the flow. The analyzing part gets done by the algorithm that were put into it. Here are some examples of physical components.

The Connectivity

Whatever physical device provides connectivity and either transmits or receives data come in the connectivity part or physical devices of IoT. Here it can be USB ports, Ethernet cable etc.

Processor

The second, essential component of the physical design of IoT will be the CPU or the processor. All the data processing happens here and it improves the decision making quality in the IoT system.

Sound & Visual

The third element is the visual component of IoT. It shows all the information that the processor sends to the screen. It uses things like HDMI and RCA. The video player is the audio and visual part of the physical design of IoT.

Storage Component

Not only a hard disc every component that stores data is the storage component of IoT. Things like SD, MMC and SDIO. It's different from the DDR and GPU is used to control the activity of an IoT system.

Logical Design of IoT

The -Logical Design of IoT is the framework or the imaginary ideal design in which the components including software and the hardware components will be laid out. It doesn't go into the depth of describing how each component will be built with low-level programming specifics.

IoT Functional

Blocks What is a functional block?

An IoT system consists of a number of functional blocks that provide the system with the capabilities for identification, sensing, actuation, communication and management. The function of the Communication functional block in short **Handle the communication for the IoT system.**

Any IoT system will have several functional blocks like Devices, communication, security, services, and application. With the help of the functional blocks, we provide sensing, identification, actuation, management, and communication capability. These blocks also include the physical components too.

IoT communication models

There are endless options of models available in an IoT system. It connects the IoT system to the server. Here are some examples

Request-response
model Push-pull model

Publish-subscribe
model Exclusive pair model

IoT Communication API

In simpler terms APIs are used to communicate between the server and the system in IoT. Some API includes.

REST-
based communication APIs Client-
server

Stateless
Cacheable

Websocket based communication API

The IoT Protocols

In simpler terms, IoT protocols are a number of procedures or sets of rules that decide how data will be transmitted between two devices generally those two computers there are many protocols each of them works differently than others on how any data will be structured and how it will be sent between devices and it will be received. There are basically 11 types of protocols for IoT. We have an article dedicated completely to the [IoT protocols](#). Do have a read if you want to know about the IoT protocols in detail, go check it out. There are 4 types of

- Bluetooth
- 6LoWPAN
- Zigbee
- Z-Wave
- WiFi
- Cellular
- Thread

- NFC
- Neul
- LoRaWAN

IoT(internetofthings)enablingtechnologies

WirelessSensorNetwork

CloudComputing

BigDataAnalyticsCommun

ications

ProtocolsEmbeddedSyste

m

1. WirelessSensorNetwork(WSN):

A WSN comprises distributed devices with sensors which are used to monitor the environmental and physical conditions. A wireless sensor network consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects WSN to the internet.

Example—

Weather monitoring system

Indoor air quality monitoring system

oil moisture monitoring system

Surveillance system

Health monitoring system

2. Cloud Computing:

It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations.

With cloud computing, users can access any resources from anywhere like databases, web servers, storage, any device, and any software over the internet.

Characteristics –

Broad network access

On demand self-services

Rapid

scalability

Measured service

Pay-per-use

Provides different services, such as—

IaaS (Infrastructure as a service)

Infrastructure as a service provides online services such as physical machines, virtual machines, servers, networking, storage and data center space on a pay per use basis. Major IaaS providers are Google Compute Engine, Amazon Web Services and Microsoft Azure etc.

Ex : Web Hosting, Virtual Machine

etc. PaaS (Platform as a service)

Provides a cloud-based environment with a very thing required to support the complete life cycle of building and delivering web-based (cloud) applications – without the cost and complexity of buying and managing underlying hardware, software provisioning and hosting. Computing platforms such as hardware, operating systems and libraries etc. Basically, it provides a platform to develop applications.

Ex: AppCloud, Google App Engine SaaS

SaaS (Software as a service)

It is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management.

SaaS Applications are sometimes called web-based software on demand software or hosted software.

SaaS Applications run on a SaaS provider's service and they manage security, availability and performance.

Ex: Google Docs, Gmail, office etc.

3. Big Data Analytics:

It refers to the method of studying massive volumes of data or big data. Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases.

Big data is gathered from a variety of sources including social network videos, digital images, sensors and sales transaction records.

Several steps involved in analyzing big data –

Data cleaning

Munging

Processing

Visualization

Examples –

Bank transactions

Data generated by IoT systems for location and tracking of vehicles

E-commerce and in Big-Basket

Health and fitness data generated by IoT systems such as fitness bands

4. Communications Protocols:

They are the backbone of IoT systems and enable network connectivity and link into applications. Communication protocols allow devices to exchange data over the network. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.

They are used in

Data

encoding Address in

gschemes

5. Embedded Systems:

It is a combination of hardware and software used to perform special tasks.

It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input/output units (display keyboard etc.) and storage devices (flash memory).

It collects the data and sends it to the internet. Emb

ded systems used in

Examples –

Digital camera

DVD player, music

player Industrial robots

Wireless Routers etc.

Types of Communication Models in IoT

There are several communication models that can be used in the Internet of Things (IoT) ecosystem, depending on the requirements of these cases. The three main communication models used in IoT are –

Depending upon its usage, the software may be classified as generic or specific. Generic software is a software that can perform multiple tasks in a different environment without being modified like a word processor software that can be used by anyone to make different types of documents as a report, whitepaper, training material, etc. Specific software is software for a particular application, like a railway reservations system, weather forecasting, etc.

Some Domain Specific Tools:

School Management System: School management system handles various activities and processes of a school to facilitate campus management like examination, attendance, admission, student's fees, timetable, teacher's training, etc. It provides a healthy interaction among teachers, students, parents.

Inventory Management : Managing multiple tasks like purchase, sales, order, delivery, stock maintenance, etc. associated with raw or processed goods in any business is called inventory management. The inventory management software ensures that stocks are never below specified limits and purchase/deliveries are done in time. Inventory management system is very useful for forecasting, utilizing economies of scale and timing.

Payroll Management System : Payroll management system deals with the financial aspects of the employee's salary, taking care of leaves, bonus, loans, etc. Some advantages of using this kind of management system are managed employee information efficiently, generate pay-slip at the

convenience of a mouse click, manages its own security. Payroll software is generally a component of HR (Human Resource) management software in big organizations.

Employee Definition

|

Salary Structure

|

Pay Element

|

Tax Details Recording

|

Leave and Time Sheet Booking

|

Employee Appraisal

|

Employee Payroll Generation

|

Salary

Payment Block diagram for Salary Payment Process

Process

Financial Accounting : Financial management software keeps an electronic record of all financial transactions of the organization. Objectives of financial accounting

Record financial transactions as and when they occur so that the data can be analyzed for preparing a financial statement.

Calculate profit or loss, to enable management to take course-correction strategies if required. Ascertain the financial strength of the company by determining its assets and liabilities.

Communicate the information to stakeholders through statements and reports, so that these stakeholders can take appropriate decisions on their investments in the business.

Hotel Management : Hotel management software helps hotel managers to keep track of inventory levels, daily orders, customer management, employee scheduling, table booking, etc.

Reservation System : A reservation system is a software that handles multiple modules like train routes, train management, seat booking, meal booking, train maintenance, train status, travel package, etc.

Weather Forecasting System : Weatherforecasting system is a real-time software that predicts the weather of a place by collecting live data about atmospheric temperature, humidity, wind level, etc. It is used to predict major disasters like earthquakes, hurricanes, tsunamis, etc.

IoT applications span a wide range of domains like:

Home

Automation Smart

Cities Environment

Energy

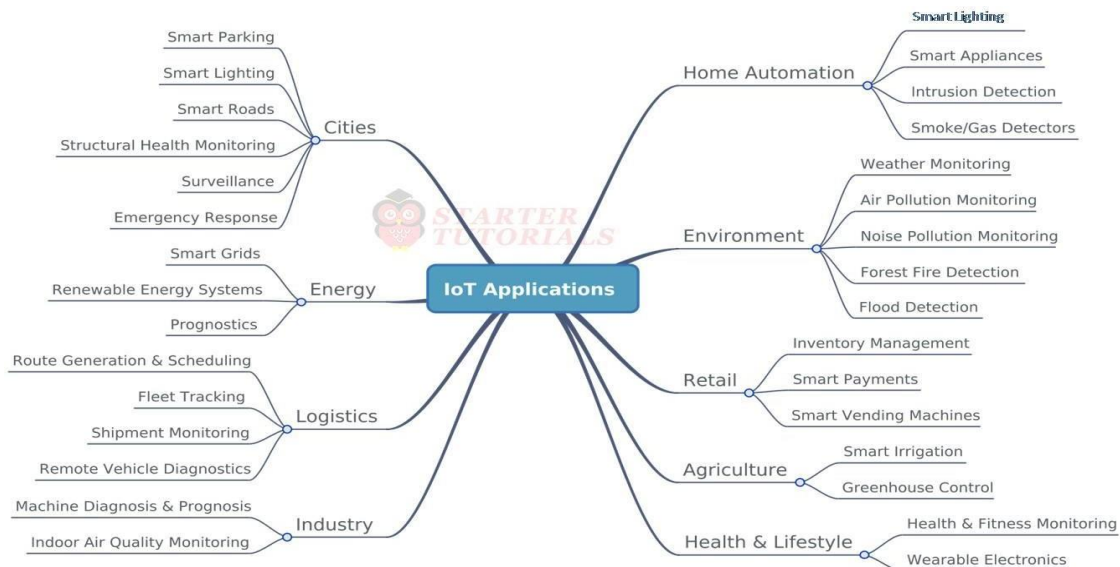
systems Retail

Logistics In

dustry Agri

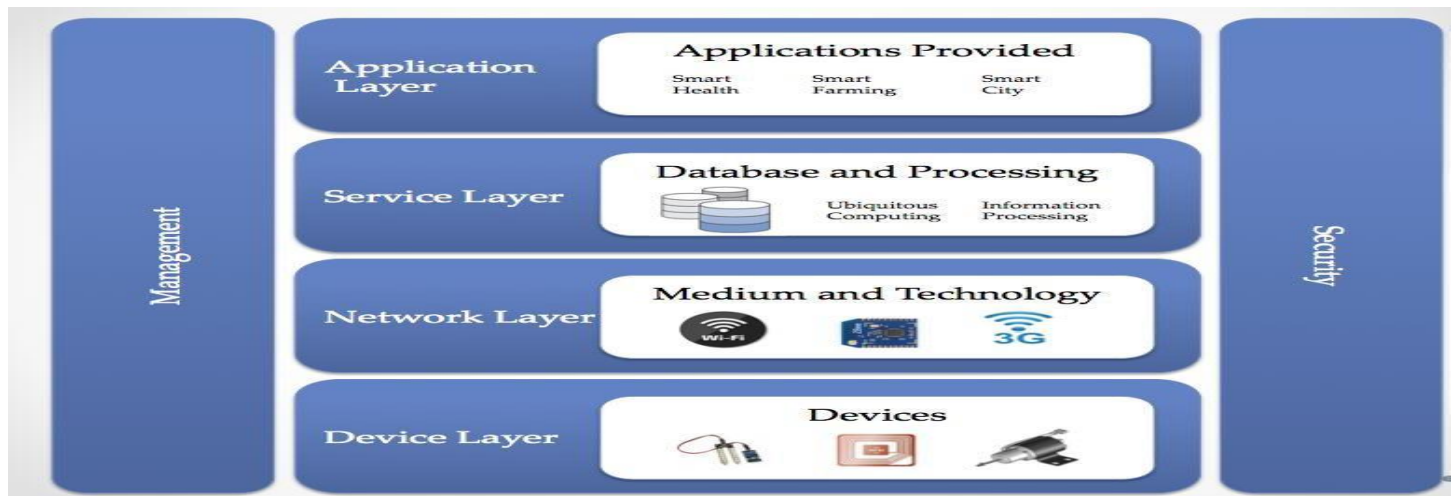
culture Heal

th



IoT Reference Model

Just like the OSI reference model for the internet, IoT architecture is defined through six layers: four horizontal layers and two vertical layers. The two vertical layers are **Management** and **Security** and they're spread over all four horizontal layers, as seen in the following diagram:



IoT Layers

The **Device Layer**: At the bottom of the stack, we have the device layer, also called the **perception layer**. This layer contains the physical things needed to sense or control the physical world and acquire data (that is, by perceiving the physical world). Existing hardware, such as sensors, RFID, and actuators, constitute the perception...

What is IoT Reference Architecture?

IoT (Internet of Things) reference architecture is a framework that provides a common understanding of the key components and their interactions in an IoT system. It serves as a blueprint for designing and implementing IoT systems and helps ensure interoperability, scalability, and security.

The IoT Reference architecture typically consists of the following layers:

Perception layer: This layer consists of sensors, actuators, and other devices that collect and generate data from the physical environment. These devices are responsible for sensing and measuring various physical parameters, such as temperature, humidity, pressure, and motion.

Network layer: This layer consists of various networking technologies, such as Wi-Fi, Bluetooth, and cellular networks, that enable devices to communicate with each other and with cloud-based servers. This layer also includes various networking protocols, such as MQTT and CoAP, that are optimized for machine-to-machine communication.

Middleware layer: This layer provides various services and functions that enable data processing, storage, and analysis. It includes various platforms, such as cloud-based platforms and edge computing platforms, that provide data processing, analytics, and storage services.

Application layer: This layer consists of various applications and services that use the data generated by IoT devices to provide value to end-users. These applications and services can be used in a wide range of domains, such as smart homes, industrial automation, healthcare, transportation, and energy management.

Security layer: This layer provides various security mechanisms, such as authentication, authorization, and encryption, to ensure the confidentiality, integrity, and availability of data in an IoT system. It also includes various security protocols,

such as TLS and DTLS, that are used to secure data transmission between devices and cloud-based servers.

IoT Protocols

The Internet of Things (IoT) is about the network of sensor devices to the web in real-time. IoT devices communicate with each other over the network, so certain standards and rules need to be set to determine how data is exchanged. These rules are called IoT Network Protocols. Today, a wide variety of IoT devices are available, and therefore different protocols have been designed.

Depending on the IoT application's functionality, its workflow or architecture varies. Basic architecture involves four layers, i.e., the Sensing layer, Network layer, Data processing layer, and Application layer.

The Sensing layer contains all the hardware, like sensors, actuators, chips, etc., that collect information. This layer is connected to the successive layer, which is the network layer, through protocols. The Network layer allows communications among devices using network protocols like cellular, Wi-Fi, Bluetooth, Zigbee, etc. The data collected by IoT devices is processed in the Data processing layer using technologies like data analytics and machine learning algorithms. This processed data can be displayed to the user through web portals, apps, or interfaces provided by the application layer. Users can directly interact and visualize the data obtained from IoT devices through these interfaces.

As IoT devices have very few components—little batteries and sensors, there is a small amount of power available. Hence, it is tough to design protocols for IoT. Also, we need to perform everything (construct topological structures, do address assignments, etc.) on wireless.

IoT Protocols Should Also Satisfy These Requirements

- Allow communication among various devices simultaneously.
- IoT is being used in critical areas like health, industries, home surveillance, etc. hence communication security needs to be ensured.
- Transport data efficiently.
- IoT devices can be added or removed from the IoT network. Hence protocols must provide scalability.

There are many such protocols developed for IoT, then how to choose one??

One way to decide which protocol to use is to consider the environment for which these protocols are designed. Some are designed for small ranges; some are for wide ranges, high data rates, low data rates, etc. They vary based on power consumption, range, cost, data rate, etc.

Short Range Communication, Low

Data Rate, Low Power Bluetooth

Bluetooth works in a frequency range of 2.4 GHz. It covers a range of 10 m to 100 m, and its data rate goes up to 1 MBPS. It supports two network topologies—point-to-point and mesh. It is suitable to send a small amount of data to personal devices like speakers, earphones, smart

watches, smart shoes, etc. This protocol can also be used for Smart Homes, including Alarms, HVAC, lighting, etc.

Zigbee

This is based on the IEEE 802.15.4 standard. Its frequency range is the same as that of Bluetooth, which is 2.4 GHz. Its range is up to 100 meters, and the data rate is a maximum of 250 KBPS. Zigbee protocol can transmit small amounts of data within a short range. This can be used in systems that require high authentication and robustness. It supports star topology, mesh topology, and cluster tree topology. Major applications observed are sensing device health in industries, smart homes, etc.,

6LoWPAN

PAN stands for Personal Area Network, and 6LoWPAN refers to IPv6 Low Power PAN. It works in a frequency ranging from 900 to 2400 MHz. The data rate is 250 KBPS, supporting two network topologies - star and mesh.

Short Range Communication, High Data Rate

Wireless LAN - Wi-Fi

Wi-Fi has high bandwidth and allows a data rate of 54 MBPS and goes up to 600 MBPS. Covers a range of 50m in the local area where providing private antennas goes to 30 km. IoT devices can be easily connected using Wi-Fi and share a large amount of data. This protocol is used in smart homes, smart cities, offices, etc

Long Range Communication, High Data Rate, Low

Power LoRaWAN

This stands for Long Range Wide Area Network. Its range is approximately 2.5 km and can go up to 15 km. The data rate is very low, which is 0.3 KBPS and goes up to a maximum of 50 KBPS. It can support many connected devices and is used in applications like Smart City, Supply Chain Management, etc.

LTE-M

LTE-M stands for Long Term Evolution for Machines. This is a type of LPWAN - Low Power Wide Area Network. This is used along with cellular networks to provide security. LTE-M works in a frequency range of 1.4 MHz - 5 MHz, and the data rate can go up to 4 MBPS.

Long Range, Low Data Rate, Low Power

Consumption Sigfox

Sigfox is used when wide area coverage is required with minimum power consumption. It aims at connecting billions of IoT devices. This protocol's frequency range is 900 MHz, covering a range of 3 km to 50 km. The maximum data rate is very low, which is 1 KBPS.

Long Range, Low Data Rate, High Power

Consumption Cellular

This is also known as a mobile network. Cellular networks are 2G, 3G, 4G, and 5G. It has frequency ranges – 900MHz, 1.8/1.9/2.1 GHz. The range is approximately 35km and goes up to 200km. The average data rate is 35KBPS – 170KBPS. Cellular networks consume high power. This protocol is not used for most IoT devices due to frequency and security issues. It can be used with IoT applications like connected cars.

IOT Communication models:

Client-Server Model

In the Client-Server communication model, the client sends encoded requests to the server for information as needed. This model is stateless, meaning that each request is handled independently and data is not retained between requests. The server categorizes the request, retrieves the data from the database or resource representation, and converts it to an encoded response that is sent back to the client. The client then receives the response.

On the other hand, in the Request-Response communication model, the client sends a request to the server and the server responds to the request by deciding how to retrieve the data or resources needed to prepare the response. Once prepared, the server sends the response back to the client.

Publish-Subscribe Model

The Publish-Subscribe communication model consists of three entities: Publishers, Brokers, and Consumers.

Publishers are responsible for generating and sending data to specific topics managed by the broker. Publishers are not aware of the consumers subscribed to the topic.

Consumers subscribe to the topics managed by the broker to receive data from the publishers. The broker is responsible for sending the data to the appropriate consumers based on their subscription to specific topics.

The broker is responsible for accepting data from the publishers and forwarding it to the appropriate consumers subscribed to that specific topic. The broker is the only entity that has information regarding the consumer to which a particular topic belongs, and publishers are not aware of this information.

Push-Pull Model

The Push-Pull communication model consists of three entities: data publishers, data consumers, and data queues. Publishers and consumers are not aware of each other. Publishers push messages or data into the queue, and consumers on the other end pull data out of the queue. The queue acts as a buffer for messages when there is a difference in the rate of data push or pull by the publisher and consumer.

Queues play an essential role in decoupling messaging between the producer and consumer, and they act as a buffer in situations where there is a mismatch in the rate at which data is pushed by

producers and pulled by consumers. This buffer helps ensure smooth communication between the two entities.

Exclusive Pair Model

Exclusive Pairs are communication models that provide full-duplex, bidirectional communication between a client and server. These models are designed for constant or continuous connections between the two entities.

Once a connection is established, both the client and server can exchange messages with each other. As long as the client does not request to close the connection, it remains open, and the server is aware of every open connection. This enables the client and server to communicate seamlessly and in real-time.

Future of IoT Communication Models

The future of IoT communication models is exciting and promising. As the number of connected devices and applications continue to increase, the need for efficient and effective communication models will become even more critical.

One of the most significant trends in IoT communication models is the shift towards edge computing. This approach involves processing data closer to the source, rather than transmitting it to a centralized cloud server. By moving processing closer to the edge of the network, latency can be reduced, and real-time responses can be achieved. This approach also reduces the amount of data that needs to be transmitted, reducing bandwidth requirements and improving efficiency.

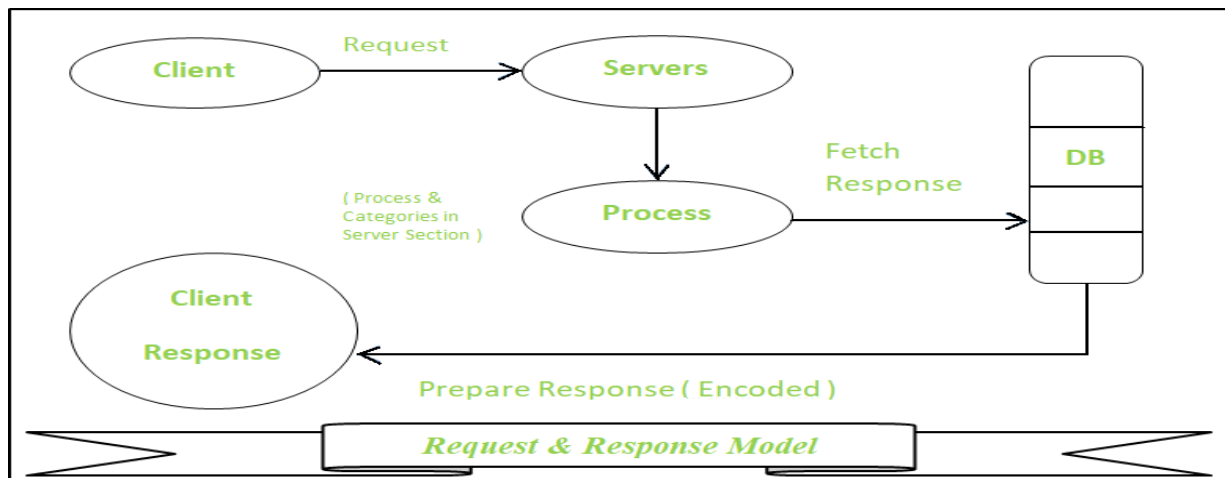
Another trend is the development of hybrid communication models that combine different communication protocols to achieve the best possible results. For example, a hybrid model might combine the Publish-Subscribe model with the Request-Response model to achieve real-time data updates while still allowing for targeted data requests.

IoT devices are found everywhere and will enable circulatory intelligence in the future. For operational perception, it is important and useful to understand how various IoT devices communicate with each other. Communication models used in IoT have great value. The IoTs allow people and things to be connected any time, any space, with anything and anyone, using any network and any service.

Types of Communication Model:

1. Request & Response Model –
This model follows a client-server architecture.

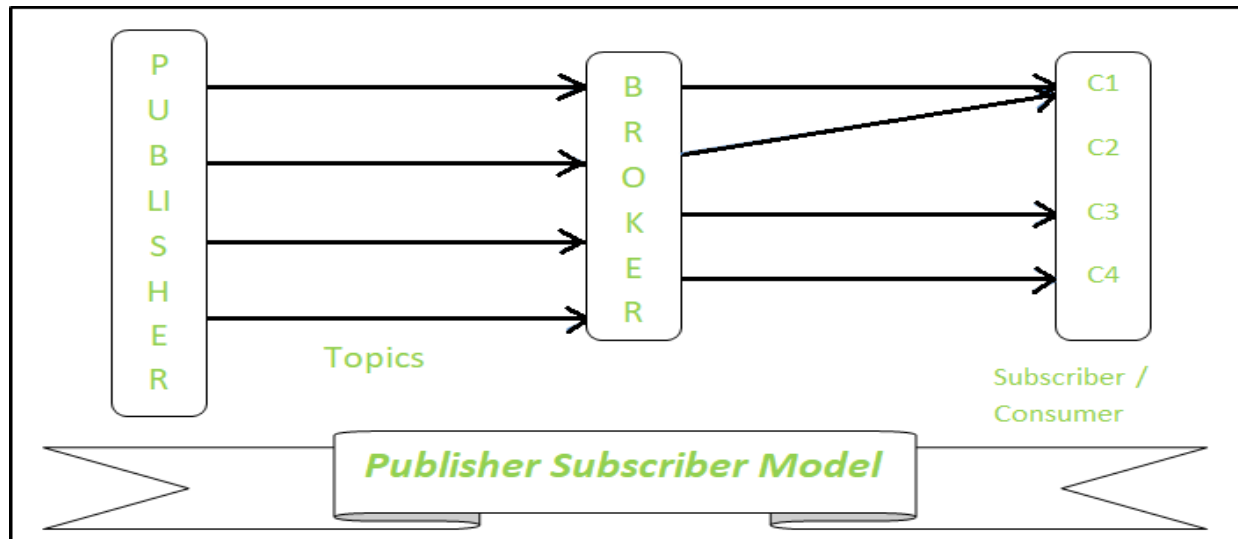
- The **client**, when required, requests the information from the server. This request is usually in the encoded format.
- This model is stateless since the data between the requests is not retained and each request is independently handled.
- The server categorizes the request, and fetches the data from the database and its resource representation. This data is converted to response and is transferred in an encoded format to the client. The client, in turn, receives the response.
- On the other hand — In **Request-Response** communication model client sends a request to the server and the server responds to the request. When the server receives the request it decides how to respond, fetches the data, retrieves resources, and prepares the response, and sends it to the client.



2. Publisher-Subscriber Model—

This model comprises three entities: Publishers, Brokers, and Consumers.

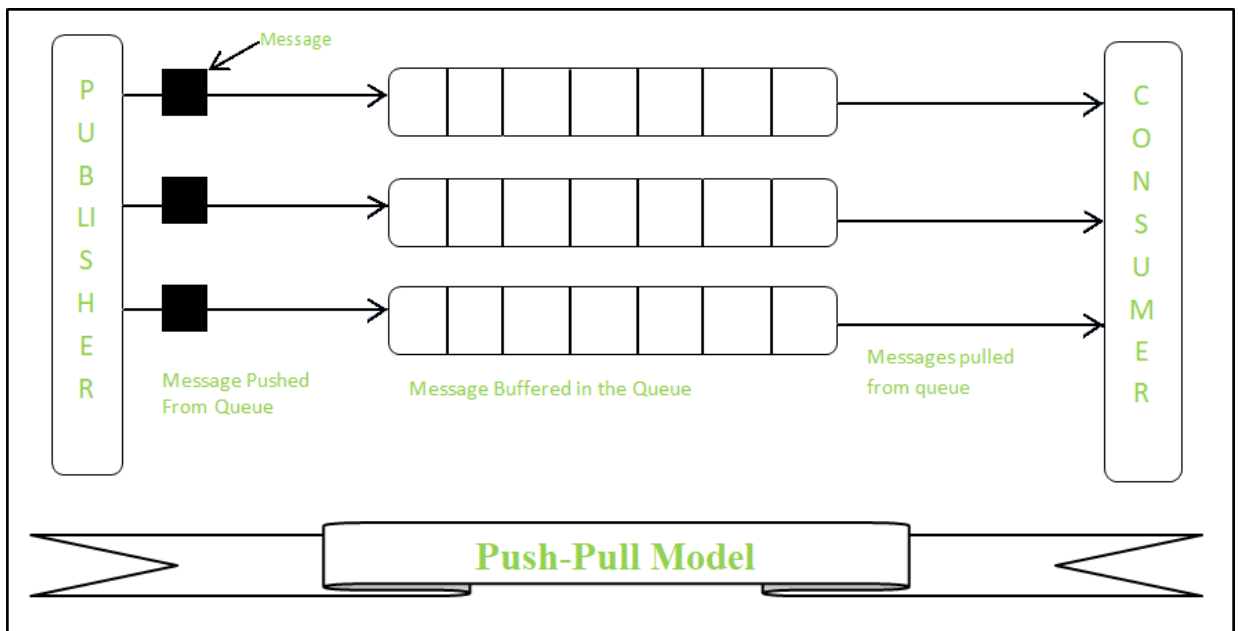
- **Publishers** are the source of data. It sends the data to the topic which are managed by the broker. They are not aware of consumers.
- **Consumers** subscribe to the topics which are managed by the broker.
- Hence, **Brokers** responsibility is to accept data from publishers and send it to the appropriate consumers. The broker only has the information regarding the consumer to which a particular topic belongs to which the publisher is unaware of.



3. Push-Pull Model-

The push-pull model constitutes data publishers, data consumers, and data queues.

- **Publishers and Consumers** are not aware of each other.
- Publishers publish the message/data and push it into the queue. The consumers, present on the other side, pull the data out of the queue. Thus, the queue acts as the buffer for the message when the difference occurs in the rate of push or pull of data on the side of a publisher and consumer.
- **Queues** help in decoupling the messaging between the producer and consumer. Queues also act as a buffer which helps in situations where there is a mismatch between the rate at which the producers push the data and consumers pull the data.



4. Exclusive Pair-

- **Exclusive Pair** is the bi-directional model, including full-duplex communication among client and server. The connection is constant and remains open till the client sends a request to close the connection.
- The **Server** has the record of all the connections which has been opened.
- This is a state-full connection model and the server is aware of all open connections.
- WebSocket based communication API is fully based on this model.



Conclusion

Finally, there is a growing focus on security and privacy in IoT communication models. As the number of connected devices continues to grow, the risk of security breaches and data theft also increases. Communication models that prioritize security and privacy will become increasingly important in the future to ensure the safe and secure exchange of data.

1. Explain in detail about the IoT enabling technology.

IoT Enabling Technologies

IoT is enabled by several technologies including Wireless Sensor Networks, Cloud Computing, Big Data Analytics, Embedded Systems, Security Protocols and architectures, Communication Protocols, Web Services, Mobile internet and semantic search engines.

- 2) **Wireless Sensor Network (WSN):** Comprises of distributed devices with sensors which are used to monitor the environmental and physical conditions. Zig Bee is one of the most popular wireless technologies used by WSNs.

WSNs used in IoT systems are described as follows:

- **Weather Monitoring System:** in which nodes collect temp, humidity and other data, which is aggregated and analyzed.
- **Indoor air quality monitoring systems:** to collect data on the indoor air quality and concentration of various gases.
- **Soil Moisture Monitoring Systems:** to monitor soil moisture at various locations.
- **Surveillance Systems:** It uses WSNs for collecting surveillance data (motion data detection).
- **Smart Grids:** use WSNs for monitoring grids at various points.

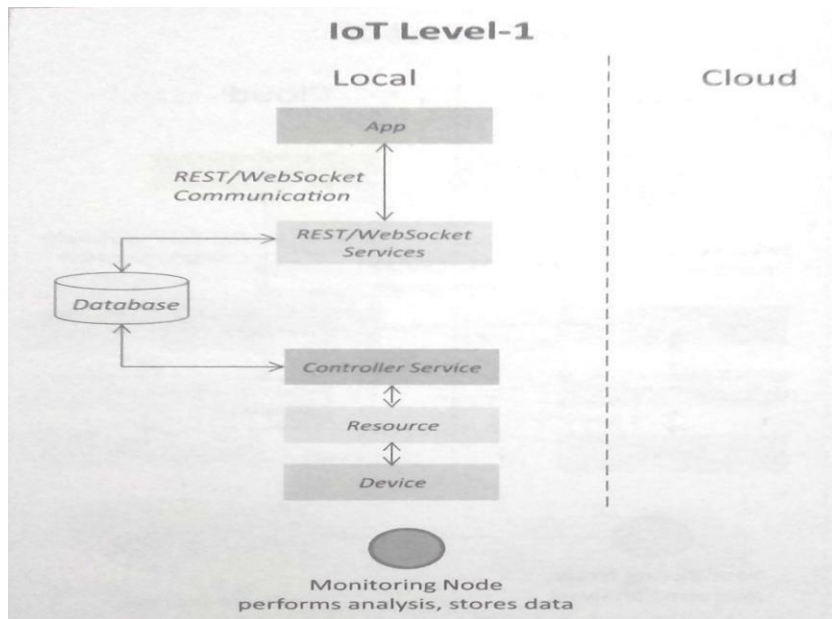
Structural Health Monitoring Systems:

It Use WSN to monitor the health of structures (building, bridges) by collecting vibrations from sensor nodes deployed at various points in the structure.

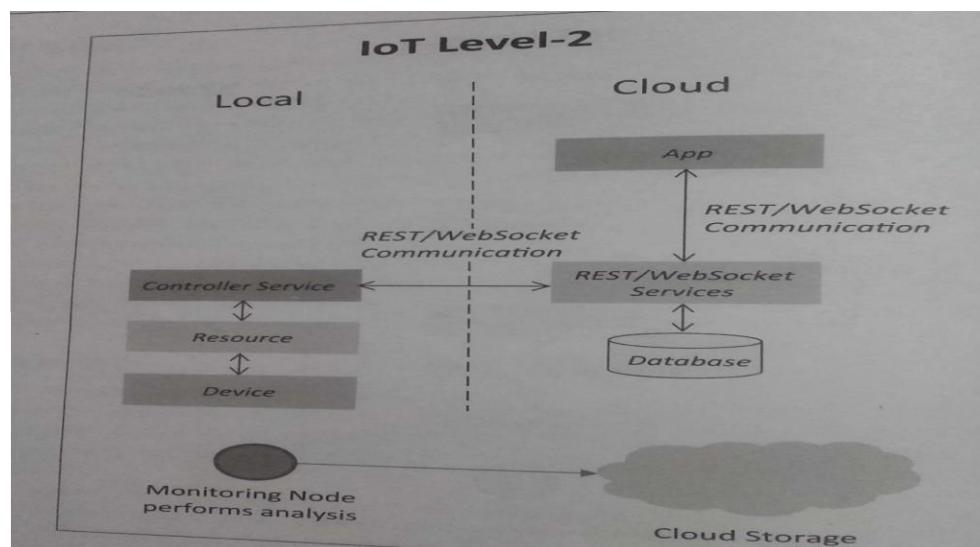
- 3) **Cloud Computing:** Services are offered to users in different forms.
 - Infrastructure-as-a-service (IaaS): provides users the ability to provision computing and storage resources. These resources are provided to the user as a virtual machine instances and virtual storage.
 - Platform-as-a-Service (PaaS): provides user the ability to develop and deploy application in cloud using the development tools, APIs, software libraries and services provided by the cloud service provider.
 - Software-as-a-Service (SaaS): provides the user a complete software application or the user interface to the application itself.
- 4) **Big Data Analytics:** Some examples of big data generated by IoT are
 - Sensor data generated by IoT systems.
 - Machine sensor data collected from sensors established in industrial and energy systems.
 - Health and fitness data generated IoT devices.
 - Data generated by IoT systems for location and tracking vehicles.
 - Data generated by retail inventory monitoring systems.
- 5) **Communication Protocols:** form the back-bone of IoT systems and enable network connectivity and coupling to applications.
 - Allow devices to exchange data over network.
 - Define the exchange formats, data encoding addressing schemes for device and routing of packets from source to destination.
 - It include sequence control, flow control and retransmission of lost packets.
- 6) **Embedded Systems:** is a computer system that has computer hardware and software embedded to perform specific tasks. Embedded System range from low cost miniaturized devices such as digital watches to devices such as digital cameras, POS terminals, vending machines, appliances etc.,

2. Explain in detail about the IoT Levels and Deployment Templates

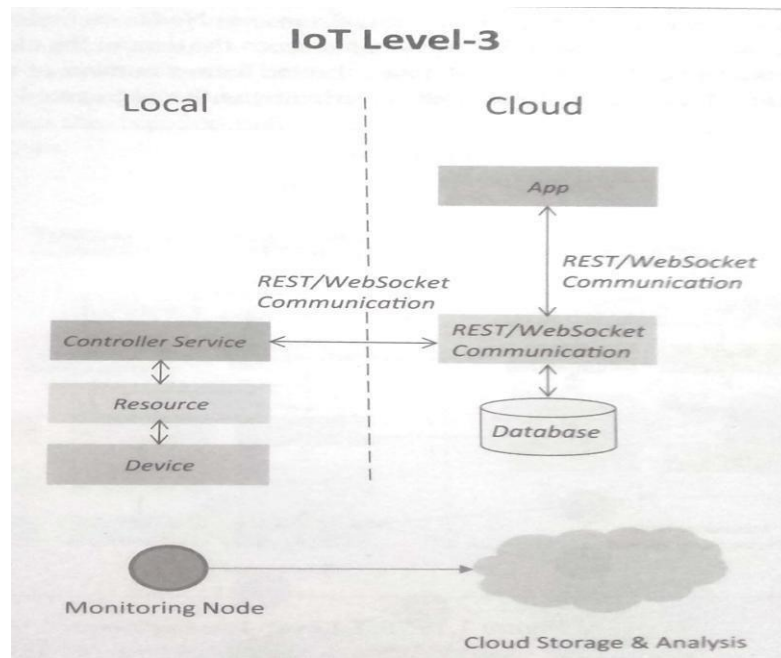
- 1) **IoT Level 1:** System has a single node that performs sensing and/or actuation, stores data, performs analysis and host the application as shown in fig. Suitable for modeling low cost and low complexity solutions where the data involved is not big and analysis requirement are not computationally intensive. An e.g. of IoT Level 1 is Home automation.



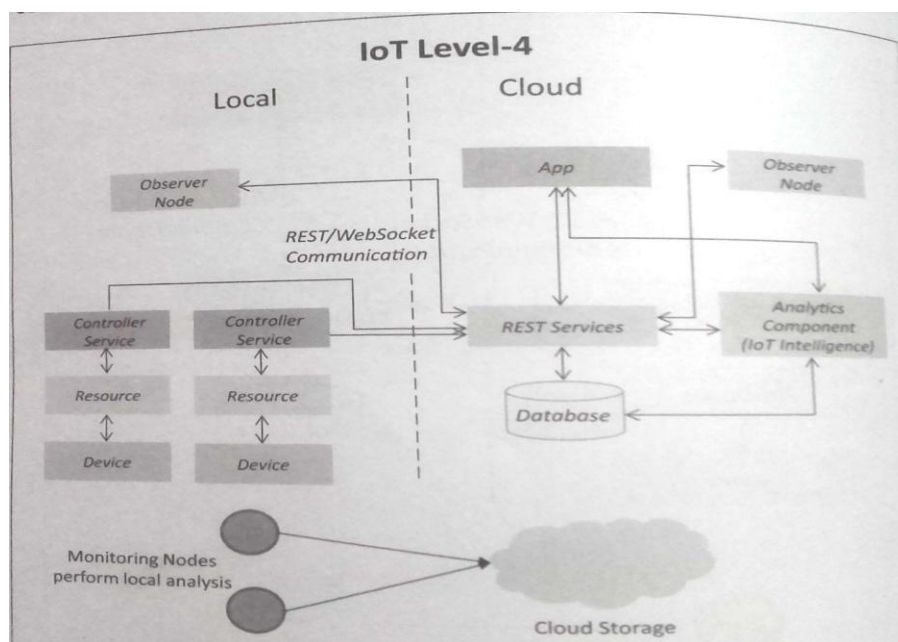
- 2) **IoT Level2:** It has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself. An example of Level2 IoT system for Smart Irrigation.



- 3) **IoT Level3:** system has a single node. Data is stored and analyzed in the cloud application is cloud based as shown in fig. Level3 IoT systems are suitable for solutions where the data involved is big and analysis requirements are computationally intensive. An example of IoT level3 system for tracking package handling.

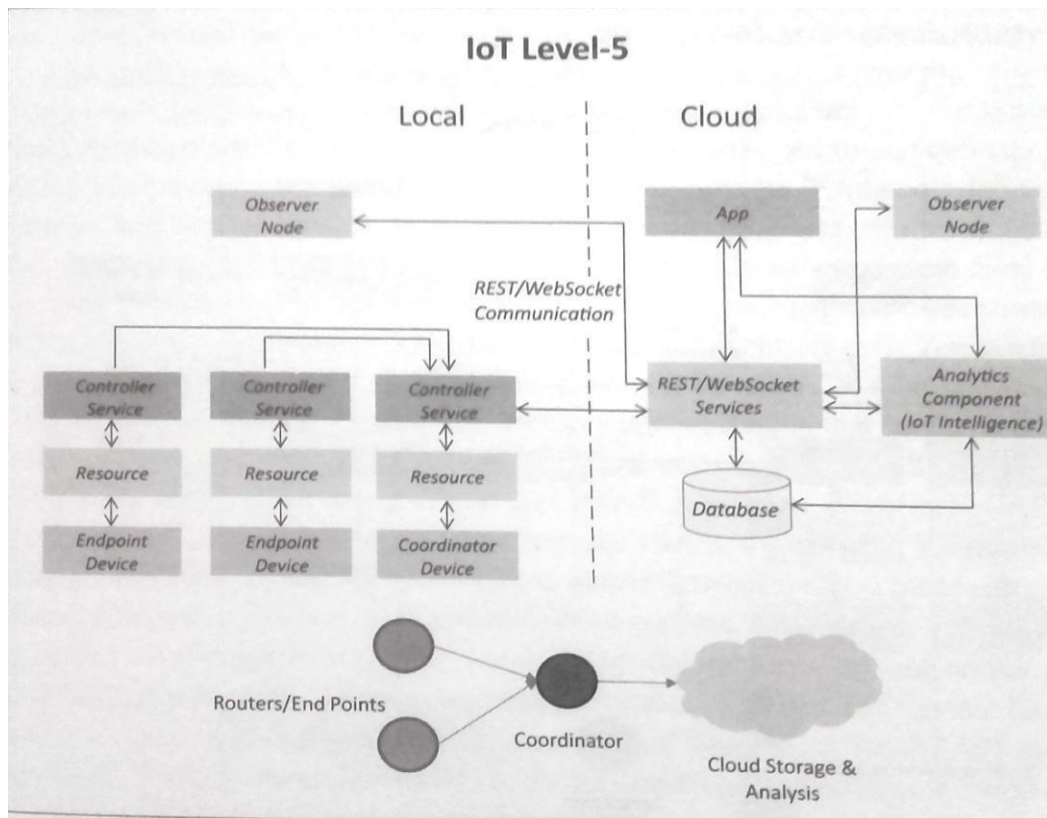


- 4) **IoT Level4:** System has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud based as shown in fig. Level4 contains local and cloud based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices. An example of a Level4 IoT system for Noise Monitoring.



- 5) **IoT Level5:** System has multiple end nodes and one coordinator node as shown in fig. The end nodes that perform sensing and/or actuation. Coordinator node collects data from the end nodes and sends to the cloud. Data is stored and analyzed in the cloud and

application is cloud based. Level5 IoT systems are suitable for solution based on wireless sensor network, in which data involved is big and analysis requirements are computationally intensive. An example of Level5 system for Forest Fire Detection.



- 6) **IoT Level6:** System has multiple independent end nodes that perform sensing and/or actuation and sensed data to the cloud. Data is stored in the cloud and application is cloud based as shown in fig. The analytics component analyses the data and stores the result in the cloud database. The results are visualized with cloud based application. The centralized controller is aware of the status of all the end nodes and sends control commands to nodes. An example of a Level6 IoT system for Weather Monitoring System.

