EC611OE: FUNDAMENTALS OF INTERNET OF THINGS

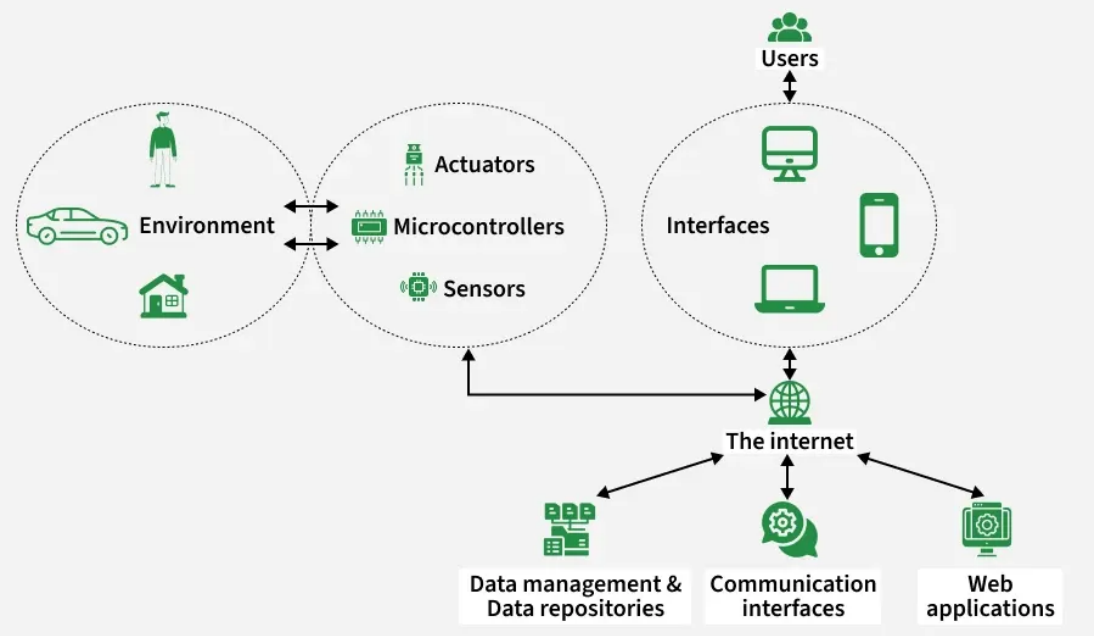
##

UNIT – I Introduction to Internet of Things: Characteristics of IoT, Physical design of IoT, Functional blocks of IoT, Sensing, Actuation, Basics of Networking, Communication Protocols, Sensor Networks.

##

Topic1: Introduction to Internet of Things:

The Internet of Things (IoT) connects everyday physical objects—like appliances, vehicles, and sensors—to the internet, allowing them to collect, exchange, and act on data without constant human intervention, creating smart environments that enhance efficiency, convenience, and decision-making in homes, cities, and industries through embedded sensors, software, and connectivity.



Core Components:

1. Things/Devices: Physical objects embedded with sensors, software, and electronics (e.g., smartwatches, smart meters, cameras).
2. Sensors: Collect real-world data (temperature, motion, light).
3. Actuators: Perform physical actions (e.g., turning lights off, adjusting a valve).
4. Connectivity: Protocols (Wi-Fi, 5G, MQTT) for communication.
5. Data Processing & Analytics: Software and AI to interpret data and make decisions.

1. Devices & Sensors

- Physical objects embedded with sensors or actuators that collect data from the environment (e.g., temperature, motion, gas, light).
- Sensors convert physical signals into digital data for further analysis.

2. Connectivity: Networks such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, or 5G that transmit data between devices, gateways, and cloud platforms.

3. Data Processing

- Edge devices, gateways, or cloud platforms process and analyze collected data, often using AI or big data technologies.
- This step transforms raw data into meaningful insights.

4. User Interface (UI)

- Applications, dashboards, or mobile apps through which users interact with IoT systems.
- Interfaces can also trigger actuators to perform automated actions.

Different types of Sensors

1. Temperature Sensors: Measure heat or temperature changes in the environment or objects.
2. Image Sensors: Capture visual data for cameras and computer vision applications.
3. Gyro Sensors (Gyroscope): Detect angular velocity and orientation of objects.
4. Obstacle Sensors: Identify the presence of obstacles to avoid collisions.
5. RF Sensors: Use radio frequency signals for detection, tracking, and communication.
6. IR Sensors (Infrared): Detect heat signatures or motion using infrared light.
7. MQ-02/05 Gas Sensors: Sense the presence and concentration of gases like CO, methane, or smoke.
8. LDR Sensor (Light Dependent Resistor): Measure light intensity and brightness levels.
9. Ultrasonic Distance Sensor: Calculate distance by using ultrasonic sound waves.

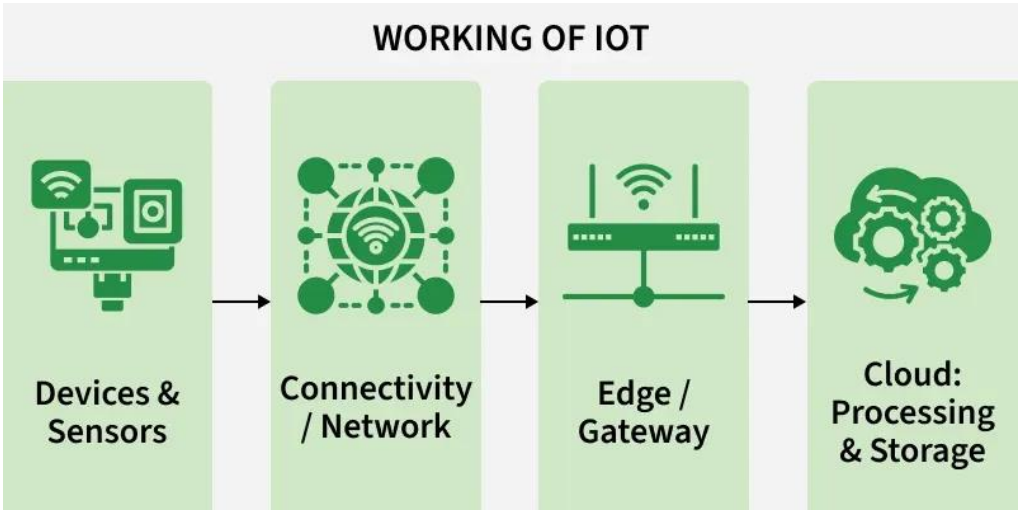
IoT Enablers

- IoT enablers are the key technologies and tools that make the Internet of Things work.
- They provide the foundation for devices to connect, collect data, process information, and deliver meaningful outcomes.
- RFID & NFC: Used for automatic identification and tracking of objects through radio waves or short-range communication.
- Sensor Technologies: Devices that measure environmental factors such as motion, temperature, gas, or light and convert them into digital signals.
- Low-Power Embedded Systems: Specialized hardware designed to consume minimal energy while delivering reliable performance, ensuring longer device life.

- Smart Networks & Protocols: Communication methods like MQTT, CoAP, Zigbee, and 5G that enable fast, efficient, and reliable data transfer.
- Cloud & Big Data: Platforms that store, manage, and analyze massive volumes of IoT data to generate insights.
- Edge/Fog Computing: Local data processing near the devices, reducing latency, improving speed, and saving bandwidth.

Working of IoT Devices

- Collect and Transmit Data: For this purpose sensor are widely used, they are used as per requirements in different application areas.
- Actuate device based on triggers produced by sensors or processing devices: If certain conditions are satisfied or according to user's requirements if certain trigger is activated then which action to perform that is shown by Actuator devices.
- Receive Information: From network devices, users or devices can take certain information also for their analysis and processing purposes.
- Communication Assistance: Communication assistance is the phenomenon of communication between 2 networks or communication between 2 or more IoT devices of same or different networks. This can be achieved by different communication protocols like MQTT, Constrained Application Protocol, ZigBee, FTP, HTTP etc.



##

Topic: 2- Characteristics of IoT

1. Always Connected: IoT devices love to stay connected, but to save energy they sometimes take small naps (sleep mode) and wake up only when needed.
2. Good at Teamwork: They can talk to all kinds of other devices big or small, old or new without complaining about differences in hardware or software.

3. Adaptive in Nature: Like a quick learner, an IoT device can adjust itself when situations change for example, a smart light getting brighter when the room gets dark.
4. Quietly Smart: They don't just collect data; they process it to give meaningful insights like a fitness tracker telling you not just how many steps you walked, but how healthy your activity level is.
5. Scalable: Whether you add one device or thousands, IoT systems are designed to grow without losing efficiency.
6. Energy Conscious: They know how to save battery, turning off when not in use and waking up only when needed, just like an energy-efficient roommate.

Characteristics of IoT

I) 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 comprising of a number of surveillance cameras. The surveillance camera can adapt modes based on whether it is day or night. The surveillance system is adapting itself based on context and changing conditions.

II) Self Configuring:

IOT devices have self-configuring capability, allowing a large number of devices to work together to provide certain functionality. These devices have the ability configure themselves setup networking, and fetch latest software upgrades with minimal manual or user interaction.

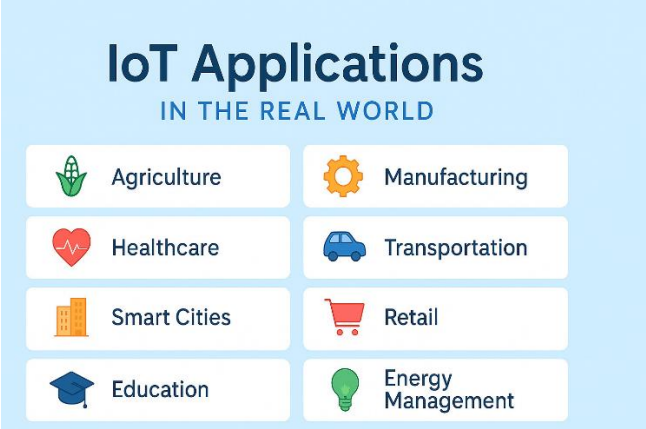
iii) Inter Operable Communication Protocols: support a number of interoperable communication protocols and can communicate with other devices and with infrastructure.

iv) Unique Identity: Each IoT device has a unique identity and a unique identifier (IP address).

v) Integrated into Information Network: that allow them to communicate and exchange data with other devices and systems.

Modern Applications of IoT:

- Smart Grids and energy saving
- Smart cities
- Smart homes/Home automation
- Healthcare
- Earthquake detection
- Radiation detection/hazardous gas detection
- Smartphone detection



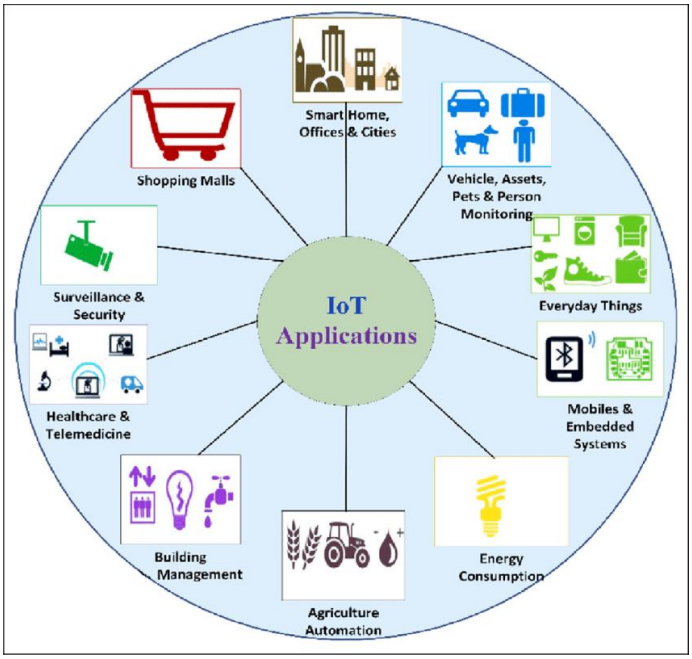


Fig: Applications of IoT

History of IOT:

1. 1982: Vending Machine: First IoT concept; reported inventory status remotely.
2. 1990: Toaster: First internet-connected appliance; remote control of devices.
3. 1999:IoT Term Coined: Kevin Ashton introduced "Internet of Things."
4. 2000: LG Smart Fridge: Remote monitoring of fridge contents; IoT in daily life.
5. 2004: Smart Watch: Wearables with fitness tracking & notifications.
6. 2007: iPhone: Smartphones became IoT hubs via apps and connectivity.
7. 2009: Cars: IoT enabled diagnostics , performance monitoring.
8. 2011: Smart TV: Internet enabled entertainment & apps.
9. 2013: Google Lens: Object recognition linking physical world to digital info.
10. 2014: Amazon Echo: Voice controlled smart home via Alexa.

11. 2015: Tesla Autopilot: Semiautonomous driving with IoT sensors/software.

Advantages of IoT

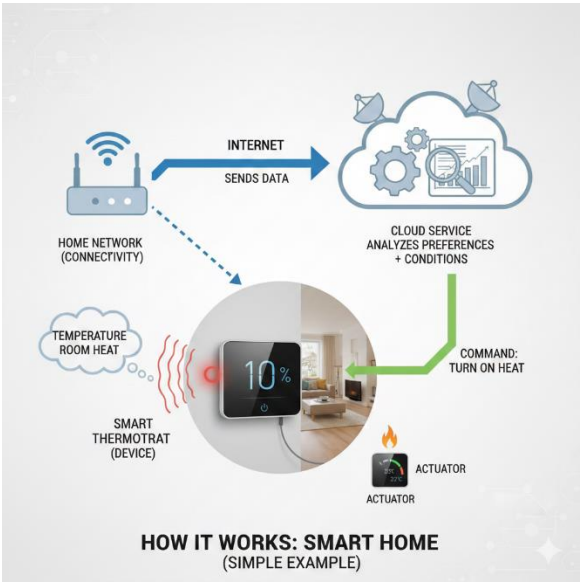
1. Improved efficiency and automation of tasks.
2. Increased convenience and accessibility of information.
3. Better monitoring and control of devices and systems.

Disadvantages of IoT

1. Potential for hacking and data breaches.
2. Collection and misuse of personal data.
3. Significant initial investment required.

How It Works (Simple Example: Smart Home)

1. Sensing: A smart thermostat (device) uses a temperature sensor to detect the room's heat.
2. Connecting: It sends this data over your home network (connectivity) to the internet.
3. Analyzing: A cloud service analyzes your preferences and current conditions.
4. Acting: The system sends a command back to the thermostat (actuator) to turn on the heat to your preferred setting.



Key Benefits & Applications

1. Smart Homes: Automated lighting, security, and climate control.
2. Smart Cities: Efficient energy use, traffic management, waste reduction.
3. Healthcare: Remote patient monitoring, wearable health trackers.
4. Agriculture: Soil monitoring, precision irrigation, livestock tracking.
5. Manufacturing (Industry 4.0): Predictive maintenance, automated quality control.

##

TOPIC: 3 Physical design of IoT

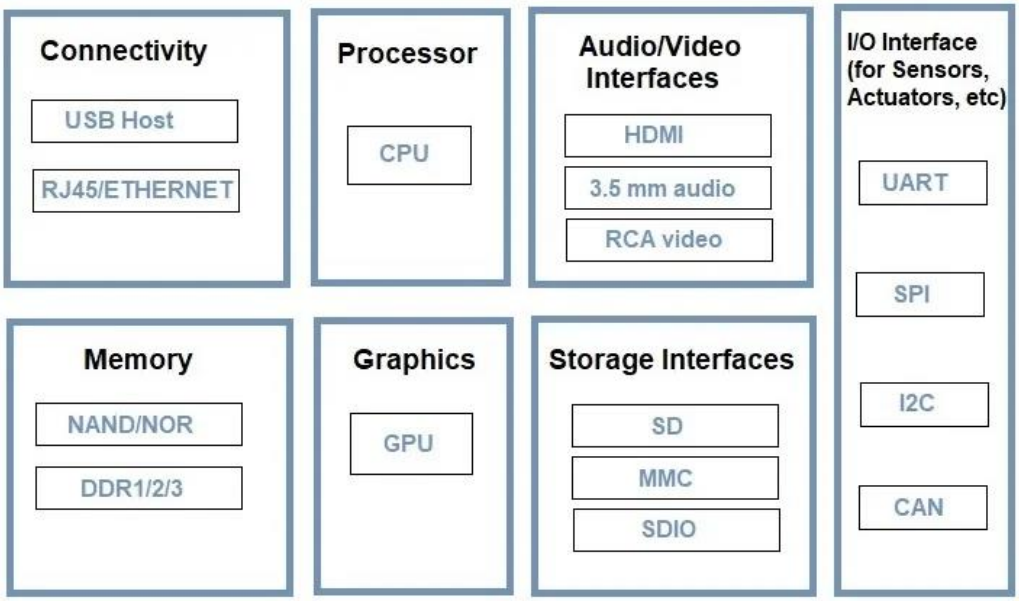
The "Things" in IoT usually refers to IoT devices, which have unique identities and can perform remote Sensing, actuating and monitoring capabilities.

IoT devices can:

- Exchange data with other connected devices and applications (directly or indirectly), or
- Collect data from other devices and process the data locally or
- Send the data to centralized servers or cloud-based application back-ends for processing the data,
- Perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints

Generic block diagram of an IoT Device

- An IoT device may consist of several interfaces for connections to other devices, both wired and wireless.
- I/O interfaces for sensors
- Interfaces for Internet connectivity
- Memory and storage interfaces
- Audio/video interfaces.



Generic Block Diagram of IoT Devices

Above picture, shows a generic block diagram of IoT device. It may consist of several interfaces for connections to other devices. IoT Device has I/O interface for Sensors, Similarly for Internet connectivity, Storage and Audio/Video. IoT Device collect data from on-board or attached Sensors

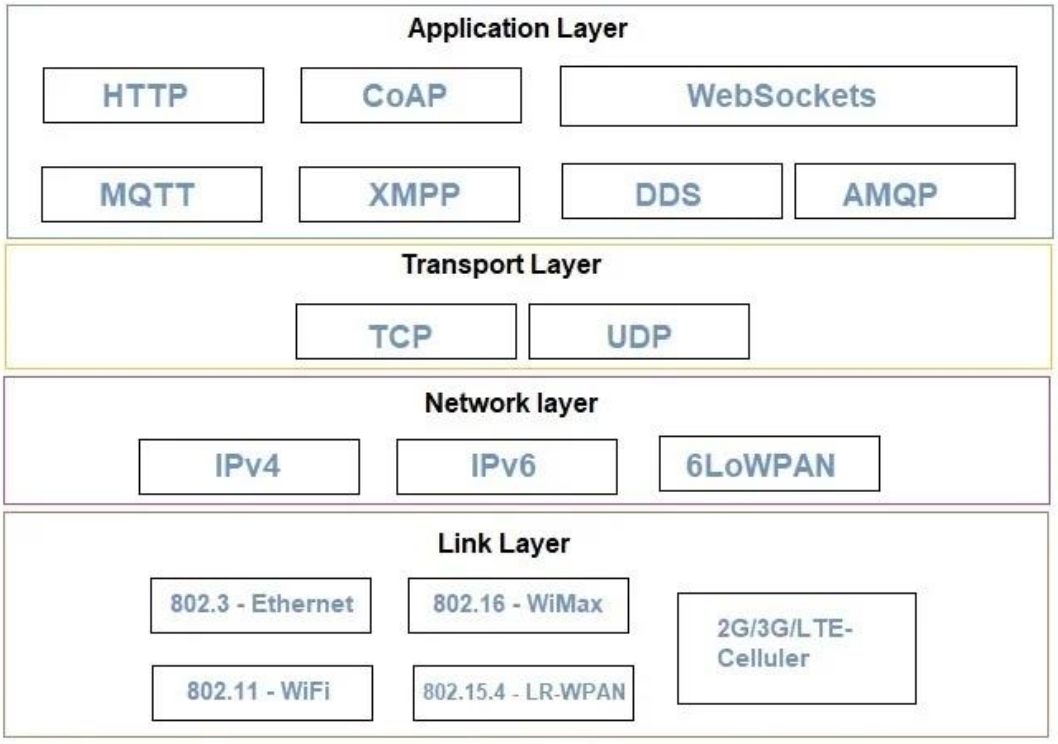
and Sensed data communicated either to other device or Cloud based sever. Today many cloud servers available for especially IoT System. These Platfrom known as IoT Platform. Actually these cloud especially design for IoT purpose. So here we can analysis and processed data easily.

How it works ? For example if relay switch connected to an IoT device can turn On/Off an appliance on the commands sent to the IoT device over the Internet.

- HDMI: High definition multimedia Interface.
- 3.5mm: Audio Jack which headphone adapter.
- RCA: Radio corporation of America.
- UART: Universal Asynchronous Receiver Transmitter.
- SPI: Serial Peripheral Interface.
- I2C: Inter integrated circuit
- CAN: Controller Area Network used for Micro-controllers and devices to communicate.
- SD: Secure digital (memory card)
- MMC: multimedia card
- SDIO: Secure digital Input Output
- GPU: Graphics processing unit.
- DDR: Double data rate

TOPIC: 4 IoT Protocols

IoT protcols help to establish Communication between IoT Device (Node Device) and Cloud based Server over the Internet. It help to sent commands to IoT Device and received data from an IoT device over the Internet.



a) Link Layer:

Protocols determine how data is physically sent over the network's physical layer or medium. Local network connect to which host is attached. Hosts on the same link exchange data packets over the link layer using link layer protocols. Link layer determines how packets are coded and signalled by the h/w device over the medium to which the host is attached.

Protocols:

- 802.3-Ethernet: IEEE802.3 is collection of wired Ethernet standards for the link layer. E.g: 802.3 uses coaxial cable; 802.3i uses copper twisted pair connection; 802.3j uses fiber optic connection; 802.3ae uses Ethernet over fiber.
- 802.11-WiFi: IEEE802.11 is a collection of wireless LAN (WLAN) communication standards including extensive description of link layer. Eg: 802.11a operates in 5GHz band, 802.11b and 802.11g operates in
- 2.4GHz band, 802.11n operates in 2.4/5GHz band, 802.11ac operates in 5GHz band, 802.11ad operates in 60Ghzband.
- 802.16 - WiMax: IEEE802.16 is a collection of wireless broadband standards including exclusive description of link layer. WiMax provide data rates from 1.5 Mb/s to 1Gb/s.
- 802.15.4-LR-WPAN: IEEE802.15.4 is a collection of standards for low rate wireless personal area network(LR-WPAN). Basis for high level communication protocols such as ZigBee. Provides data rate from 40kb/s to250kb/s.
- 2G/3G/4G-Mobile Communication: Data rates from 9.6kb/s(2G) to up to100Mb/s(4G).

b) Network/Internet Layer:

Responsible for sending IP datagrams from source n/w to destination n/w. Performs the host addressing and packet routing. Datagrams contains source and destination address.

Protocols:

- IPv4: Internet Protocol version4 is used to identify the devices on a n/w using a hierarchical addressing scheme. 32 bit address. Allows total of 2*32addresses.
- IPv6: Internet Protocol version6 uses 128 bit address scheme and allows 2*128 addresses.
- 6LOWPAN:(IPv6 over Low power Wireless Personal Area Network) operates in 2.4 GHz frequency range and data transfer 250 kb/s.

c) Transport Layer:

Set up on connection with ACK as in TCP and without ACK as in UDP. Provides functions such as error control, segmentation, flow control and congestion control.

Protocols:

TCP: Transmission Control Protocol used by web browsers (along with HTTP and HTTPS), email (along with SMTP, FTP). Connection oriented and stateless protocol. IP Protocol deals with sending packets, TCP ensures reliable transmission of protocols in order. Avoids n/w congestion and congestion collapse.

UDP: User Datagram Protocol is connectionless protocol. Useful in time sensitive applications, very small data units to exchange. Transaction oriented and stateless protocol. Does not provide guaranteed delivery.

d) Application Layer:

Defines how the applications interface with lower layer protocols to send data over the n/w. Enables Process-to-process communication using ports.

Protocols:

HTTP: Hyper Text Transfer Protocol that forms foundation of WWW. Follow request response model Stateless protocol.

CoAP: Constrained Application Protocol for machine-to-machine (M2M) applications with constrained devices, constrained environment and constrained n/w. Uses client-server architecture.

Web Socket: allows full duplex communication over a single socket connection.

MQTT: Message Queue Telemetry Transport is lightweight messaging protocol based on publish subscribe model. Uses client server architecture. Well suited for constrained environment.

XMPP: Extensible Message and Presence Protocol for real time communication and streaming XML data between network entities. Support client-server and server-server communication.

DDS: Data Distribution Service is data centric middleware standards for device-to-device or machine-to-machine communication. Uses publish-subscribe model.

AMQP: Advanced Message Queuing Protocol is open application layer protocol for business messaging. Supports both point-to-point and publish-subscribe model.

Example: Smart Home Thermostat
Scenario: Imagine a smart thermostat installed in a home. Its job is to monitor the room temperature and adjust heating or cooling based on user preferences.

How Communication Happens?

Step	Description	Protocols Involved
1. Data Collection	The thermostat senses the room temperature.	—
2. Data Transmission to Cloud	It sends temperature data to a cloud server for analysis.	**MQTT** or **CoAP** over **UDP**
3. Cloud Processing	The cloud server checks if the temperature is within the desired range.	—

Step	Description	Protocols Involved
4. Command Sent to Device	If adjustment is needed, the cloud sends a command back to the thermostat (e.g., "Turn on heater").	**MQTT** or **HTTP** over **TCP**
5. Action Taken	The thermostat receives the command and activates the heater.	—

Why Protocols Matter?

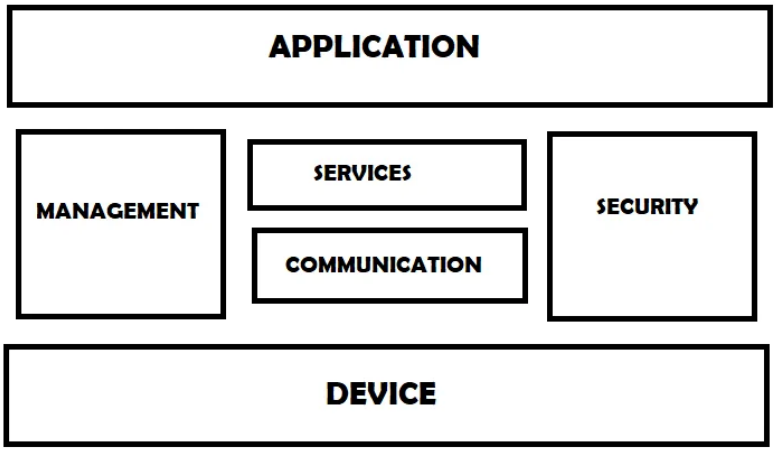
- **MQTT** is lightweight and ideal for devices with limited power and bandwidth.
- **TCP/UDP** ensures reliable or fast transmission depending on the need.
- **IPv6/6LoWPAN** helps devices communicate efficiently over constrained networks.

LOGICAL DESIGN of IoT

Refers to an abstract represent of entities and processes without going into the low level specifies of Implementation.

1) IoT Functional Blocks
2) IoT Communication Models
3) IoT Comm. APIs

Topic5-Functional Blocks of IoT



An IoT system comprises of a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication and management.

Functional blocks are:

1. **Device:** An IoT system comprises of devices that provide sensing, actuation, and monitoring and control functions.
2. **Communication:** Handles the communication for the IoT system.

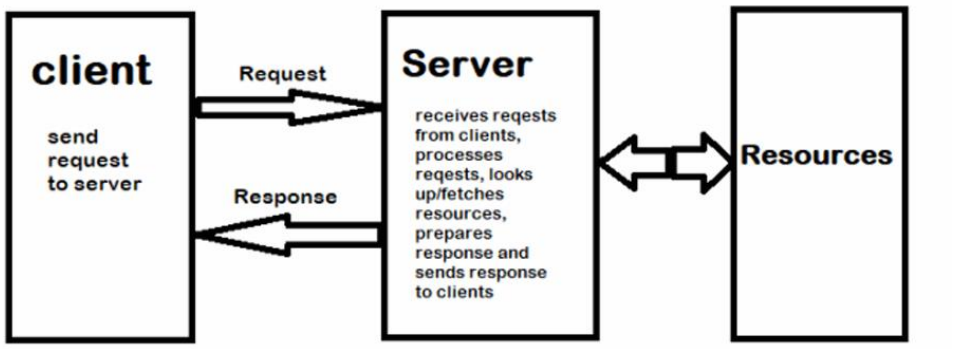
3. **Services:** services for device monitoring, device control service, data publishing services and services for device discovery.
4. **Management:** This block provides various functions to govern the IoT system.
5. **Security:** this block secures the IoT system and by providing functions such as authentication, authorization, message and content integrity, and data security.
6. **Application:** This is an interface that the users can use to control and monitor various aspects of the IoT system. Application also allow users to view the system status and view or analyze the processed data.

IoT Communication Models:

A) Request-Response
B) Publish-Subscribe
C) Push-Pull
D) Exclusive Pair

A) Request-Response

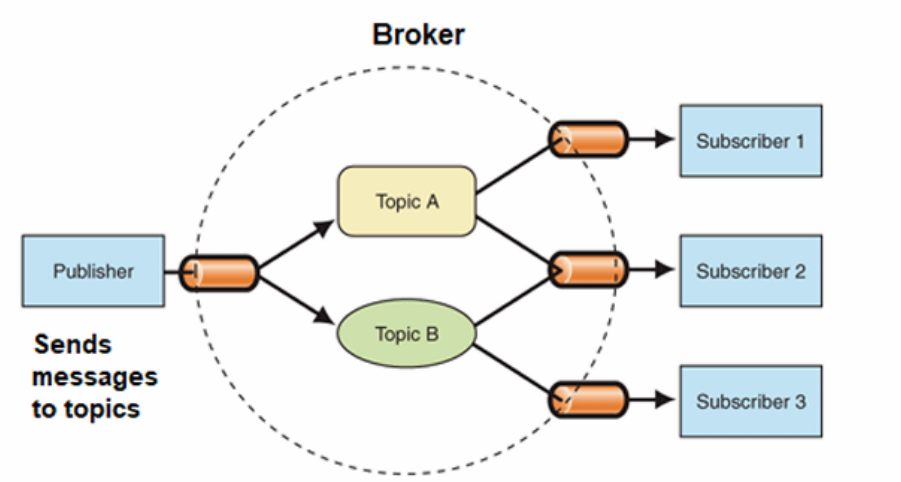
Request-Response is a communication model in which the client sends requests to the server and the server responds to the requests. When the server receives a request, it decides how to respond, fetches the data, retrieves resource representations, prepares the response, and then sends the response to the client.



Request-Response Communication Model

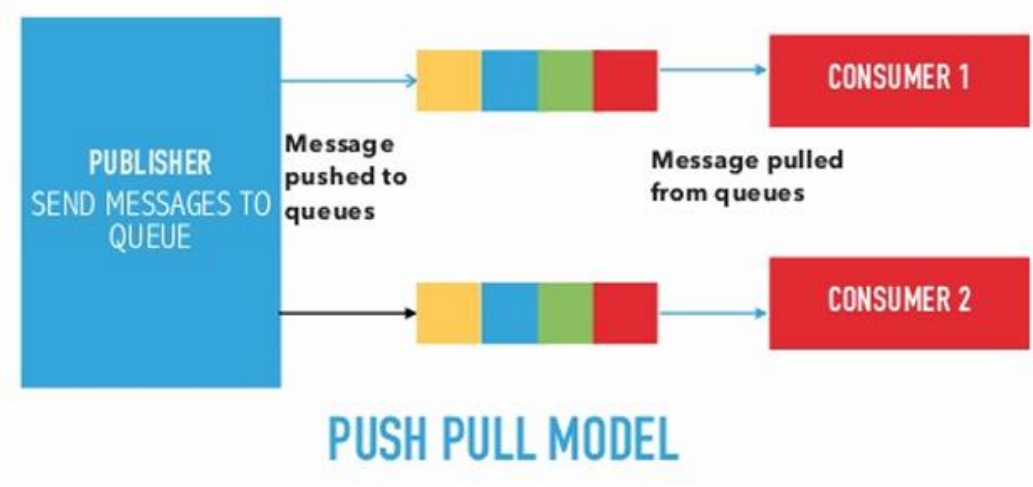
B) Publish-Subscribe communication model:

a. Publish-Subscribe is a communication model that involves publishers, brokers and consumers.
b. Publishers are the source of data. Publishers send the data to the topics, which are managed by the broker. Publishers are not aware of the consumers.
c. Consumers subscribe to the topics that are managed by the broker.
d. When the broker receives data for a topic from the publisher, it sends the data to all the subscribed consumers



C) Push-Pull communication model:

a. Push-Pull is a communication model in which the data producers push the data to queues and the consumers pull the data from the queues. Producers do not need to be aware of the consumers.
b. Queues help in decoupling the messaging between the producers and consumers.
c. Queues also act as a buffer, which helps in situations when there is a mismatch between the rate at which the producers push data and the rate at which the consumers pull.



D) Exclusive Pair communication model:

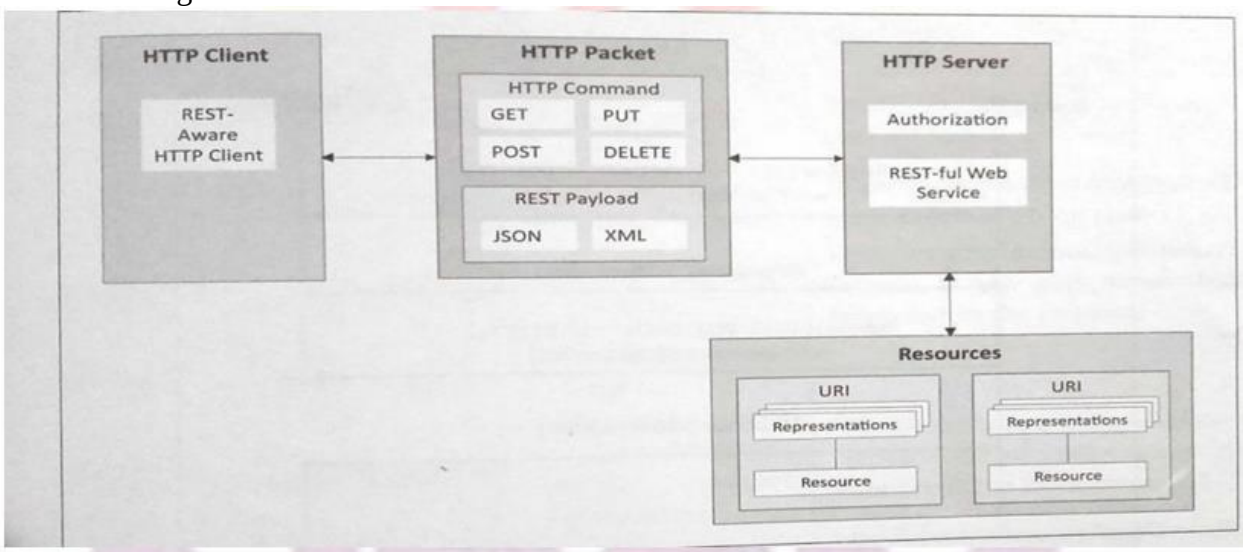
a. Exclusive Pair is a bidirectional, duplex communication model that uses a persistent connection between the client and server.
b. Once the connection is setup it remains open until the client sends a request to close the connection.
c. Client and server can send messages to each other after connection setup.

3)IoT Communication APIs:

a) REST based communication APIs(Request-Response Based Model)

b) WebSocket based Communication APIs(Exclusive PairBasedModel)

a) REST based communication APIs: Representational State Transfer(REST) is a set of architectural principles by which we can design web services and web APIs that focus on a system's resources and have resource states are addressed and transferred.The REST architectural constraints: Fig. shows communication between client server with REST APIs.



Client-Server:

The principle behind client-server constraint is the separation of concerns. Separation allows client and server to be independently developed and updated.

Stateless:

Each request from client to server must contain all the info. Necessary to understand the request, and cannot take advantage of any stored context on the server.

Cache-able:
Cache constraint requires that the data within a response to a request be implicitly or explicitly labeled as cache-able or non-cacheable. If a response is cache-able, then a client cache is given the right to reuse that response data for later, equivalent requests.

Layered System:
constraints the behavior of components such that each component cannot see beyond the immediate layer with which they are interacting.

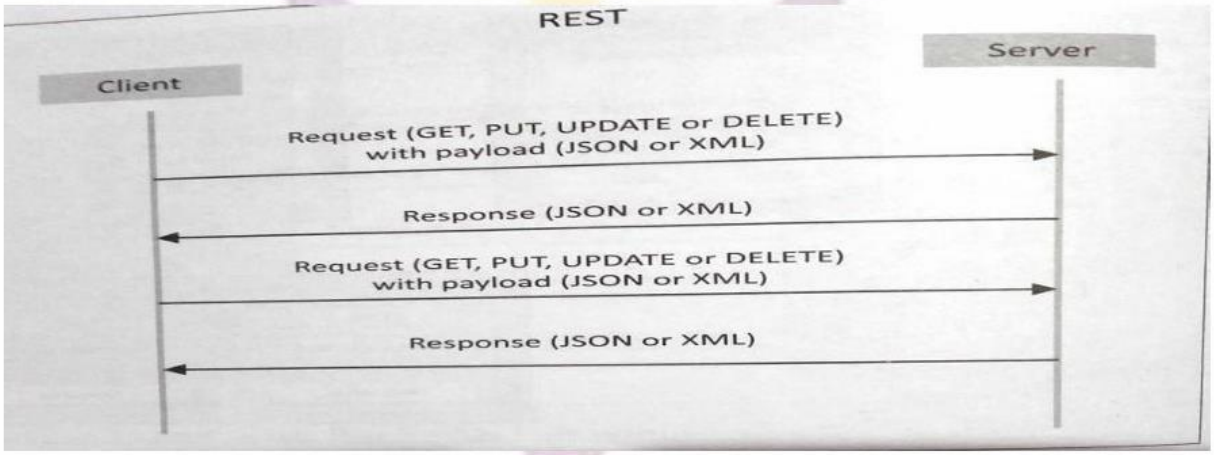
User Interface:
constraint requires that the method of communication between a client and a server must be uniform.

Code on Demand:
Servers can provide executable code or scripts for clients to execute in their context. This constraint is the only one that is optional.

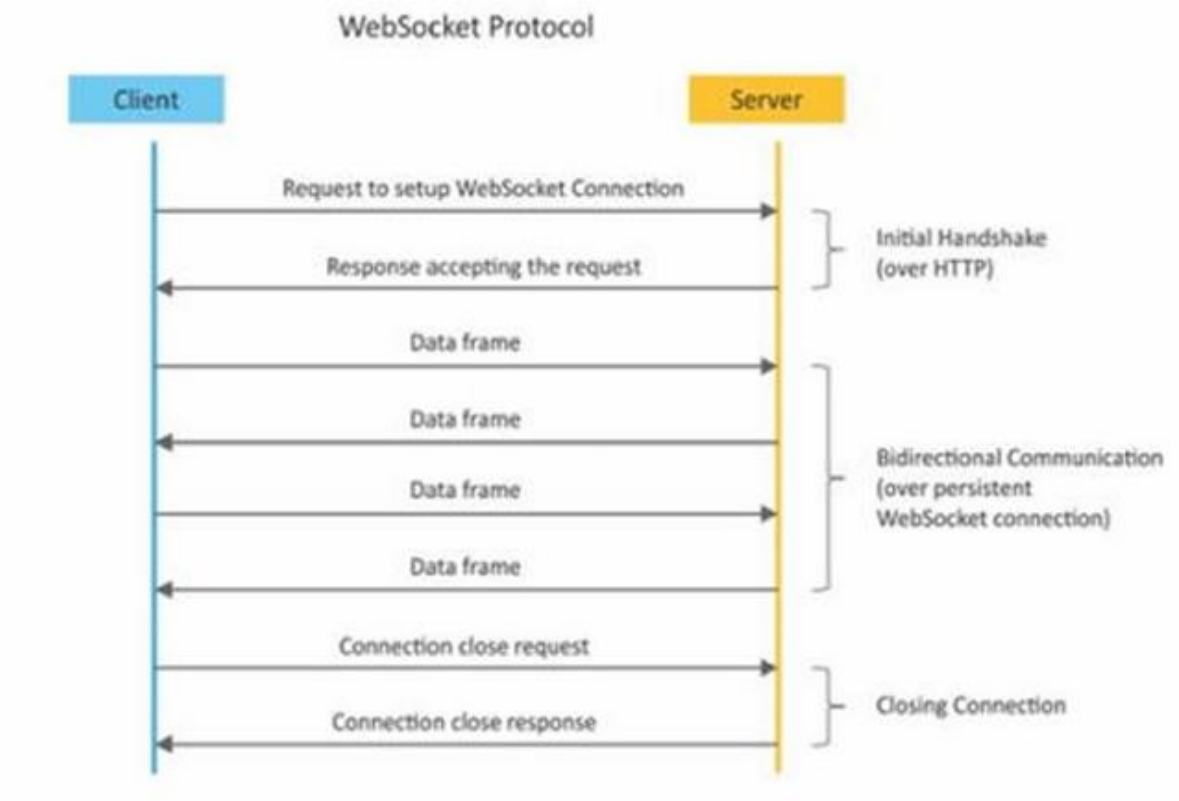
Request-Response model used by REST:

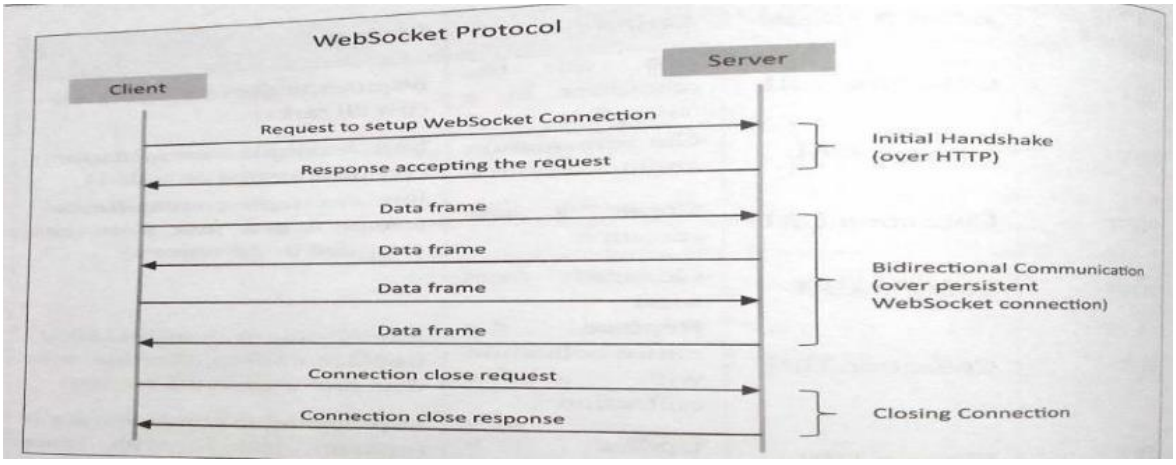
RESTful webservice is a collection of resources, which are represented by URIs. RESTful web API has a base URI (e.g: http://example.com/api/tasks/). The clients and requests to these URIs using the methods defined by the HTTP protocol (e.g: GET, PUT, POST or DELETE). A RESTful web service can support various internet media types.

Request-Response model used by REST:



b) Web Socket Based Communication APIs: Web Socket APIs allow bi-directional, full duplex communication between clients and servers. Web Socket APIs follow the exclusive pair communication model.





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.

TOPIC-6: Sensing, Actuation

What is sensing?
Sensing is the process of detecting and measuring physical, chemical, or biological properties from the environment and converting them into a signal that can be interpreted by a human or a machine.
In engineering and technology, sensing is performed by sensors, which act as the "eyes and ears" for electronic systems.

In the context of the Internet of Things (IoT), **sensing** is the first and most critical stage of the process. It is the act of a device "feeling" or "detecting" changes in its physical environment and converting that physical information into a digital signal that a computer can understand.

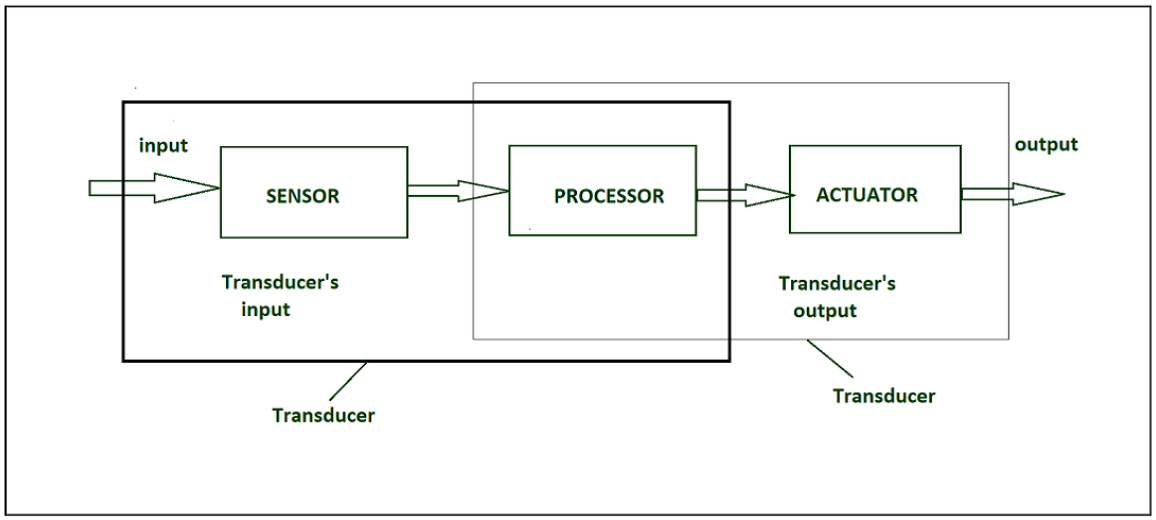
Think of sensors as the **"sensory organs"** (eyes, ears, skin) of a digital system.

How Sensing Works

The process typically follows these three steps:

1. **Detection:** A sensor encounters a physical phenomenon (like heat, light, or pressure).
2. **Transduction:** The sensor converts that physical energy into an electrical signal (voltage or current).
3. **Digitization:** The electrical signal is converted into a digital format (binary code) so the IoT system can process it.

Sensors are the devices that can detect and response to changes in the environment. These changes can be in form of light, temperature, motion, moisture or any other physical property. The sensor converts these physical changes into signal that can be measured. Sensors play an important role in IoT which will make an ecosystem for collecting, analyzing, and processing data about a specific environment so that it can be monitored, managed, and controlled more easily and efficiently. Sensors bridge the gap between the physical world and the logical world.



Transducer: It converts the signal from one physical form to another physical form. It is also called energy converter. For example, microphone converts sound to electrical signal. It is based on the principle of conservation of energy.

Classification of Sensors

Based on Power Requirement

1. Active Sensors: These sensors can *generate their own electrical signal* in response to physical changes and do not require external excitation power

Examples of Active Sensors:

1. Radar sensors: Emit radio waves and measure reflections to detect distance, speed, and movement (used in aircraft navigation, weather monitoring, and speed guns).
2. LiDAR sensors: Emit laser beams to create 3D maps of surroundings (used in autonomous vehicles, drones, and topographic mapping).
3. Sonar sensors: Emit sound waves underwater to detect objects or measure depth (used in submarines and fish finders).
4. Ultrasonic sensors: Emit high-frequency sound waves to measure distance (used in parking sensors, robotics, and industrial automation).
5. Infrared active sensors: Emit infrared light to detect motion or proximity (used in TV remotes, automatic doors, and security systems).
6. Laser rangefinders: Emit laser pulses to measure precise distances (used in surveying, construction, and sports like golf).

Real-Life Example: Think of a **car's reverse parking sensor**

- The sensor emits ultrasonic waves.
- These waves bounce back when they hit an obstacle.
- The sensor calculates the distance and alerts the driver with beeps.

That is an **active sensor in action**—it sends out energy and listens for the response.

2. Passive Sensors: These sensors *require an external power source (excitation)* and modify that signal according to the physical quantity being measured.

Examples of Passive Sensors:

1. **Thermocouples / Temperature sensors**: Detect heat or temperature changes without emitting energy.
2. **Photodiodes / Light sensors**: Measure ambient light levels (used in automatic street lights or smartphones adjusting screen brightness).
3. **Infrared sensors (passive IR)**: Detect infrared radiation naturally emitted by objects (used in motion detectors for security systems).
4. **Cameras**: Capture visible light reflected from objects (used in surveillance, photography, and machine vision).
5. **Seismometers**: Detect vibrations or seismic waves from earthquakes.
6. **Microphones**: Pick up sound waves from the environment without generating signals themselves.
7. **Radiometers**: Measure natural electromagnetic radiation (used in satellites for weather and climate monitoring).

Real-Life Example:

Think of an **automatic street light**:

- It has a light sensor (photodiode).
- When sunlight decreases in the evening, the sensor detects low ambient light.
- The system turns the streetlight ON.
- The sensor emits no energy—it only *receives* natural light.

Active vs Passive Sensors:

Feature	Active Sensor	Passive Sensor
Energy emission	Emits energy (sound, light, radio waves)	Does not emit energy
Examples	Radar, LiDAR, Sonar, Ultrasonic	Thermocouple, Camera, Microphone, PIR sensor
Use case	Detecting distance, mapping, obstacle detection	Monitoring natural signals like heat, light, sound

Based on the Conversion Phenomenon

This classification is based on the input and output conversion

- **Photoelectric**: It Changes light to electrical signals.
- **Thermoelectric:** It Changes temperature difference to electrical voltage.
- **Electrochemical**: It Changes chemical reactions to electrical signals.
- **Electromagnetic**: It Changes magnetic fields to electrical signals.
- **Thermoptic**: It Changes temperature changes to electrical signals.

Based on Output Type

1. Analog Sensors: It produce an output signal which is usually in the form of voltage, current, or resistance, proportional to the measured quantity.

Examples of Analog Sensors:

1. **Temperature sensors (Thermistor, RTD, Thermocouple)** Output changes continuously with temperature.
2. **Light sensors (Photoresistor / LDR)** Resistance varies with the intensity of light.
3. **Pressure sensors** Voltage output changes with applied pressure (used in weather stations, industrial machines).
4. **Sound sensors (Microphones)** Convert sound waves into continuous electrical signals.
5. **Gas sensors (MQ series)** Detect concentration of gases like CO_2, methane, or smoke with analog voltage output.
6. **Humidity sensors** Provide continuous voltage based on moisture levels in the air.
7. **Force sensors (Force-sensitive resistors)** Resistance changes with applied force or weight.

Real-Life Example:

Think of a **room thermometer**:

- As the temperature rises, the sensor's voltage output increases smoothly.
- As the temperature falls, the voltage decreases.
- This continuous change is what makes it an **analog sensor**.

2. Digital Sensors: It provide discrete or digital data as output.

Examples of Digital Sensors:

1. **PIR (Passive Infrared) Motion Sensor** Detects movement by sensing infrared radiation changes. Output: HIGH (1) when motion is detected, LOW (0) otherwise.
2. **Digital Temperature Sensor (DHT11, DS18B20)** Provides temperature and humidity readings directly in digital form.
3. **Proximity Sensor (IR or Ultrasonic with digital output)** Detects presence of an object and gives a binary signal (object present or not).
4. **Digital Accelerometer (ADXL345)** Measures acceleration and outputs digital data via I^2C/SPI communication.
5. **Magnetic Sensor (Hall Effect with digital output)** Detects magnetic fields and outputs ON/OFF signals (used in door sensors).

6. **Digital Light Sensor (BH1750)** Measures light intensity and sends digital values over I²C.
7. **Fingerprint Sensor** Captures and processes fingerprint data digitally for authentication systems.

Real-Life Example:

Think of a **motion sensor light**:

- The PIR sensor detects movement.
- If motion is detected, it sends a digital signal (1) to the controller.
- The controller turns the light ON.
- When no motion is detected, the signal is 0, and the light stays OFF.

That's a **digital sensor**—clear ON/OFF signals instead of continuous values.

Analog vs Digital Sensors:

Feature	Analog Sensor	Digital Sensor
Output	Continuous signal (voltage/current)	Discrete values (0/1 or digital data)
Examples	Thermistor, LDR, Microphone	PIR sensor, DHT11, Hall Effect sensor
Use case	Precise measurement of varying quantities	Simple detection or direct digital communication

Common Types of Sensing

Depending on what needs to be measured, different sensors are used:

Sensor Type	What it "Senses"	Real-World Example
Temperature	Heat levels/energy	Smart thermostats or medical monitors.
Proximity	Presence of a nearby object	Phones turning off the screen when held to your ear.
Motion (PIR)	Physical movement	Security cameras or automatic lights.
Humidity	Moisture in the air	Smart irrigation systems for farming.
Image	Light/Visual data	Facial recognition doorbells.

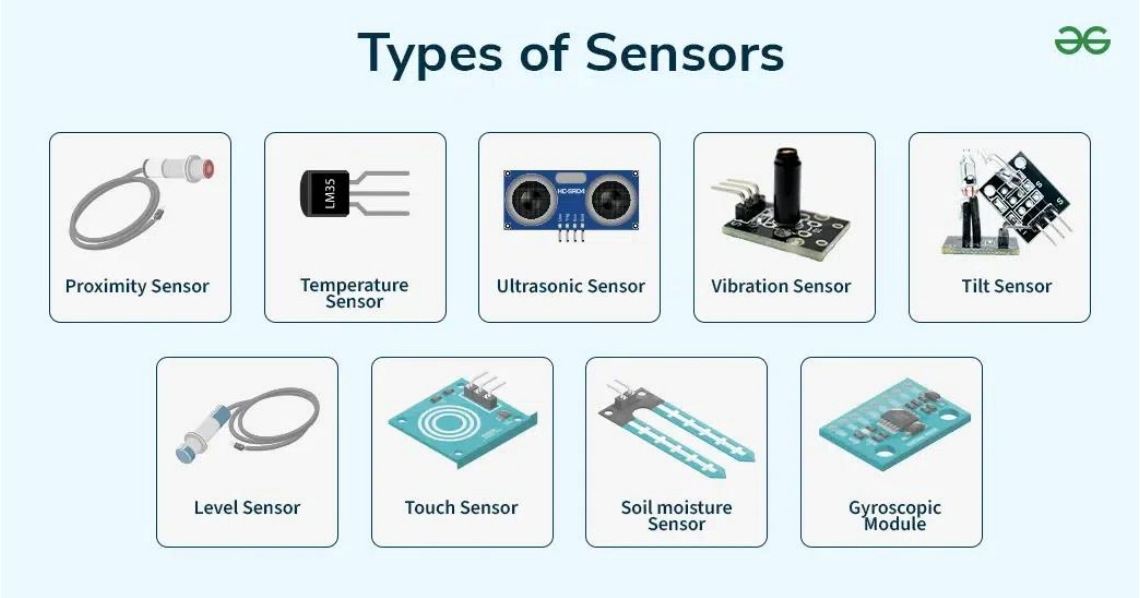
Sensor Type	What it "Senses"	Real-World Example
Acoustic[5]	Sound waves/vibrations[6]	Voice-controlled assistants (Alexa, Google Home).[7]

Types of Sensors

1. **Temperature sensors:** Monitoring temperature of used devices in industrial applications. it is used to measure temperature. this can be air temperature, liquid temperature or the temperature of solid. It can be analog or digital. In an **Analog Temperature Sensor**, the change in the Temperature correspond to change in its physical property like resistance or voltage. LM35 is a classic Analog Temperature Sensor. In **Digital Temperature Sensor**, the output is a discrete digital value, DS1621 is digital sensor which generates 9 bits temperature data.
2. **Accelerometer sensors:** It measures the rate of change of velocity and this sensor generate magnitude and acceleration of the acceleration. Accelerometer sensor sensor ADXL335 provides 3 axes (X,Y, and Z) values in analog voltage. it is used in car electronics, ships, and agricultural machines.
3. **Alcohol sensors:** as the name suggests it detects alcohol. Usually, alcohol sensors are used in breathalyzer devices, which determine whether the person is drunk or not. Law enforcement personnel uses breathalyzers to catch drunk-and-drive culprits.
4. **Radiation sensors:** Radiation Sensors/Detectors are electronic devices that sense the presence of alpha, beta, or gamma particles and provide signals to counters and display devices. Radiation detectors are used for surveys and sample counting.
5. **Position sensors:** Position Sensors are electronic devices used to sense the positions of valves, doors, throttles, etc. and supply signals to the inputs of control or display devices. Key specifications include sensor type, sensor function, measurement range, and features that are specific to the sensor type. Position sensors are used wherever positional information is needed in a myriad of control applications. A common position transducer is a so-called string-pot, or string potentiometer.
6. **Gas sensors:** It measures and detects concentration of different gases which is present in the atmosphere or any other environment.
7. **Torque sensors:** This sensor is used for measuring the rotating torque and it is used to measure the speed of the rotation.
8. **Optical sensors:** it is also called photosensors which can detect light waves at different points in the light spectrum including ultraviolet light, visible light, and infrared light. it is extensively used in smartphone, robotics and Blu-ray players.
9. **Proximity sensors:** This sensor is used to detect the distance between two objects or detect the presence of an object. it is used in elevators, parking lots, automobiles, robotics, and numerous other environment.
10. **Touch sensors:** Touch sensing devices detect physical contact on a monitored surface. Touch sensors are used extensively in electronic devices to support trackpad

and touchscreen technologies. They're also used in many other systems, such as elevators, robotics and soap dispensers.

11. **Image sensor:** it is used for distance measurement, pattern matching, color checking, structured lighting, and motion capture and it is also used in different applications such as 3D imaging, video/broadcast, space, security, automotive, biometrics, medical, and machine vision.



Application of Types of Sensors

Given below are the Application of Types Of Sensors

1. **Automotive Industry:** They are used in the Automotive industry for monitoring engine temperature, speed and other parameters.
2. **Smart Homes**: They are used in the Smart Homes for detecting movements, Control HVAC and other measurements.
3. **Robotics:** They are used in the Robotics for object recognition, Tracking the position and measuring force.
4. **Transportation**: Sensors such as GPS , Load, and Speed sensors are used in transportation infrastructure.

Actuation:

Actuation is the process of converting a control signal or energy (such as electricity, air pressure, or fluid pressure) into physical motion or action. In a system, if sensing acts as the "eyes and ears," actuation acts as the "muscles" that carry out commands.

In the Internet of Things (IoT), **actuation** is the final step where the digital decision is turned back into a physical action. If sensing is the "feeling," then actuation is the **"doing."**

An **actuator** is a component that receives a command from the system (the "brain") and uses energy to move or control a mechanism. It is essentially the **muscle** of the IoT system.

How Actuation Works

The process is the exact reverse of sensing:

1. **Command Received:** The central controller (cloud or local processor) sends a digital signal to the actuator.
2. **Energy Conversion:** The actuator takes energy (electricity, air pressure, or fluid) and converts it into a physical force.
3. **Physical Action:** The device performs a task, such as opening a valve, spinning a motor, or turning on a heater.

Common Types of Actuators

Actuators are classified by the type of energy they use to create motion:

Actuator Type	Power Source	Common IoT Use Case
Electrical	Electricity (Motors/Solenoids)	Opening smart locks or spinning a cooling fan.
Pneumatic	Compressed Air	Industrial robotic arms or automated factory valves.

Actuator Type	Power Source	Common IoT Use Case
Hydraulic	Pressurized Liquid	Heavy machinery like smart excavators or dump trucks.
Thermal	Heat/Temperature	Traditional radiator valves that expand to shut off flow.
Relays	Electrical Switch	Turning on a high-power appliance like a water heater.

Real-World Examples

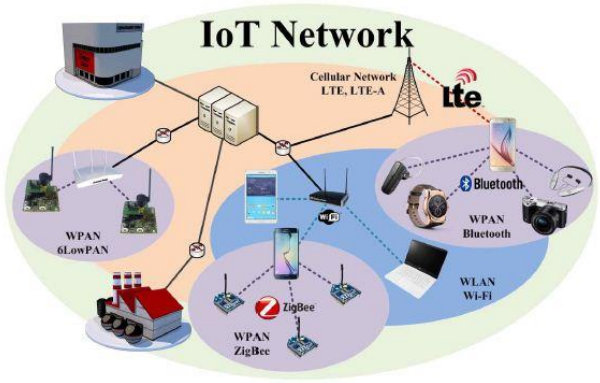
- **Smart Home:** When your smart lock receives an "unlock" command from your phone, an **electric motor** (actuator) physically slides the bolt back.
- **Smart Agriculture:** If a sensor detects dry soil, the system triggers a **solenoid valve** (actuator) to open and let water flow into the sprinklers.
- **Healthcare:** An automated insulin pump uses a **linear actuator** to push a tiny plunger and deliver a precise dose of medicine.

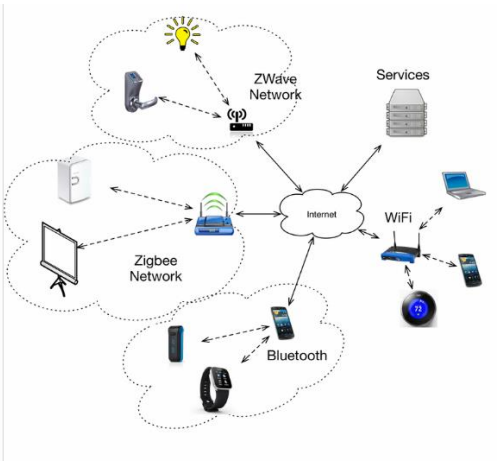
Sensors vs. Actuators

Feature	Sensor	Actuator
Role	Detector (The Eyes/Ears)	Performer (The Muscles)
Direction	Physical ⟶ Digital	Digital ⟶ Physical
Location	Input of the system	Output of the system

TOPIC-7: Basics of Networking, Communication Protocols

IoT networking connects physical devices (sensors, actuators) to exchange data for monitoring & control, using protocols like Wi-Fi, Bluetooth, Zigbee locally, then the Internet (Cloud/Edge) for processing via gateways, routers, and backend services, bridging the digital/physical worlds for automation and insights, requiring robust security.





Core Components & Flow:

1. Sensing & Data Collection: Devices (nodes) with sensors gather real-time data (temp, motion, location) from the physical world.
2. Local Communication: Data moves from sensors via short-range protocols (Zigbee, BLE, Wi-Fi) to a local hub or gateway.
3. Gateway: Manages local traffic, translates protocols, and bridges the local network to the broader Internet.
4. Internet & Cloud/Edge: Data travels over the internet to cloud or edge servers for storage, heavy processing, and analytics.
5. Backend Services & Applications: Analyzed data drives applications (dashboards, alerts) and triggers actions (actuators).

6. Actuation: Commands sent back through the network to perform physical tasks (e.g., turning off a light).

Key Protocols & Technologies:

- Short-Range: Bluetooth (BLE), Zigbee, Z-Wave (for home automation).
- Medium/Long-Range: Wi-Fi, Cellular (4G/5G), LoRaWAN, NB-IoT (for wide area/low power).
- Internet Protocols: TCP/IP, MQTT, CoAP (for efficient messaging).

Essential Infrastructure:

- Routers/Switches: Direct data packets within networks.
- Gateways: Connect different network types (e.g., Zigbee to Wi-Fi).
- Cloud/Edge Platforms: For scalable data processing (AWS IoT, Azure IoT).

Key Considerations:

- Security: Data encryption, intrusion detection, privacy are crucial due to many connected devices.
- Scalability: Handling massive numbers of devices.
- Power Efficiency: Especially for battery-powered sensors (e.g., BLE, LoRaWAN).

IoT NETWORK ARCHITECTURE:

1. Autonomous Network Architecture :

- Autonomous networks are not connected to the public networks. However, it does not mean that the Internet access is forbidden. It is possible via gateway if required.
- While designing autonomous networks, though not mandatory, IP protocol suite is still commonly adopted dueto its scalability and flexibility.
- The large address capacity provided by IPv6 is required in most cases.

Example: Autonomous information collected by the parking sensor due to the occupancy of parking slots in a wireless manner and sent to the control center.

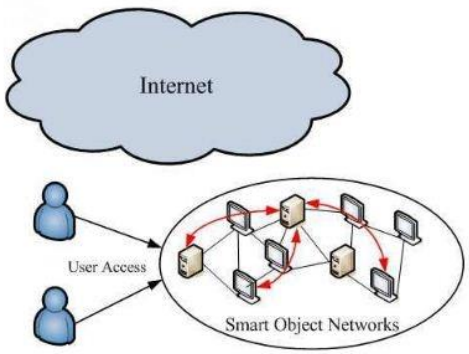


Fig: Autonomous Network Architecture

Private school campus:

- All classrooms (devices) are connected internally.
- They use a common language (IP protocols) to communicate.
- The school has its own address system (IPv6).
- If needed, they can connect to the outside world (internet) through a gate (gateway).

2.Ubiquitous Network Architecture :

- Smart objects or 'things' network are a part of the Internet.
- Through the Internet gateway, authorized users will have access to the information provided by smart objects networks either directly fetching from the device or by means of intermediate servers.
- The servers acts as a sink to collect data from each objects.

Features :

- Multitier – The network architecture is hierarchical, comprising both multi-access networks and wireless multi-hop networks.
- Multiradio – It is uncommon nowadays to have a number of radio access technologies available to connect to the Internet, either covering the same or complimenting geographical areas. These networks could be WLAN, WiMAX, macro-cellular, femto-cellular or even ad-hoc. The synergy and integration of different networks in multi-access and multi-operator environment introduces new opportunities for better communication channels and an enhanced quality of provided applications and services.

Examples: Structural Health Monitoring – monitoring the health of any structures small or big like building, bridges etc. Passive wireless sensors are embedded within a concrete structure which sends radio signals of suitable amplitude and phase characteristics periodically using radio frequencies. The data collected from these sensors are then analyzed to detect anomalies.

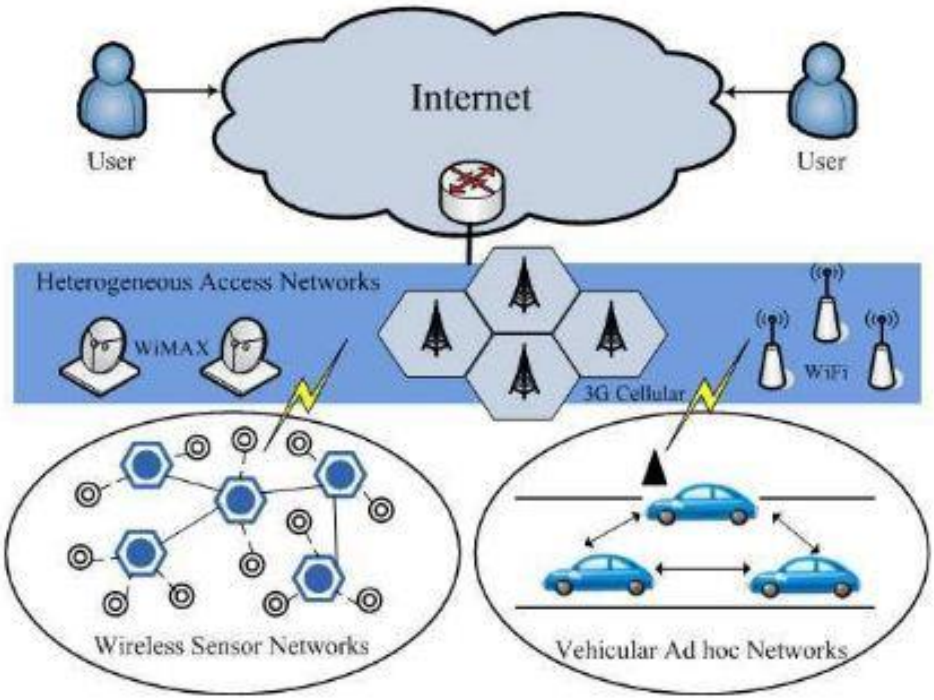


Fig: Ubiquitous Network Architecture

Types of layers of IoT architecture

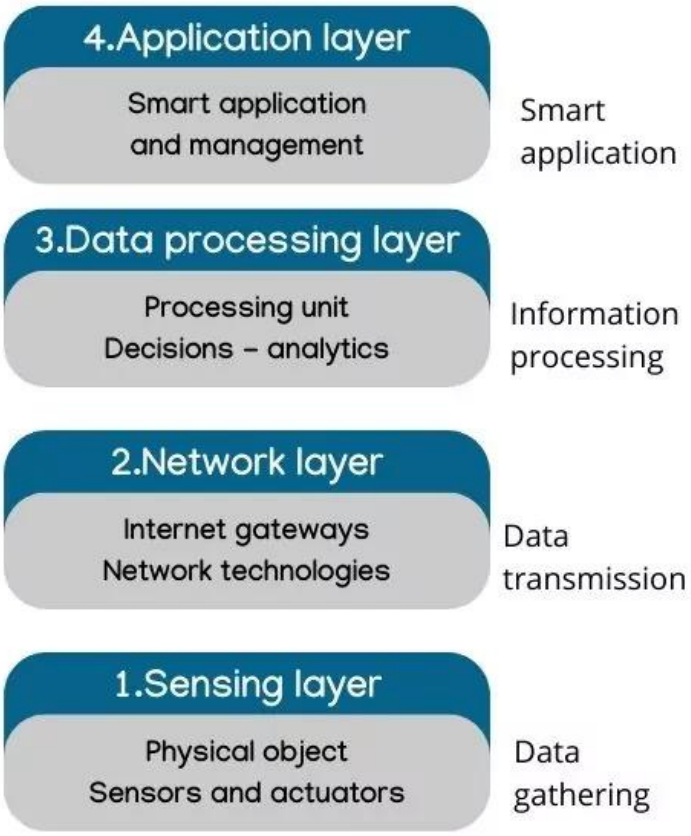


Fig: Basic layers of IoT architecture

The most common layers of Internet of Things architecture are 4, however, it doesn't mean that every IoT device has the same amount, the minimum to guarantee a stable project is four layers, but depending on the complexity, an IoT product development company can decide to add more layers to the project.

1. Sensing layer:

This layer of IoT architecture contains all the different devices and sensors that are in charge of collecting data (from surroundings or specific tasks).

2.Network layer

This layer is responsible for the data transfer between the devices and the internet, this is made usually through a gateway that is in charge of adding additional processes.

In this layer, the most important part is protocol configuration, data encryption, malware protection, and authentication.

3.Data processing layer

This IoT architecture layer is in charge of managing all data analysis, but in a previous state of processing. This layer is very useful for IoT analytics. Another important aspect to consider, the data processing layer can be located in the gateway or in the cloud.

4.Application layer

This is where the data is processed and shown to the end-user. This IoT layer is usually located in the cloud. The application displays the data, and decisions can be made according to the information provided.
For instance, a person that is using a smart home system can see in his phone the temperature levels of the house thanks to the different temperature sensors installed in each IoT device. The user really doesn't know which part of the system is performing a specific task of the IoT architecture, but all layers work together to deliver the data in such a way that it can be read and understood.

IoT NETWORK PROTOCOLS:

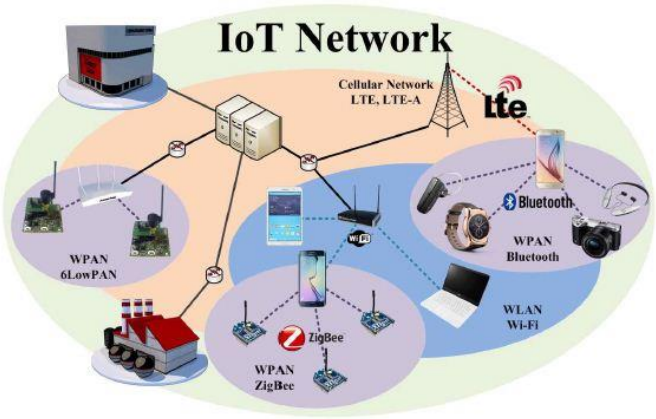


Fig: IoT Network

- WPAN (Wireless Personal Area Network) which include networks like Zigbee, Bluetooth, 6LowPAN etc.
- On a slightly larger wireless network area scale, WLAN (Wireless Local Area Network) which includes Wi-Fi is to be used.
- On a larger scale, the mobile communication technologies like 2G, 3G,4G, LTE remains. Smartphones and mobile communication system will be used and they will connect to the base stations and base stations will provide connectivity to the Wide Area Network (WAN) which is the Internet.
- Smartphones are equipped with bluetooth and wi-fi, therefore we can think of an IoT network. The most common topology control is the WPAN which is bluetooth or NFC(Near Feild Communication). The WPAN are connected to a smartphone and the smartphone can bring the signal up through 3G,4G,LTE through the base station and the base station will connect that to the WAN.

- Therefore we get a technology linking on another technology.

Wearable IoT Networks :

Wearable devices (e.g., shoes,watch, glasses, belt, etc.) can be used to detect biometric information. Smart device collects the information and communicates with control center and/or medical server through the Internet.

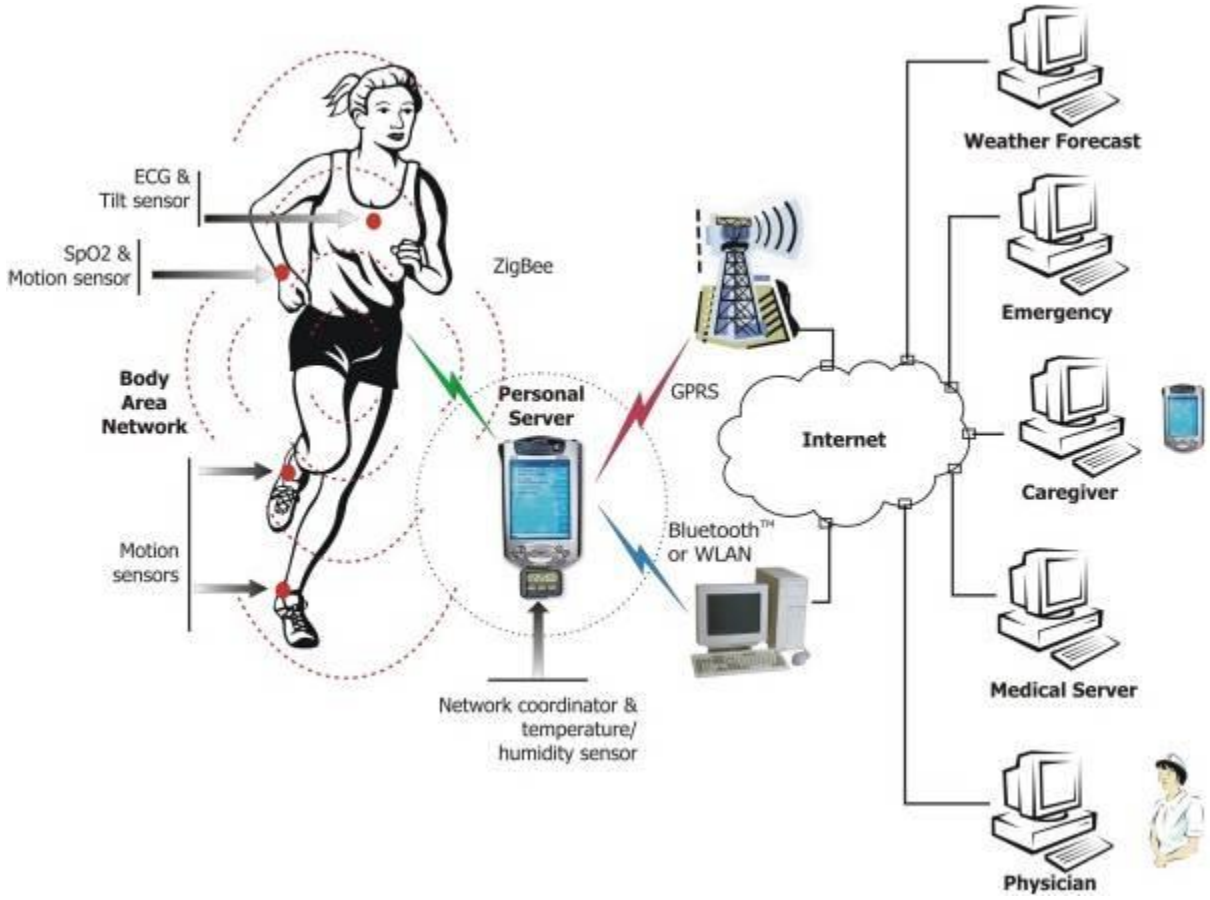


Fig: Wearable IoT Networks

Wi-Fi :

Wi-Fi is a WLAN (Wireless Local Area Network) technology based on the IEEE 802.11 standards.

Wi-Fi Devices :

Smartphones, Smart Devices, Laptop Computers, PC, etc.

Applications Areas :

Home, School, Computer Laboratory, Office Building, etc.

Wi-Fi devices and APs (Access Points) have a wireless communication range of about 30 meters indoors.

Wi-Fi data rate is based on its protocol type :

- IEEE 802.11a can achieve up to 54 Mbps
- IEEE 802.11b can achieve up to 11 Mbps
- IEEE 802.11g can achieve up to 54 Mbps
- IEEE 802.11n can achieve up to 150 Mbps
- IEEE 802.11ac can achieve up to 866.7 Mbps
- IEEE 802.11ad can achieve up to 7 Gbps

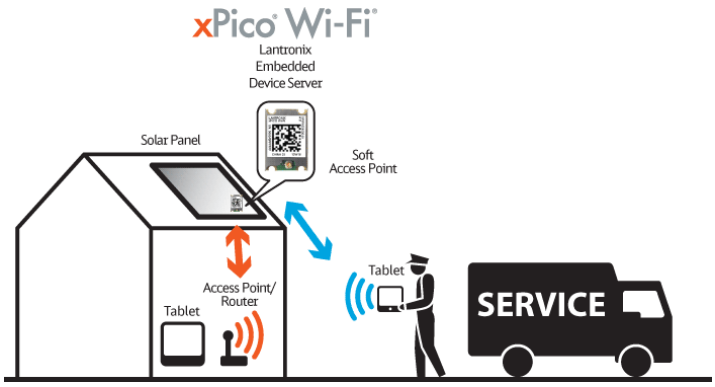


Fig: Wi-Fi IoT Networks.

Bluetooth:

- Bluetooth is a WPAN (Wireless Personal Area Network) protocol designed by the Bluetooth SIG (Special Interest Group)
- Replaces cables connecting many different types of devices
    - Mobile Phones & Headsets
    - Heart Monitors & Medical Equipment
- Bluetooth's standard PAN range is usually 10 meters (50 m in Bluetooth 4.0)
- Bluetooth Low Energy (in Bluetooth 4.0) provides reduced power consumption and cost while maintaining a similar communication range.
- Bluetooth 2.0 + EDR can achieve up to 2.1 Mbps
- Bluetooth 3.0 + HS can achieve up to 24 Mbps
- Bluetooth 4.0 can achieve up to 25 Mbps

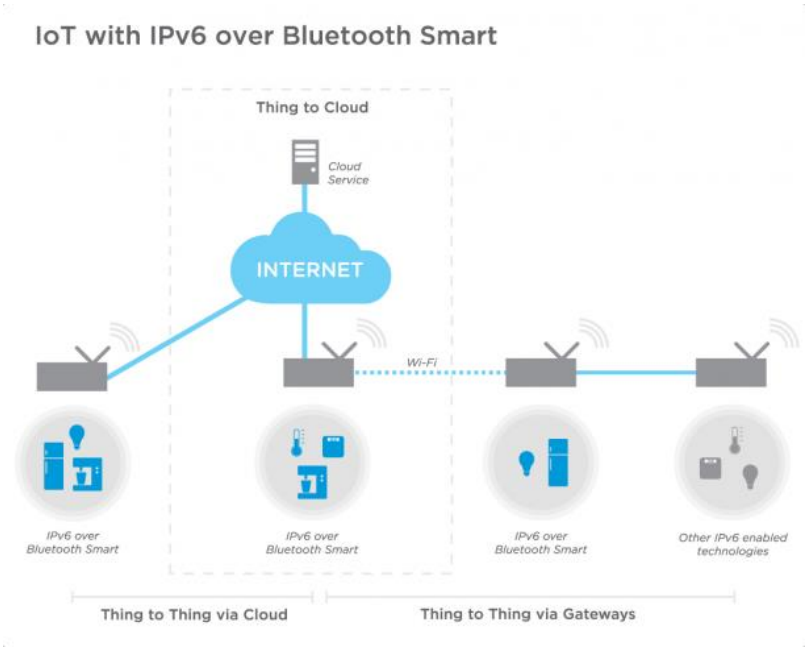


Fig: Bluetooth IoT Network

IEEE 802.15.4 Standard :

Low-cost, low-speed, low-power WPAN (Wireless Personal Area Network) protocol.

IEEE 802.15.4 applications

ZigBee, 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), WirelessHART (Highway Addressable Remote Transducer), RF4CE (Radio Frequency for Consumer Electronics), MiWi (Microchip Wireless Protocol), and ISA100.11a

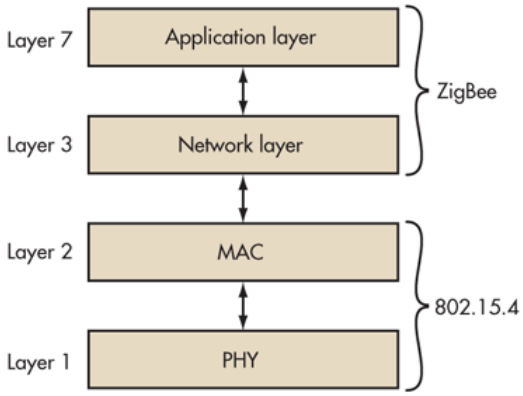


Fig: IEEE 802.15.4 and Zigbee layer in OSI Model.

ZigBee :

- Supported by the ZigBee Alliance
- Provides IEEE 802.15.4 higher layer protocols required for low powered radio system.
    - IEEE 802.15.4 defines the physical and MAC layers.
    - ZigBee provides the application and network layer protocols.
- ZigBee works well in isolated network environments.

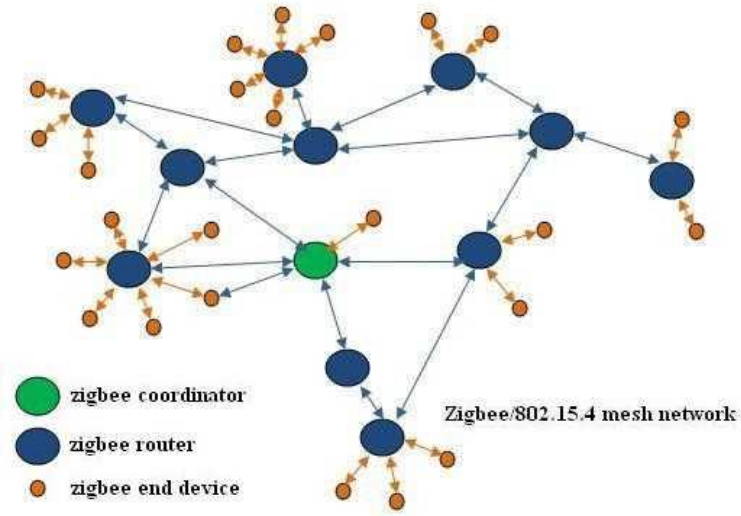


Fig: Zigbee Network

Zigbee network is made up of Coordinator (C), which is required to establish a network connection. 'C' establishes PAN, router (R) which provide the network connection to the end devices and End Device (E), which are the IoT devices connected to the network.

6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) :

- Supports IPv6 packets over IEEE 802.15.4 WPANs
- Enables IPv6 IoT wireless network support
- Low power design aspect included.
- Good for battery operated IoT devices
- 6LoWPAN is an IETF (Internet Engineering Task Force) standard that uses the IEEE 802.15.4 WPAN technology.

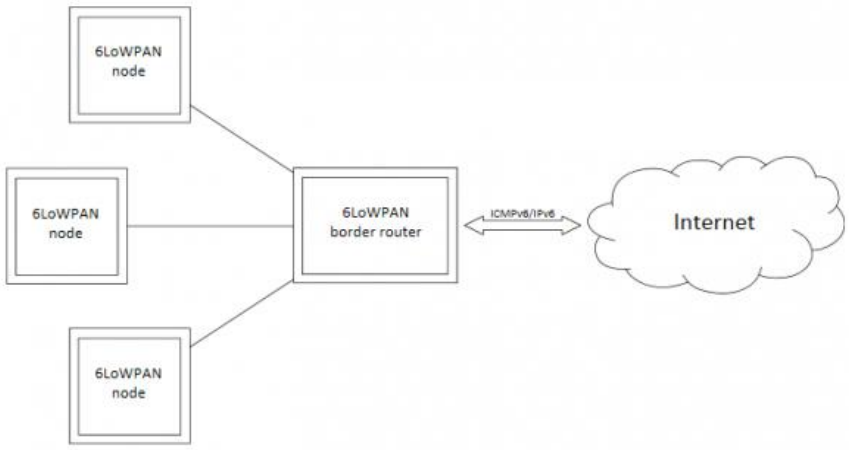


Fig: 6lowPAN

In the 6LoWPAN node, Bluetooth Smart devices can connect to the internet over Bluetooth Smart using a border router. The border router acts as a device that is connected to the internet and provides access for the nodes to the internet.

Z- Wave :

The Z-Wave protocol is an interoperable, wireless, RF-based communications technology designed specifically for control, monitoring and status reading applications in residential and light commercial environments.

- Low Powered RF communications technology that supports full mesh networks without the need for a coordinator node.
- Operates in the sub-1GHz band; impervious to interference from Wi-Fi and other wireless technologies in the 2.4-GHz range (Bluetooth, ZigBee, etc.).
- Designed specifically for control and status apps, supports data rates of up to 100kbps, with AES128 encryption, IPV6, and multi-channel operation.

Fig: Z – wave applications.

UDP :

- Data networking protocol.
- Incorporated under the architecture of TCP/IP protocol.
- UDP is robust and that is why TCP/IP has mainly standardized UDP for real-time data transfer.

Fig: IoT Network Layers of OSI model

In the diagram below, we get a clear differentiation of IP Suite and IP Smart Object (IoT) suite.

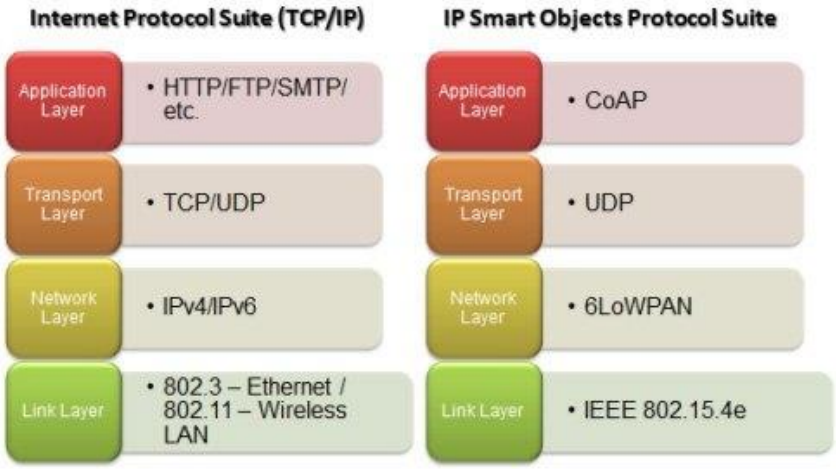
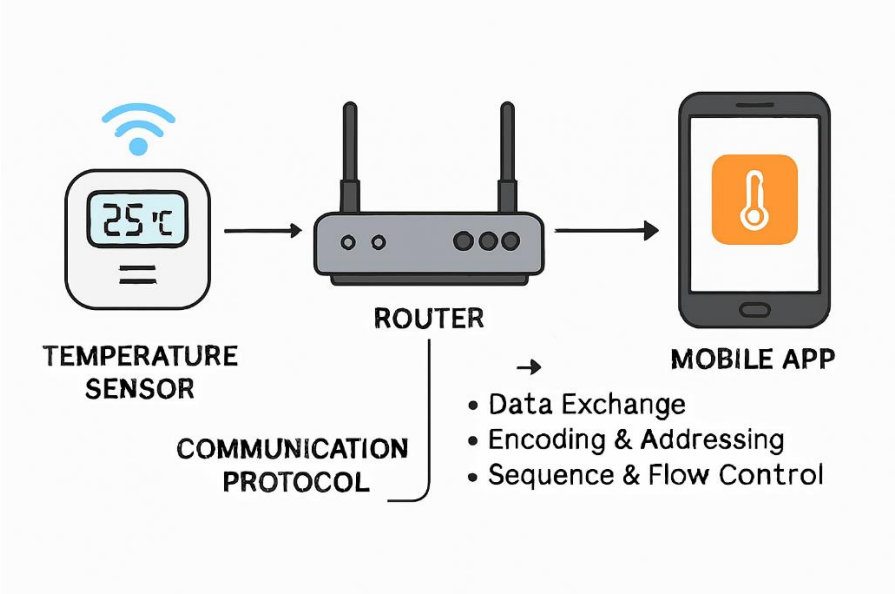


Figure : TCP/IP Stack and IP Smart Objects Protocol Stack

Communication Protocols:

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 includes sequence control, flow control and retransmission of lost packets.



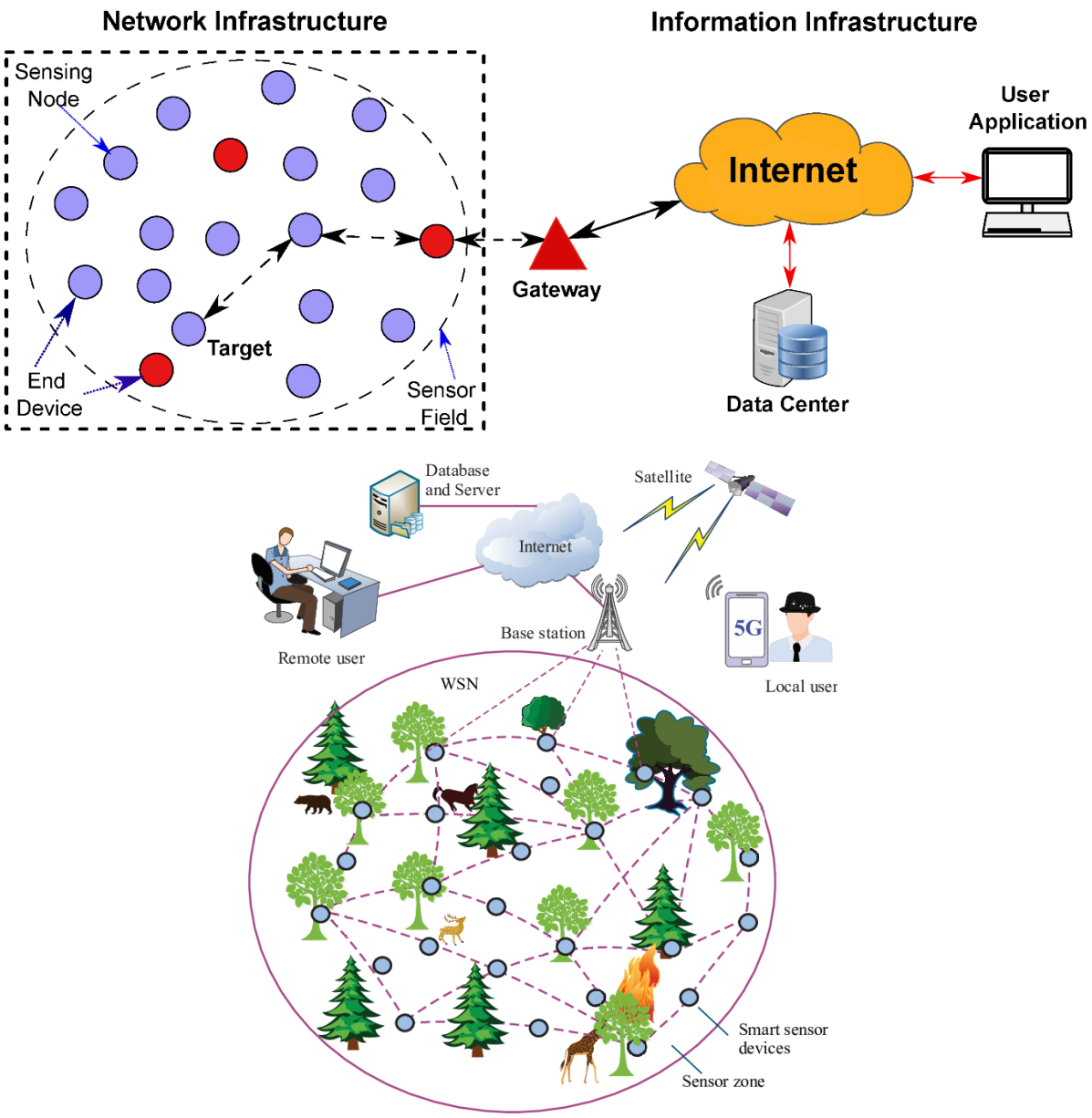
1. The **sensor** sends data packets

2. The **router** forwards them using addressing and routing.

3. The **mobile app** receives and interprets the data with sequence control, flow control, and retransmission.

TOPIC 8: Wireless Sensor Networks

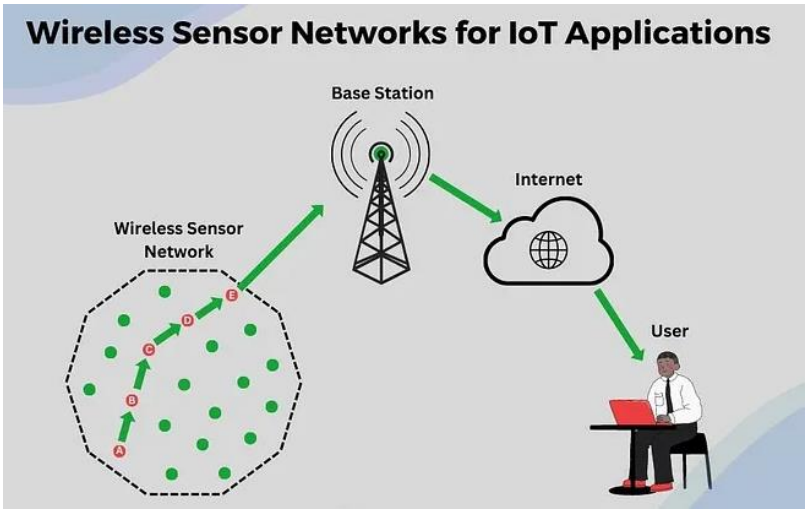
A wireless sensor network comprises of distributed devices with sensors, which are used to monitor the environmental and physical conditions. A WSN consist of a number of end nodes and routers and a coordinator. The coordinator collects the data from all the nodes. Coordinator also acts as a gateway that connects the WSN to the internet.



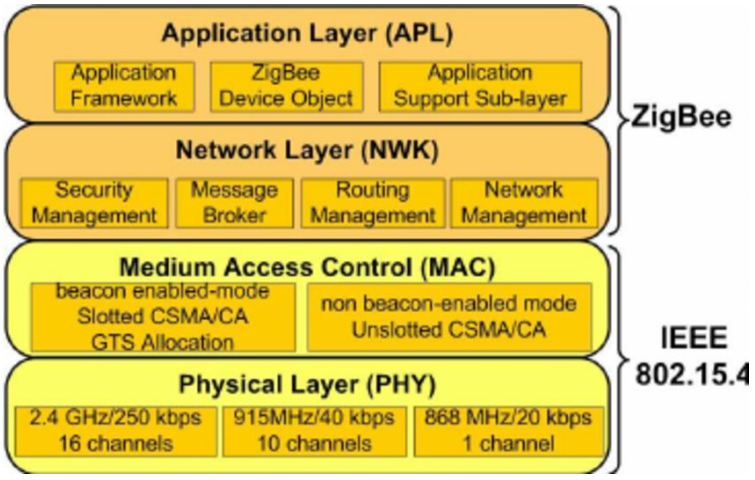
WSNs used in IoT systems are described as follows:

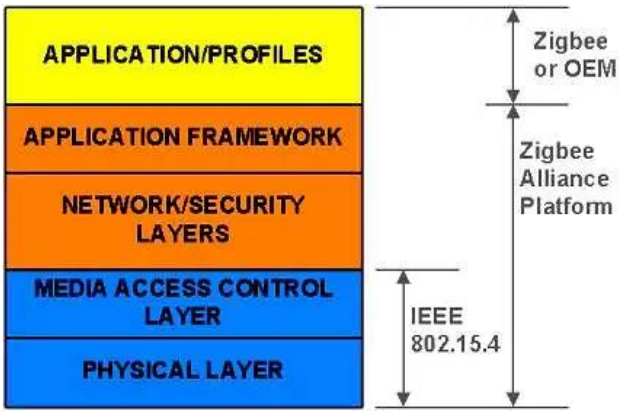
- **Weather Monitoring System**: in which nodes collect temperature, humidity and other data, which is aggregated and analyzed.
- **Indoor air quality monitoring systems**: to collect data on the indoor air quality and concentration of various gases.
- **Soil Moisture Monitoring Systems**: to monitor 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.

- **Structural Health Monitoring Systems**: Use WSNs to monitor the health of Structures (building, bridges) by collecting vibrations from sensor nodes deployed at various points in the structure.



WSNs are enabled by wireless communication protocols such as IEEE 802.15.4. Zig Bee is one of the most popular wireless technologies used by WSNs .Zig Bee specifications are based on IEEE 802.15.4. Zig Bee operates 2.4 GHz frequency and offers data rates upto 250 KB/s and range from 10 to 100meters.





Cloud Computing

Cloud computing is a transformative computing paradigm that involves delivering applications and services over the internet. Cloud computing involves provisioning of computing, networking and storage resources on demand and providing these resources as metered services to the users, in a "pay as you go". Cloud computing resources can be provisioned on-demand by the users, without requiring interactions with the cloud service provider. The process of provisioning resources is automated.

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 users as a virtual machine instances and virtual storage.
- **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.
- **Software-as-a-Service(SaaS):** Provides the user a complete software application or the User interface to the application itself. The cloud service provider manages the underlying cloud infrastructure including servers, network, operating systems, storage, and application software.

Big data Analysis

Big data is defined as collections of data sets whose volume , velocity or variety is so large that it is difficult to store, manage, process and analyze the data using traditional databases and data processing tools.

Some examples of big data generated by IoT are

1. Sensor data generated by IoT systems
2. Machine sensor data collected from sensors established in industrial and energy systems.
3. Health and fitness data generated IoT devices.

4. Data generated by IoT systems for location and tracking vehicles.
5. Data generated by retail inventory monitoring systems.

The underlying characteristics of Big Data are

Volume: There is no fixed threshold for the volume of data for big data. Big data is used for massive scale data.
Velocity: Velocity is another important characteristic of Big Data and the primary reason for exponential growth of data.
Variety: Variety refers to the form of data. Big data comes in different forms such as structured or unstructured data including test data, image, audio, video and sensor data.

Embedded Systems:
Embedded Systems is a computer system that has computer hardware and software embedded to perform specific tasks. Key components of embedded system include microprocessor or micro controller, memory (RAM, ROM, Cache), networking units (Ethernet Wi-Fi Adaptor), input/output units (Display, Keyboard, etc..,) and storage (Flash memory). Embedded System range from low cost miniaturized devices such as digital watches to devices such as digital cameras, POS terminals, vending machines, appliances etc.,

DOMAIN SPECIFIC IoTs

1) Home Automation:

a) Smart Lighting: helps in saving energy by adapting the lighting to the ambient conditions and switching on/off or diming the light when needed.
b) Smart Appliances: make the management easier and 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, LPGetc.

2) Cities:

a) Smart Parking: make the search for parking space easier and convenient for drivers. Smart parking are powered by IoT systems that detect the no. of empty parking slots and send information over internet to smart application backbends.
b) Smart Lighting: for roads, parks and buildings can help in saving energy.
c) Smart Roads: Equipped with sensors can provide information on driving condition, travel time estimating and alert in case of poor driving conditions, traffic condition and accidents.
d) Structural Health Monitoring: uses a network of sensors to monitor the vibration levels in the structures such as bridges and buildings.

e) Surveillance: The video feeds from surveillance cameras can be aggregated in cloud based scalable storage solution.
f) Emergency Response: IoT systems for fire detection, gas and water leakage detection can help in generating alerts and minimizing their effects on the critical infrastructures.

3) Environment:

a) Weather Monitoring: Systems collect data from a no. of sensors attached and send the data to cloud based applications and storage back ends. The data collected in cloud can then be analyzed and visualized by cloud-based applications.

b) Air Pollution Monitoring: System can monitor emission of harmful gases (CO2, CO, NO, NO2 etc.,) by factories and automobiles using gaseous and meteorological sensors. The collected data can be analyzed to make informed decisions on pollutions control approaches.

c) Noise Pollution Monitoring: Due to growing urban development, noise levels in cities have increased and even become alarmingly high in some cities. IoT based noise pollution monitoring Systems use a no. of noise monitoring systems that are deployed at different places in a city. The data on noise levels from the station is collected on servers or in the cloud. The collected data is then aggregated to generate noise maps.

d) Forest Fire Detection: Forest fire can cause damage to natural resources, property and human life. Early detection of forest fire can help in minimizing damage.

e) River Flood Detection: River floods can cause damage to natural and human resources and human life. Early warnings of floods can be given by monitoring the water level and flow rate. IoT based river flood monitoring system uses a no. of sensor nodes that monitor the water level and flow rate sensors.

4) Energy:

a) Smart Grids: is a data communication network integrated with the electrical grids that collects and analyze data captured in near real time about power transmission, distribution and consumption. Smart grid technology provides predictive information and recommendations to utilities, their suppliers, and their customers on how best to manage power. By using IoT based sensing and measurement technologies, the health of equipment and integrity of the grid can be evaluated.

b) Renewable Energy Systems: IoT based systems integrated with the transformers at the point of interconnection measure the electrical variables and how much power is fed into the grid. For wind energy systems, closed-loop controls can be used to regulate the voltage at point of interconnection, which coordinate wind turbine outputs and provides power support.

c) Prognostics: In systems such as power grids, real-time information is collected using specialized electrical sensors called Phasor Measurements Units (PMUs) at the substations. The information received from PMUs must be monitored in real-time for estimating the state of the system and for predicting failures.

5) Retail:

a) Inventory Management: IoT systems enable remote monitoring of inventory using data collected by RFID readers.

b) Smart Payments: Solutions such as contact-less payments powered by technologies such as Near Field Communication (NFC) and Bluetooth.

c) Smart Vending Machines: Sensors in smart vending machines monitors its operations and send the data to cloud, which can be used for predictive maintenance.

6) Logistics:

a) Route generation & scheduling: IoT based system backed by cloud can provide first response to the route generation queries and can be scaled upto serve a large transportation network.

b) Fleet Tracking: Use GPS to track locations of vehicles inreal-time.

c) Shipment Monitoring: IoT based shipment monitoring systems use sensors such as temparature, humidity, to monitor the conditions and send data to cloud, where it can be analyzed to detect foods spoilage.

d) Remote Vehicle Diagnostics: Systems use on-board IoT devices for collecting data on Vehicle operations (speed, RPMetc.) and status of various vehicle subsystems.

7) Agriculture:

a) Smart Irrigation: to determine moisture amount in the soil.

b) Green House Control: to improve productivity.

8) Industry:

a) Machine diagnosis and prognosis

b) Indoor Air Quality Monitoring

9) Health and Lifestyle:

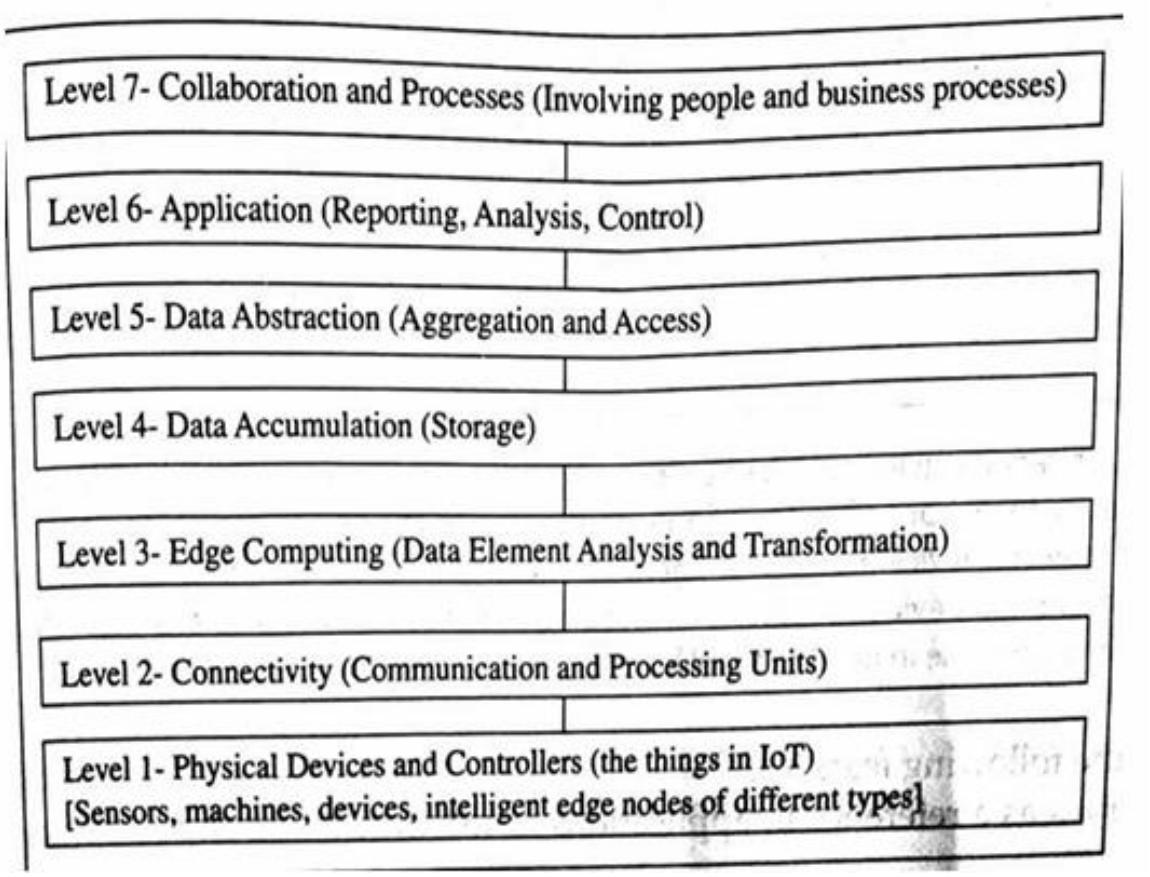
a) Health & Fitness Monitoring

b) Wearable Electronics

IoT Architectural View:

- The IoT system is defined in different levels called as tiers. A model enables the conceptualization of the framework.
- A reference model can be used to depict the building blocks, successive interactions and integration.

The diagram below depicts the CISCO presentation of a reference model comprising of seven levels and the functions of each level.

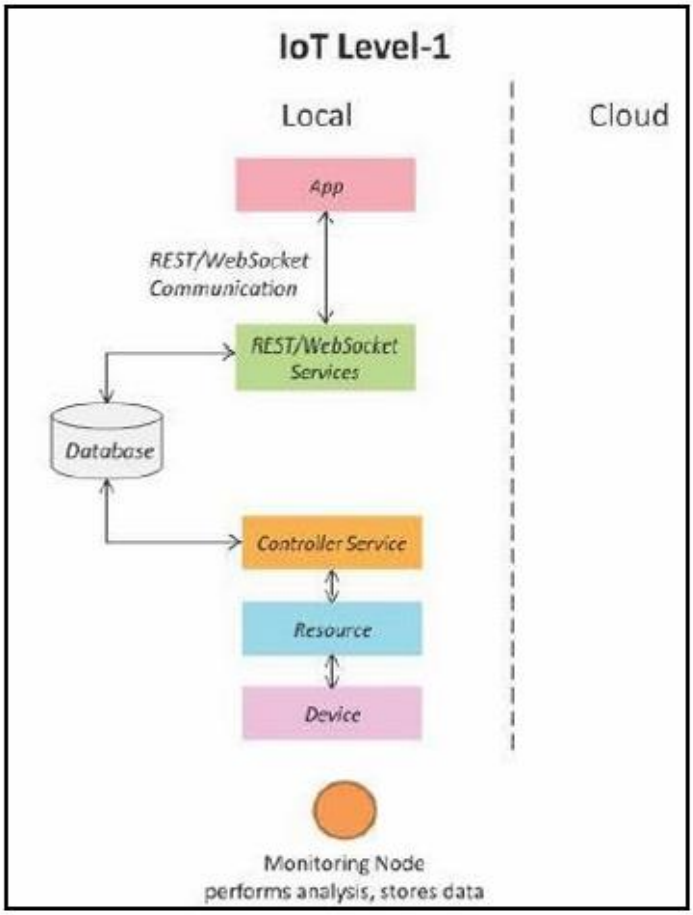


Features of the architecture:

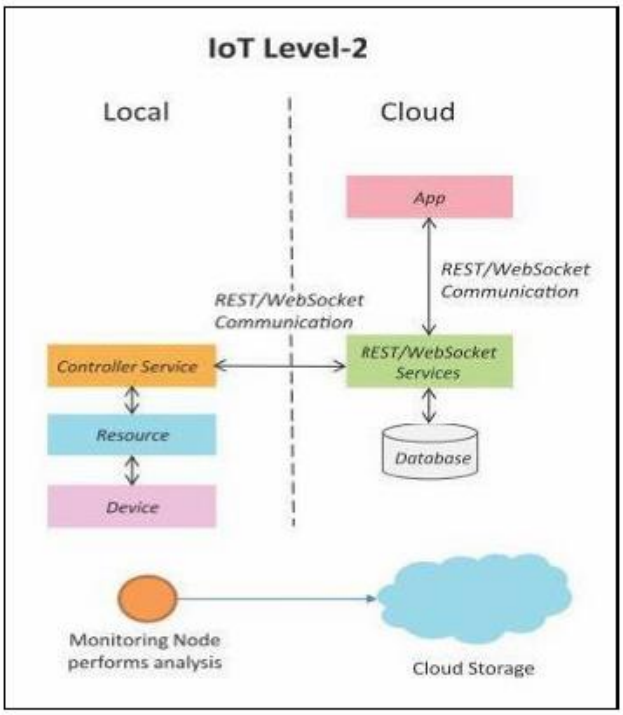
- The architecture serves as a reference in the applications of IoT in services and business processes.
- A set of sensors which are smart, capture the data, perform necessary data element analysis and transformation as per device application framework and connect directly to a communication manager.
- The communication management subsystem consists of protocol handlers, message routers and access management.
- Data routes from gateway through the Internet and data Centre to the application server or enterprise server which acquires that data.
- Organization and analysis subsystems enable the services, business processes, enterprise integration and complex processes.

IOT Levels and Deployment Templates

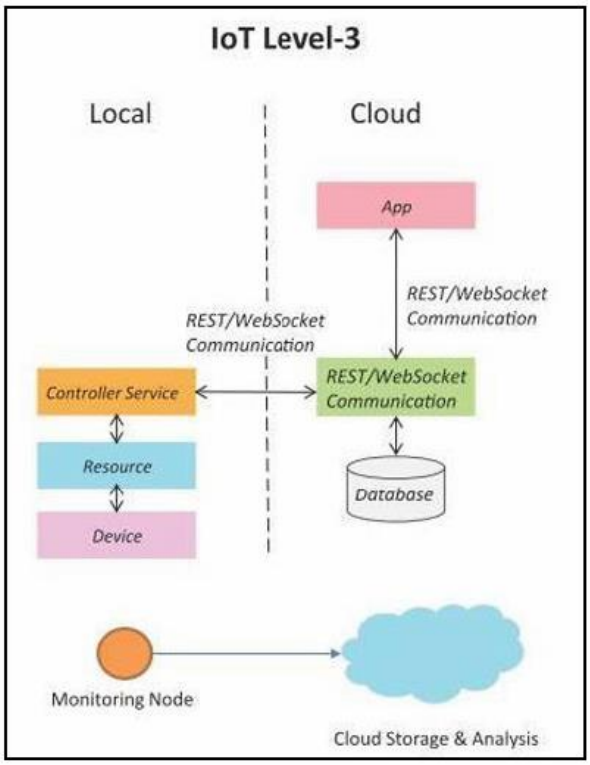
IoT Level 1: System has a single node that performs sensing and/or actuation, stores data, performs analysis and host the application as shown in fig. Suitable for modeling low cost and low complexity solutions where the data involved is not big and analysis requirement are not computationally intensive. An e.g., of IoT Level1 is Home automation.



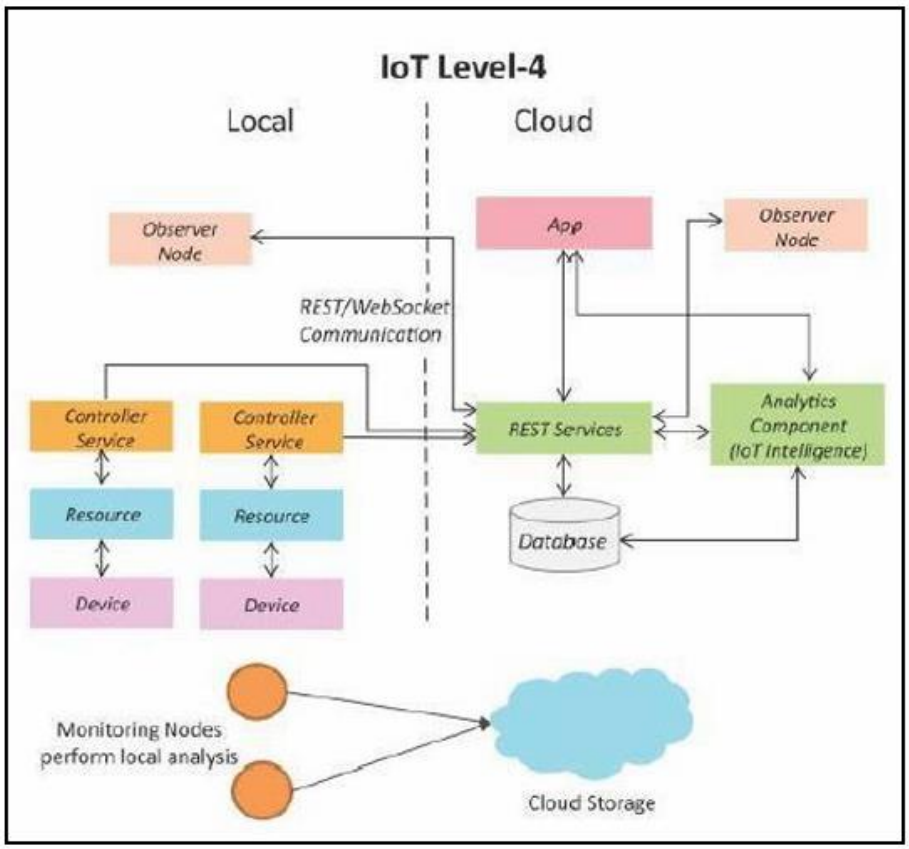
IoT Level2: has a single node that performs sensing and/or actuating and local analysis as shown in fig. Data is stored in cloud and application is usually cloud based. Level2 IoT systems are suitable for solutions where data are involved is big, however, the primary analysis requirement is not computationally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



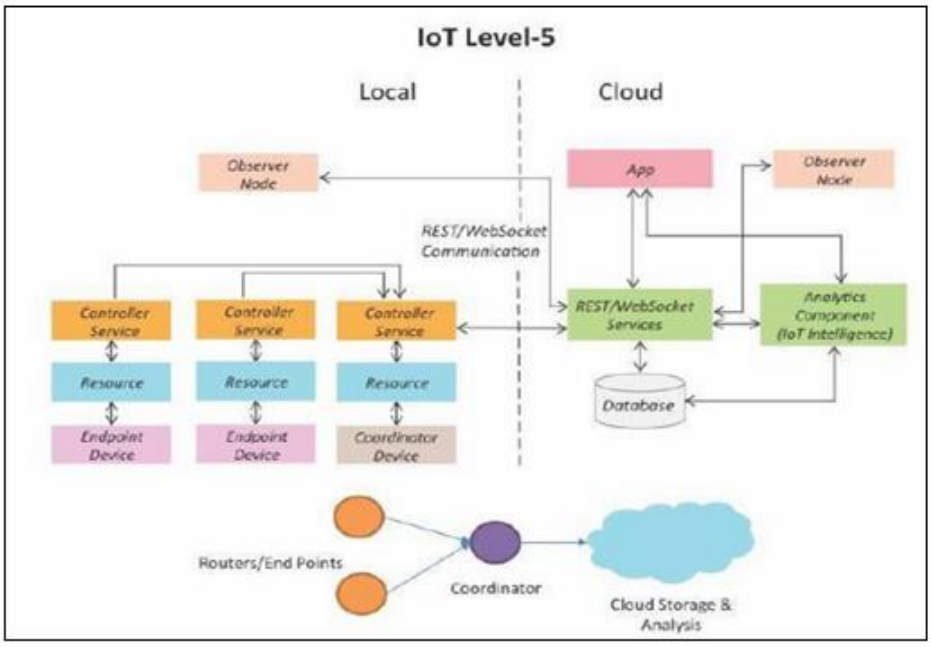
IoT Level3: system has a single node. Data is stored and analyzed in the cloud application is cloud based as shown in fig. Level3 IoT systems are suitable for solutions where the data involved is big and analysis requirements are computationally intensive. An example of IoT level3 system for tracking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



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.



IoT Level 5: 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.



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.