IoT Module 1

Contents: Introduction and Definition of IoT, Applications – Characteristics - Things in IoT - IoT Stack – IoT enabling Technologies – IoT challenges – IoT Levels

(book: Vijay Madisetti, Arshdeep Bahga, Internet of Things: A Hands-On Approach, Orient Blackswan)

Introduction:

Q. What is Internet of Things (IoT):

- IoT comprises *things* that have unique identities and are connected to the internet, where the things are devices that are not traditionally associated with the Internet.
- The common devices in the network may include PCs, mobile phones, etc. But in IoT the devices may include irrigation pump, electric car, thermostats, watches, etc.
- IoT allows these *things* to communicate, collaborate and exchange data and control information while executing meaningful applications towards a common user/machine goal.
- That lower level data is converted into meaningful information by filtering, processing, categorizing, condensing and contextualizing the data.

Q. Definition of IoT

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 the information network, often communicating data associated with users and their environment.

- A dynamic global network infrastructure having self configuring capabilities.
- The devices are called *things* and have unique identities and physical attributes.
- The things use intelligent interfaces to communicate data with the users and their environment.
- They use standard and interoperable communication protocols.
- They are seamlessly integrated into the information network.

Q. IoT Applications

1. Homes
    a. Smart lighting that adapt the lighting to suit the ambient conditions
    b. Smart appliances that can be remotely monitored and controlled.
    c. Intrusion detection systems.
    d. Smart smoke sensors.
2. Cities
    a. Smart parking systems providing status updates on available slots.

   b. Smart lighting that helps in saving energy.
   c. Smart roads that provide information on driving conditions and structural health monitoring systems.
3. Environment
   a. Weather monitoring.
   b. Air and noise pollution.
   c. Forest fire detection.
   d. River flood detection.
4. Energy Systems
   a. Smart grid.
   b. Grid integration of renewable energy sources and health management systems.
5. Retail
   a. Inventory management.
   b. Smart payment.
   c. Smart vending machines.
6. Logistics
   a. Location and Route Management.
   b. Inventory Tracking and Warehousing.
   c. Autonomous and Self-Driving Cars.
   d. Drone-Based Delivery.
7. Industry
   a. Smart diagnosis and prognosis for predicting faults and their cause.
8. Agriculture
   a. Smart irrigation systems for saving water while increasing productivity.
9. Health
   a. Health and fitness monitoring systems.
   b. Wearable electronics.

Q. Characteristics of IoT

1. Dynamic and Self adapting
2. Self-configuring
3. Interoperable Communication Protocols
4. Unique Identity
5. Integrated into Information Network

1. Dynamic and Self adapting
   - IoT devices may have the capability to dynamically adapt with changing context and take actions based on their operating conditions, user's context or sensed environment.
   - Eg: Surveillance cameras changing from light mod to infrared mode during night time.
2. Self-configuring
   - Allows a large number of devices to work together to provide certain functionality.
   - Configure themselves, setup the networking, and fetch latest software upgrades with minimal manual intervention.

- Eg: weather monitoring systems.

3. Interoperable Communication Protocols
   - Support a number of interoperable communication protocols to communicate with each other and with the infrastructure.
4. Unique Identity
   - Each IoT device has a unique identity/identifier to identify it in the network.
   - Eg: IP address or URI (Uniform Resource Identifier)
   - Helps the devices to communicate with each other.
   - Helps to query the devices, monitor its status, control them remotely, configure and manage the infrastructure, etc.
5. Integrated into Information Network
   - Integrated into the network to communicate and exchange data with other devices and systems.
   - Helps to be dynamically discovered, describe themselves, and talk with other devices and the users.
   - Helps to build collective intelligence and make them smarter than being separated.
   - Eg: Weather predicting nodes generate weather updates by monitoring different geographical areas and by collaborating among them.

Q. Explain "Things" in IoT.
Q. With a neat block diagram, explain about a typical IoT device.

- *Things* in IoT refers to IoT devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities.
- They may exchange data with other connected devices and applications (directly or indirectly), or collect data from other devices and process the data either locally or send the data to centralized servers or cloud-based application back-ends for processing the data, or perform some tasks locally and other tasks within the IoT infrastructure, based on time and space constraints (ie, memory, processing capabilities, communication latencies and speeds, and deadlines).

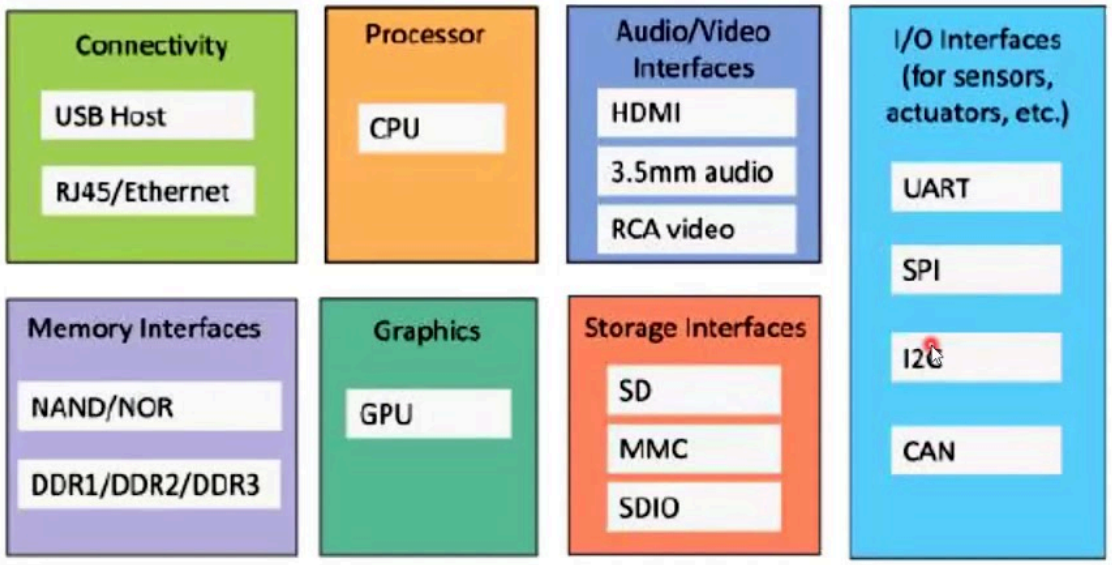


Fig: Generic block diagram of an IoT device

- Has several wired/wireless interfaces for
    1. I/O interfaces for sensors
    2. Interfaces for internet connectivity
    3. Memory and storage interfaces
    4. Audio/video interfaces
- An IoT device can collect various types of data from the on-board/attached sensors, such as temperature, humidity, light intensity.
- The sensed data can be communicated either to other devices or to cloud based servers/storage.
- IoT devices can be connected to actuators (*a device that converts energy into motion*) that allow them to interact with other physical entities (including non-IoT devices and systems) in the vicinity of the device.
- Eg: a relay switch connected to an IoT device can turn an appliance on/off based on the commands sent to the IoT device over the internet.
- IoT devices can be of many types such as wearable sensors, smart watches, LED lights, automobile and industrial machines. Almost all IoT devices generate data in some form or the other which are processed into meaningful information for further actions.

Q. Explain IoT technology stack.
Q. Explain the different components in an IoT system.

- The IoT technology stack refers to the multiple layers of hardware, software and communication technologies that connect objects over the internet to monitor or control them.
- The following layers make up the IoT technology stack:

1: Device Hardware

- Acts as the interface between the physical object and the server (local or cloud).
- Includes processing units, sensors, actuators and other input/output (I/O) components.
- To collect the data from the sensors, process and analyze them, there will be processing units which can range from simple microcontrollers to industrial computers.
- Sensors measure physical parameters, such as temperature, humidity, pressure or vibration.
- Actuators can be used to control devices, such as motors, pumps, heaters or lights.
- Other I/O components may include buttons, displays or speakers.

2: Device software

- Runs on the device's processor and controls its functionality.
- Device software typically consists of an operating system (OS) and application software.
- The OS configures and manages the device's hardware to provide a platform for the application software to run on.
    - Common embedded operating systems include FreeRTOS, Embedded Linux and Raspberry Pi OS.

- Application software uses the OS's interfaces to give the device its specific functionality.
    - For example, an application might be used to control a motor, read sensor data and transmit live or periodic status reports over a wired or wireless connection.

3: Communications

- This is how devices connect to the internet and transfer data.
- There are a variety of different technologies that can be used for IoT communications:
    - Wired Network
    - Wi-Fi
    - Bluetooth
    - Zigbee
    - 2G/3G/4G/5G cellular networks
    - LPWANs (Low Power Wide Area Networks)
    - LoRaWAN, Sigfox (unlicensed LPWANs)
- Also there will be **communication protocols** in many different standards for communication.
- Protocols are like rules for how data should be formatted and transmitted.
- Standard protocols used in the IoT include MQTT, HTTPS and CoAP.

4: Cloud Platform

- This is the hardware and software services located in internet-based data centers.
- It is where the data from IoT devices is recorded, captured, processed, analyzed and stored.
- It offers a centralized service containing computing resources and databases that can be accessed whenever from wherever.
- Offers ease of scalability in terms of infrastructure capacity and the management of device data.
- Cloud platforms usually provide tools and services that make it easier to develop and deploy IoT applications.
- Some cloud service providers include Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

5: Cloud Applications

- These applications run on top of the cloud platform and provide the end-user with a way to interact with the IoT system.
- Cloud applications include the user interfaces of dashboards, reporting suites, analytical and artificial intelligence modules.
- They can be used to view data from sensors and control actuators embedded in static or mobile machinery, plant or fleets of vehicles.

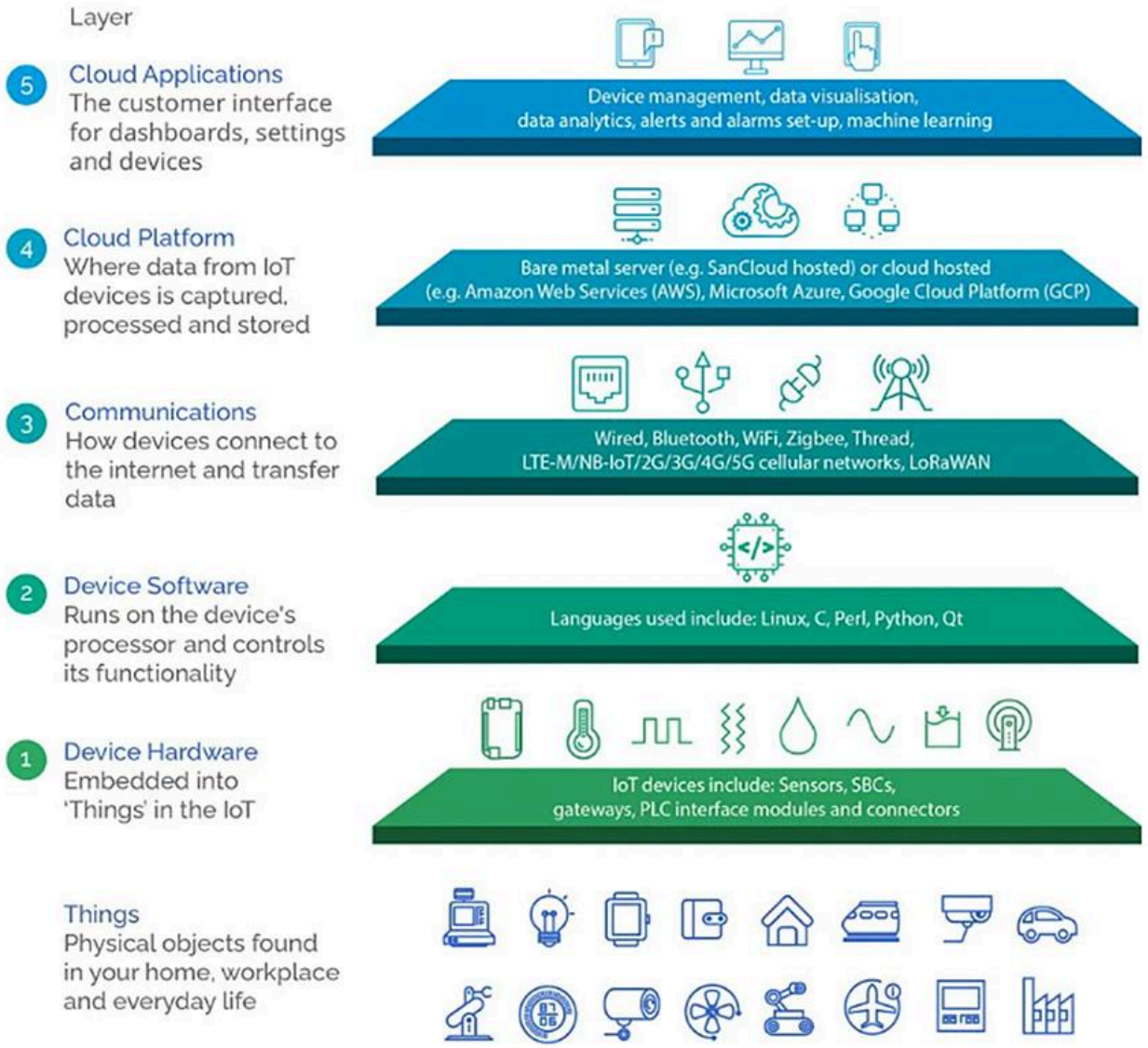


Fig: IoT Technology Stack Diagram

Q. Explain IoT Communication Models

1. *Request-Response*
   - *Clients send requests to the server and the server responds.*
   - *Each request-response pair is independent of others.*
2. *Publish-Subscribe*
   - *Has publishers, brokers and consumers.*
   - *Publishers send the data to the topics which are managed by the broker.*
   - *When a broker receives data for a topic, it sends the data to all the subscribed consumers of that topic.*
3. *Push-pull*
   - *The data producers push the data to queues and the consumers pull the data from the queue when it is ready.*

4. *Exclusive Pair*
    - *Bidirectional connection between the client and the server.*
    - *For data transfer, the client and server need to set up a connection.*
    - *The connection remains open until the client requests the server to close it.*

IoT Enabling Technologies

IoT is enabled by several technologies. Some are given below.

1. **Wireless Sensor Networks (WSN)**
    - WSN consists of wirelessly distributed devices with sensors for monitoring environmental and physical conditions.
    - There will be;
        - **End nodes** having several sensors for collecting the data from the surroundings.
        - A **coordinator** for collecting the data from the end nodes and passing the processed data to the Internet.
        - **Routers** to route the data from the end nodes to the coordinator. Some end nodes can act as routers also.
    - WSN uses wireless communication protocols such as Wifi, ZigBee which can cover an area from 10 to 100 meters.
    - The end nodes will be low cost and low power consuming nodes, continuously monitoring the surroundings.
    - The end nodes may be large in number with self configuring capabilities such that addition or malfunctioning of a node will lead to self reconfiguration without any manual intervention.

2. **Cloud Computing**
    - A method of **delivering services and applications** over the Internet.
    - Provides computing, networking and storage resources on demand in a **pay as you go** model.
    - Cloud services can be accessed through standard access mechanisms that provide platform-independent access (ie, from computers, mobile phones, etc.).
    - Cloud services are available in different forms such as;
        - **Infrastructure-as-a-Service (IaaS):**
            - Provides computing and storage resources over the cloud.
            - As virtual machine instances and virtual storages.
            - Users can deploy operating systems and applications of their choice.
            - The physical infrastructure is managed by the service provider.
            - Users are billed on a pay-per-use manner.
            - Google Compute Engine (GCE), Amazon Web Services (AWS) Elastic Compute Cloud (EC2), Microsoft Azure.
        - **Platform-as-a-Service (PaaS):**
            - Provides the ability to develop, deploy, manage and configure applications in the cloud using development tools, application

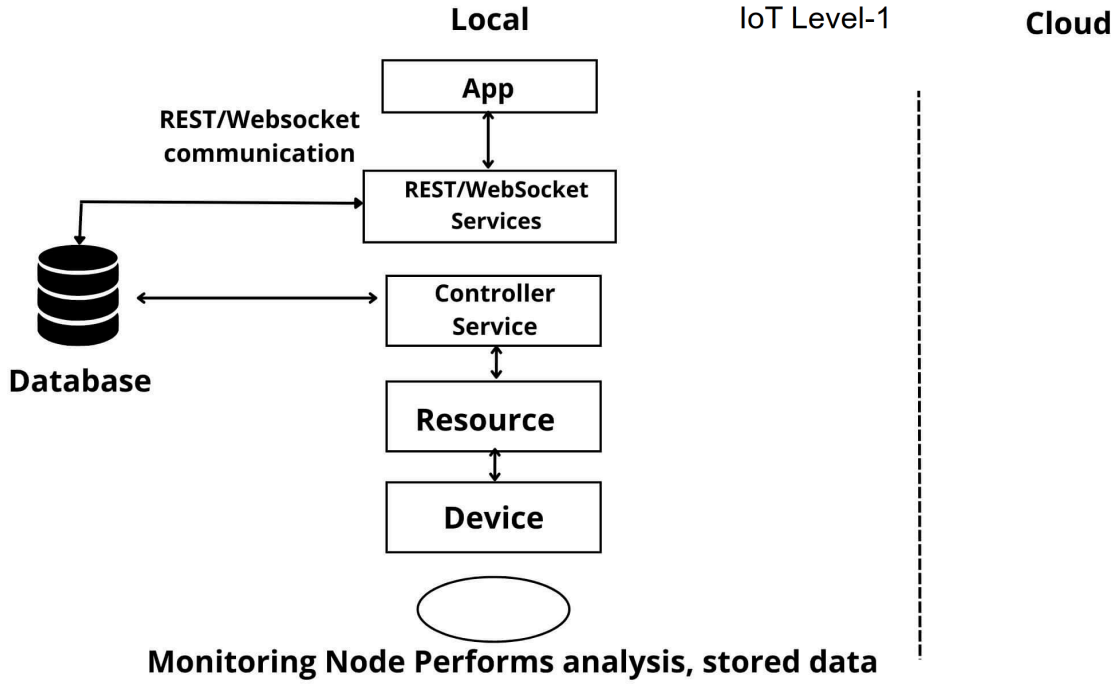
programming interfaces (API), software libraries and services provided by the cloud service provider.
        - The cloud service provider manages the underlying cloud infrastructure including servers, network, operating system and storage.
        - Eg: Google App Engine, AWS Elastic Beanstalk
    - **Software-as-a-Service (SaaS):**
        - Provides the users a complete software application or a user interface to the application itself.
        - The cloud service provider manages the underlying cloud infrastructure including servers, operating system, application software, storage and network.
        - The user need not know the underlying architecture of the cloud.
        - The user accesses the application through a thin client interface such as a web browser, mobile app, etc.
        - Eg: Google Workspace, Dropbox

3. **Big Data Analytics**
    - Big data is a collection of data sets whose volume, variety and velocity are so large that it is difficult to store, manage, process and analyze the data using traditional databases and data processing tools.
    - Big data analytics involves several steps starting from data cleansing, data classification, data processing and visualization.
    - Some examples of Big Data generated by IoT systems are;
        - Sensor data generated by IoT systems such as weather monitoring stations.
        - Data generated by IoT systems for location tracking of vehicles.
        - Health and fitness data generated by IoT devices such as wearable fitness bands.
    - Three V's of Big Data
        - Volume: The volume of data generated by the IoT systems will be very huge, even if the amount of useful information in them may be small. Collecting, storing, filtering, analyzing, classifying these data is very difficult.
        - Velocity: Refers to how fast the data is generated from all over the world.
        - Variety: Refers to the forms of data. This data consists of text of various kinds, audio, video, images, etc.
4. **Embedded Systems**
    - An embedded system is an electronic system that has computing hardware and software embedded in them to **perform specific tasks**.
    - That will have a microprocessor/microcontroller, memory (RAM, ROM, etc.), networking units, I/O units and storage.
    - Some have special units such as Digital Signal Processors, Graphics processors, etc.
    - Embedded systems may have special types of operating systems such as RTOS (Real Time OS).
    - Most of the embedded systems have miniature, low-cost hardware.

IoT Levels

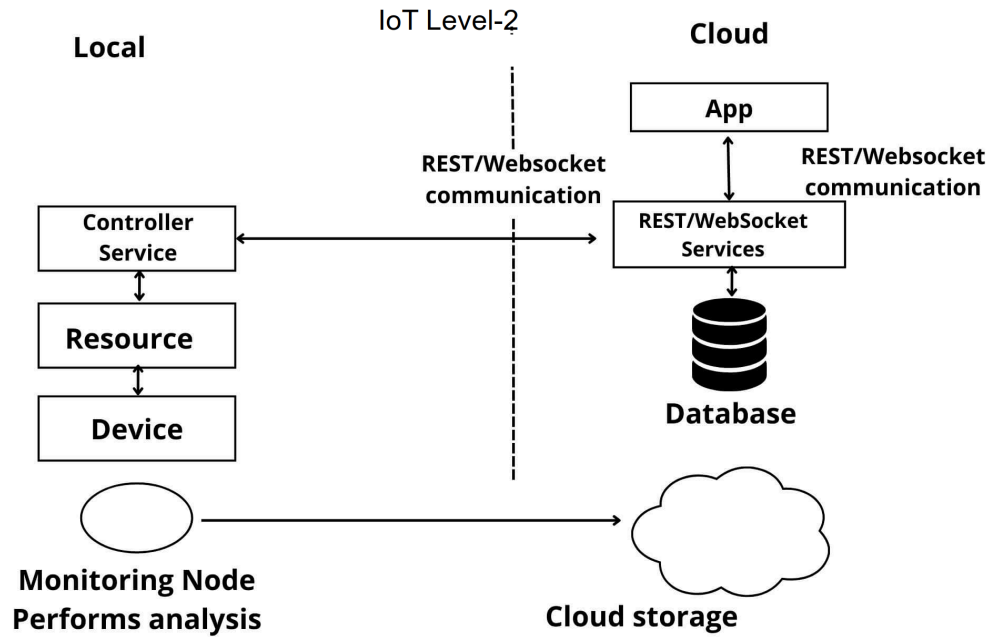
IoT Level-1

- It has a single node/device that performs sensing and/or actuation, stores data, performs analysis and hosts the application.
- Suitable for modeling low-cost, low-complexity systems where the amount of data and computations are small.
- Eg: A **small home automation system** consisting of a single node that handles the lights and appliances remotely. The device has electronic relay switches to manage the appliances, and stores the status information in a local database. A web service manages this data, a controller service triggers the relay switches and the application in the user's mobile/computer controls all this through the Internet.



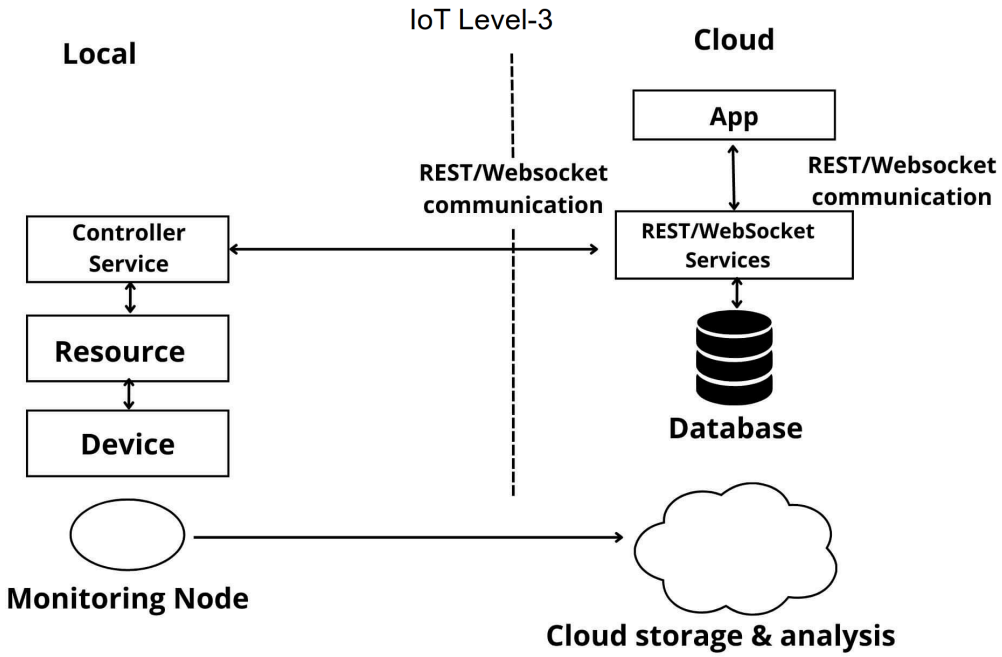
IoT Level-2

- A **single node that performs sensing and/or actuation and local analysis.**
- The **data is stored in the cloud** and the **application is usually cloud-based**.
- Useful for small systems where the data is big, but the analysis is not complex and can be done locally itself.
- Eg: A Smart Irrigation System consisting of a single node that monitors the soil moisture level and controls the irrigation system. The data from the sensors are collected by the controller service. If it drops below a threshold, the actuator is worked and sprinkles water. But the data is continuously sent to the cloud storage for later visualization over a period of time.



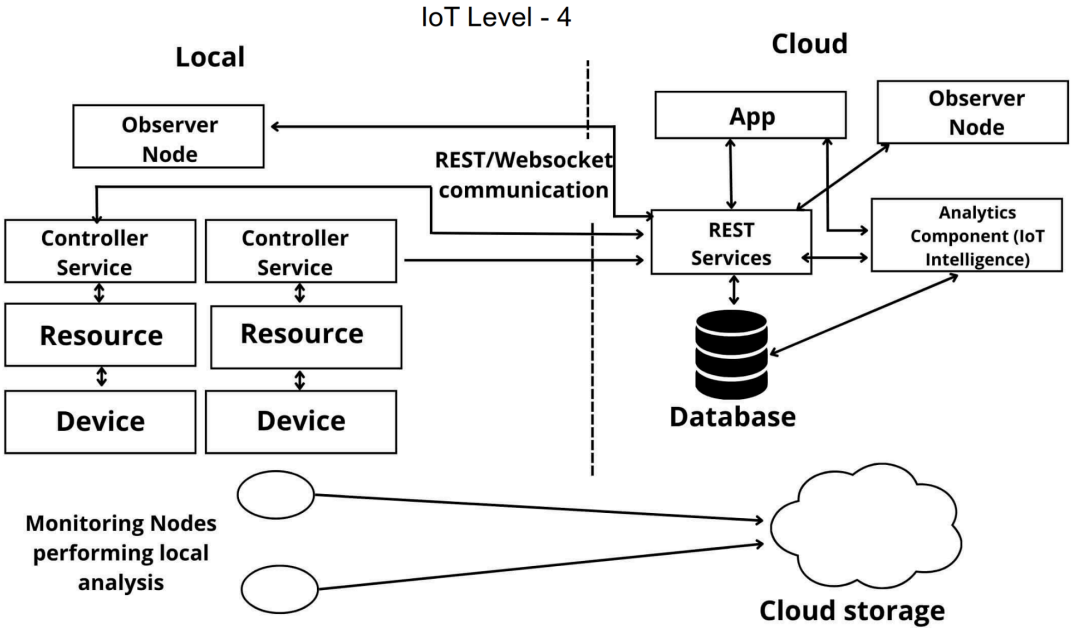
IoT Level-3

- A single sensor node collects the data, stores the data in the cloud where it is analyzed.
- Useful where the data involved is big and the analysis requirements are computationally intensive.
- Eg: An IoT system for tracking package handling. It consists of a single node (for a package) that monitors the vibration levels for a package being shipped. The device uses accelerometer and gyroscope sensors for monitoring vibration levels. The controller service sends the sensor data to the cloud in real time. The data is stored in the cloud, analyzed there, and decides actions. The data can be visualized in real time also.



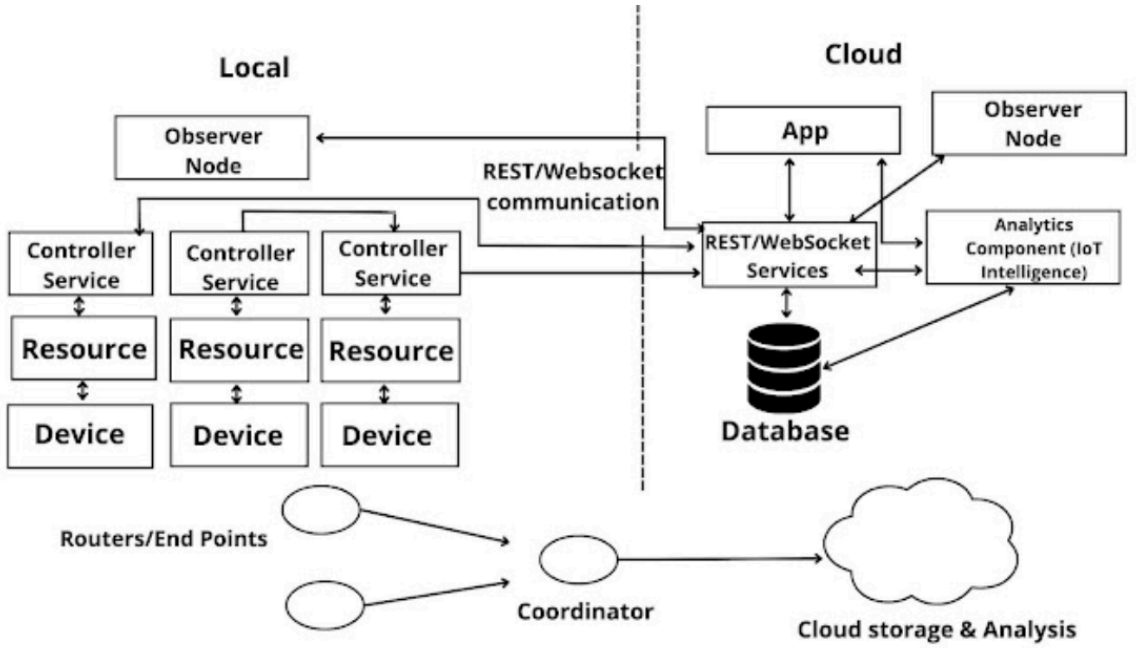
IoT Level-4

- **Multiple** nodes that perform **local** analysis.
- Data is stored in the cloud and the application is cloud-based.
- There are local and cloud-based **observer** nodes which can subscribe to and receive information collected in the cloud from IoT devices.
- Observer nodes can process information and use it for various applications, but do not perform any control functions.
- Suitable for solutions where multiple nodes are required, the data involved is big and the analysis requirements are computationally intensive.
- Eg: A noise monitoring system consisting of multiple independent nodes placed in different locations for monitoring noise levels in an area. The nodes collect data using its sound sensors and store it in the cloud. The cloud-based application visualizes the aggregated data.



IoT Level-5

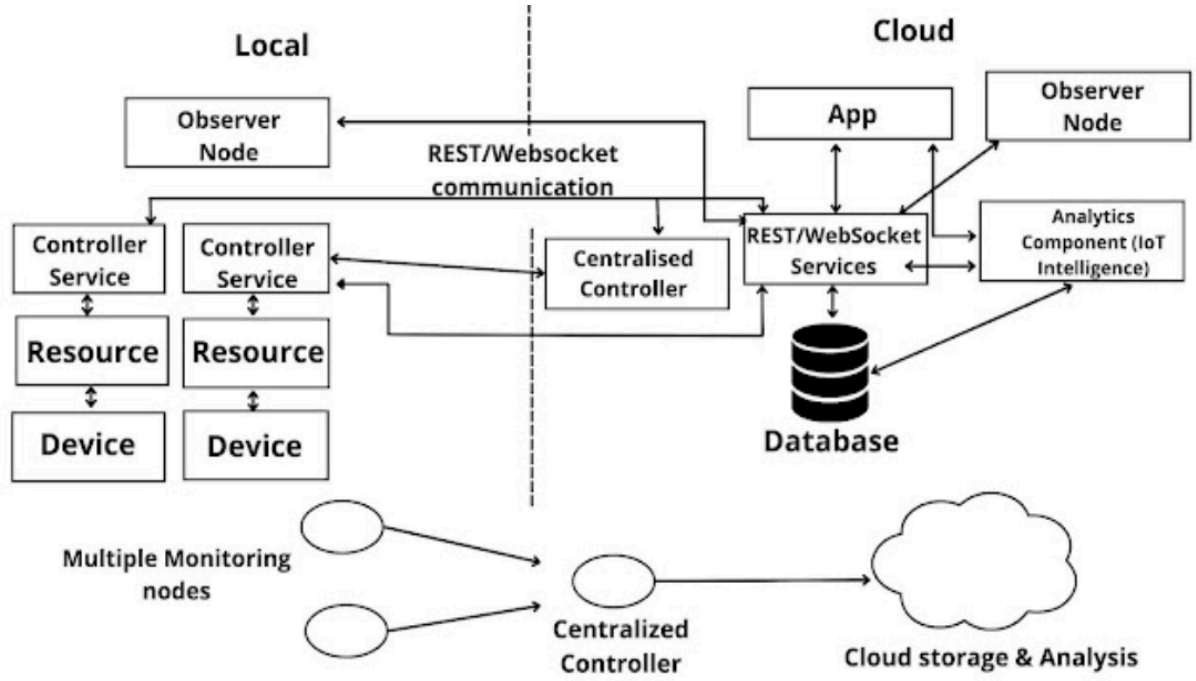
- Multiple end nodes and one coordinator node.
- End nodes perform sensing and/or actuation.
- Coordinator node collects the data from end nodes and sends it to the cloud.
- Data is stored and analyzed in the cloud and the application is cloud-based.
- Suitable for Wireless Sensor Networks, in which the data involved is big and the analysis requirements are computationally intensive.
- Eg: The forest fire detection system consists of multiple nodes placed in different locations for monitoring temperature, humidity and carbon dioxide levels in the forest. The end nodes have sensors for sensing these. The coordinator node collects these data from end nodes and sends it to the cloud where it is stored, analyzed, and predictions and visualizations are made.



IoT Level-5

IoT Level-6

- Multiple independent end nodes that perform sensing and/or actuation and send data to the cloud.
- Data is stored in the cloud and the application is cloud-based.
- The data in the cloud is analyzed and the results are stored in the cloud database itself.
- The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes.
- Eg: In a weather monitoring system, multiple nodes are placed in different locations for monitoring temperature, humidity and pressure in that area using their sensors. The end nodes send data to the cloud database in real time. The data analysis, result calculation, weather prediction, etc are done in the cloud. A cloud-based application is used for visualizing the data.



IoT Level-6

IoT challenges

Major challenges are;

- Security challenges
- Design challenges
- Scalability challenges
- Reliability challenges
- Power consumption
- Deployment challenges

Security challenges in IoT :

1. Lack of encryption
2. Insufficient testing and updating
3. Risk of default passwords
4. IoT Malware and ransomware
5. Inadequate device security
6. Lack of standardization
7. Vulnerability to network attacks
8. Unsecured data transmission
9. Software vulnerabilities
10. Insider threats

To address these challenges, it is important to implement security measures such as encryption, secure authentication, and software updates to ensure the safe and secure operation of IoT devices and systems.

Design challenge in IoT :

Design challenges in IoT (Internet of Things) refer to the technical difficulties and trade-offs involved in creating connected devices that are both functional and secure. Some of the key design challenges in IoT include:

- Interoperability
- Security such as Device security, Network security, Data security and Privacy

To address these security challenges, organizations should implement robust security measures such as encryption, firewalls, and regular software updates. Additionally, they should conduct regular security audits and assessments to identify and address potential security risks.

Scalability challenges:

Scalability refers to the ability of a system to handle increasing workloads or numbers of users without a significant decline in performance. In the context of the Internet of Things (IoT), scalability is a major challenge as the number of connected devices is rapidly growing, leading to an increased volume of data and communication. Scalability challenges in IoT include:

1. Data management
2. Network capacity
3. Device management

To address these scalability challenges, organizations should adopt scalable architectures, such as cloud computing, that can accommodate the growing number of IoT devices and the data they generate. Additionally, they should implement efficient data management and storage solutions, such as distributed databases and data lakes, to handle the increased volume of data.

Reliability challenges:

Reliability refers to the ability of a system to perform its intended function consistently and without failure over time. In the context of the Internet of Things (IoT), reliability is a critical concern, as the failure of even a single IoT device can have significant consequences. Some of the reliability challenges in IoT include:

1. Device failure
2. Network connectivity
3. Data accuracy

To address these reliability challenges, organizations should implement robust and reliable hardware and software designs for IoT devices, and conduct regular testing and maintenance to identify and resolve any issues. They should also implement redundant systems and failover mechanisms to ensure that the system continues to function in the event of a failure.

Power consumption:

Power consumption refers to the amount of energy that a system or device uses. In the context of the Internet of Things (IoT), power consumption is a critical challenge, as many IoT devices are

designed to be small, low-power, and operate using batteries. Some of the power consumption challenges in IoT include:

1. Battery life
2. Energy efficiency
3. Power management

To address these power consumption challenges, organizations should adopt low-power technologies and energy-efficient designs for IoT devices. They should also implement effective power management techniques, such as sleep modes, to reduce the power consumption of IoT devices when they are not in use.

Deployment challenges in IoT :

The deployment of Internet of Things (IoT) systems can present several challenges, including:

1. Connectivity
2. Cross platform capability
3. Data collection and processing
4. Lack of skill set
5. Integration
6. Network infrastructure
7. Device management
8. Data management
9. Security
10. Cost