UNIT I **Introduction to IOT**

Introduction - Definition and Characteristics of IoT - Physical design - IoT Protocols - Logical design - IoT communication models, IoT Communication APIs - Enabling technologies - Wireless Sensor Networks, Cloud Computing, Embedded Systems, IoT Levels and Templates - Domain specific IoTs -home, city ,Environment, energy, Agriculture and Industry

1.1 Introduction

- The Internet of Things represents the whole way from collecting data, processing it, taking an action corresponding to the signification of this data to storing everything in the cloud. All this is made possible by the internet
- The Internet of things has become a very widely spread concept in the last few years. The reason for this is mainly the need to computerize and control most of the surrounding objects and have access to data in real time.
- Example: Parking sensors, about phones which can check the weather and so on

1.1.1 Definition & Characteristics of IoT Definition:

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

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:**

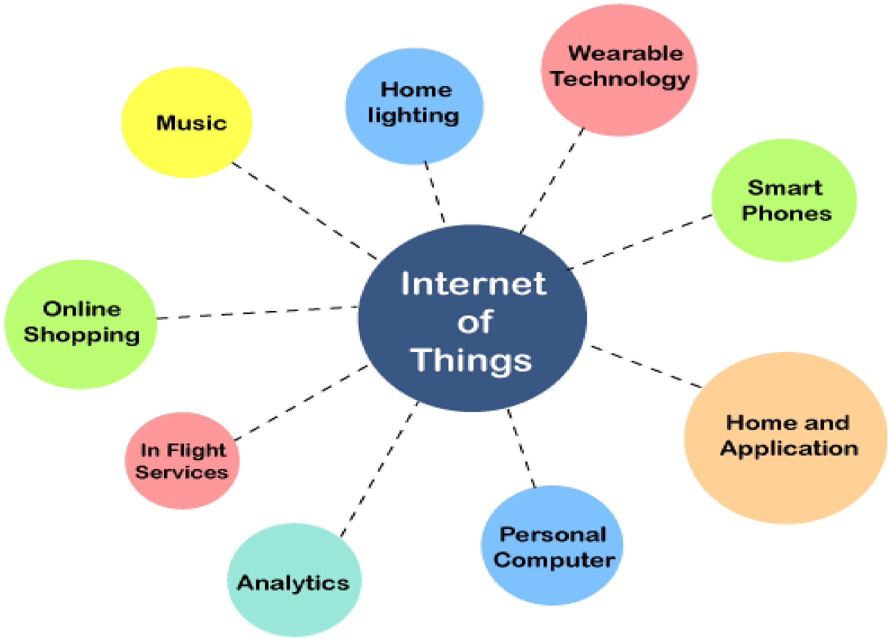
IOT devices have self configuring capability,allowing a large number of devices to work together to provide certain functionality. These devices have the ability configure themselves setup networking, and fetch latest software upgrades with minimal manual or user interaction.

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

Applications of IoT:



1) Home
2) Cities
3) Environment
4) Energy
5) Retail
6) Logistics
7) Agriculture
8) Industry
9) Health &LifeStyle

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.

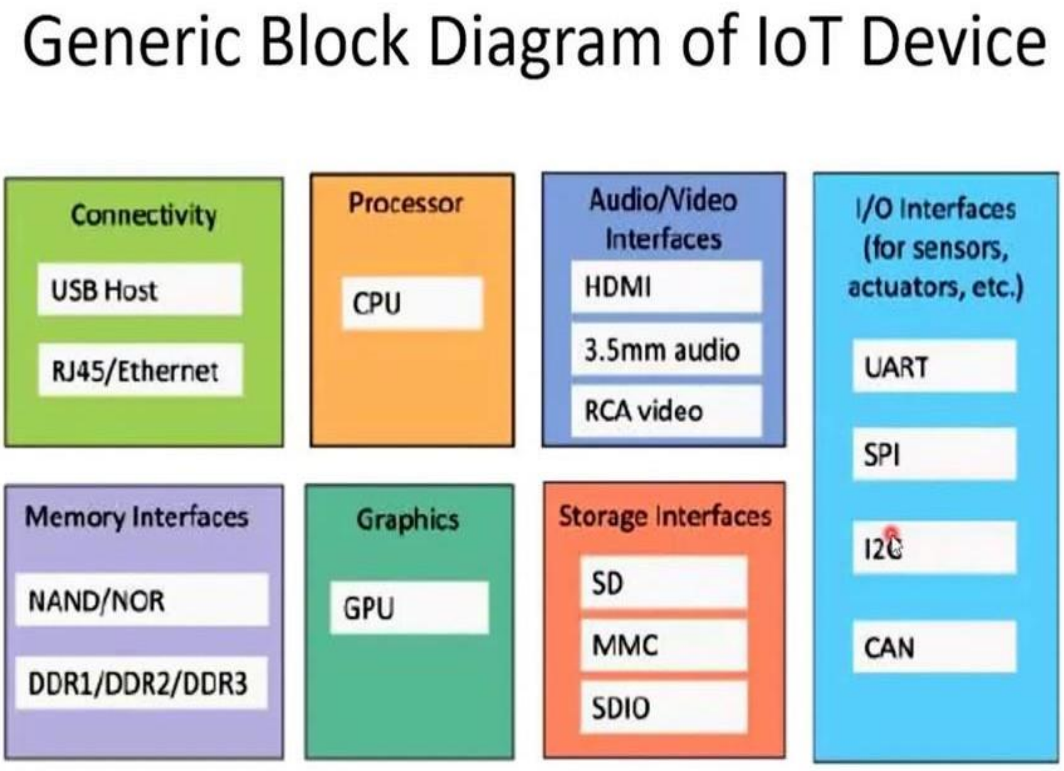
IoT devices can:

- 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.



- 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

IoT Protocols:

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. Eg: 802.3 uses co-axial cable; 802.3i uses copper twisted pair connection; 802.3j uses fiber optic connection; 802.3ae uses Ethernet overfiber.
- 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)

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:

Provides end-to-end message transfer capability independent of the underlying n/w. 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 congestioncollapse.
- 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 requestresponse 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.
- WebSocket: allows full duplex communication over a single socket connection.
- MQTT: Message Queue Telemetry Transport is light weight 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.

LOGICAL DESIGN of IoT

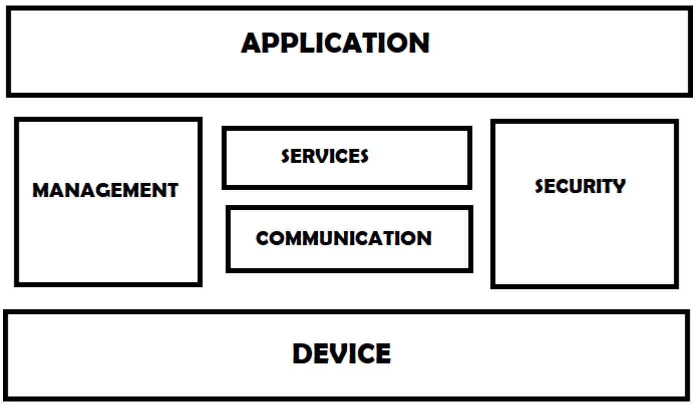
Refers to an abstract represent of entities and processes without going into the low level specifies of implementation.

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

1) IoT Functional Blocks:

Provide the system the capabilities for identification, sensing, actuation, communication and management

- Device: An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.
- Communication: handles the communication for IoT system.
- Services: for device monitoring, device control services, data publishing services and services for device discovery.
- Management: Provides various functions to govern the IoT system.
- Security: Secures IoT system and priority functions such as authentication, authorization, message and context integrity and data security.
- Application: IoT application provide an interface that the users can use to control and monitor various aspects of IoT system.



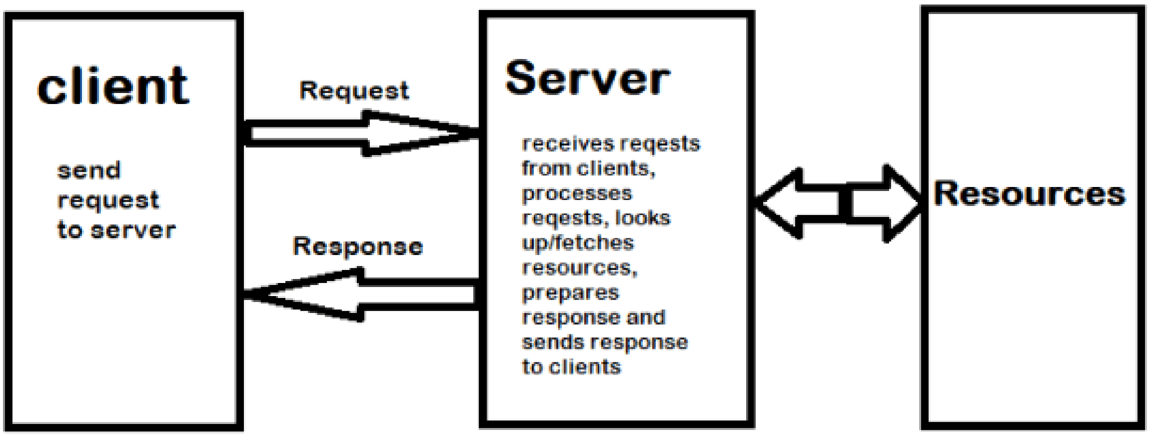
2) IoT Communication Models:

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

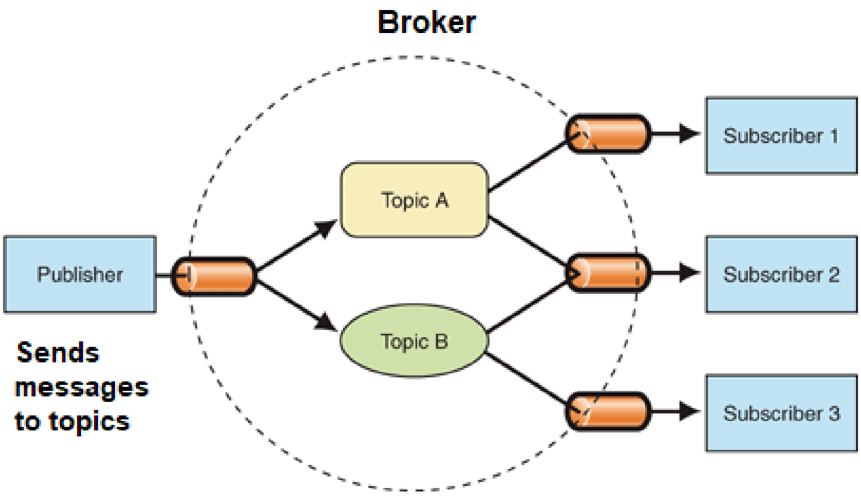
B) Publish-Subscribe communication model:

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 which 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

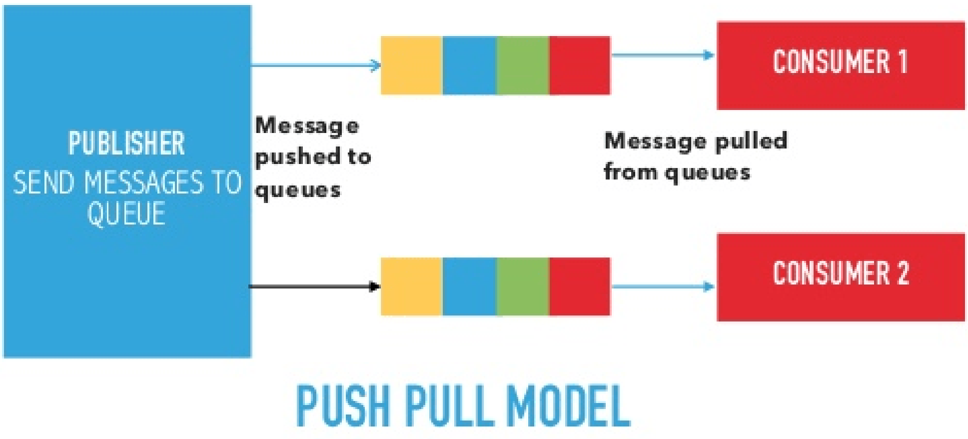


C) Push-Pull communication model:

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, fully duplex communication model that uses a persistent connection between the client and server.

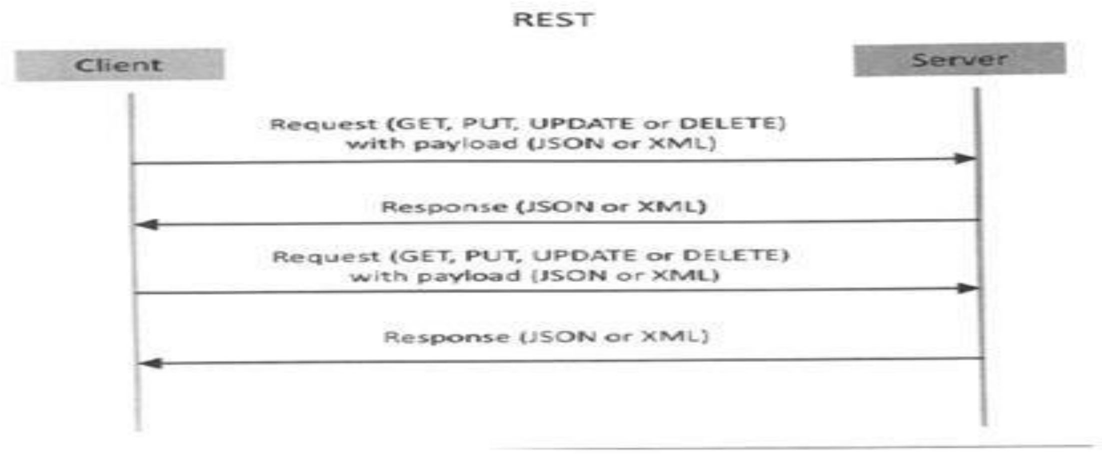
b. Once the connection is setup it remains open until the client sends a request to close the connection.

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)

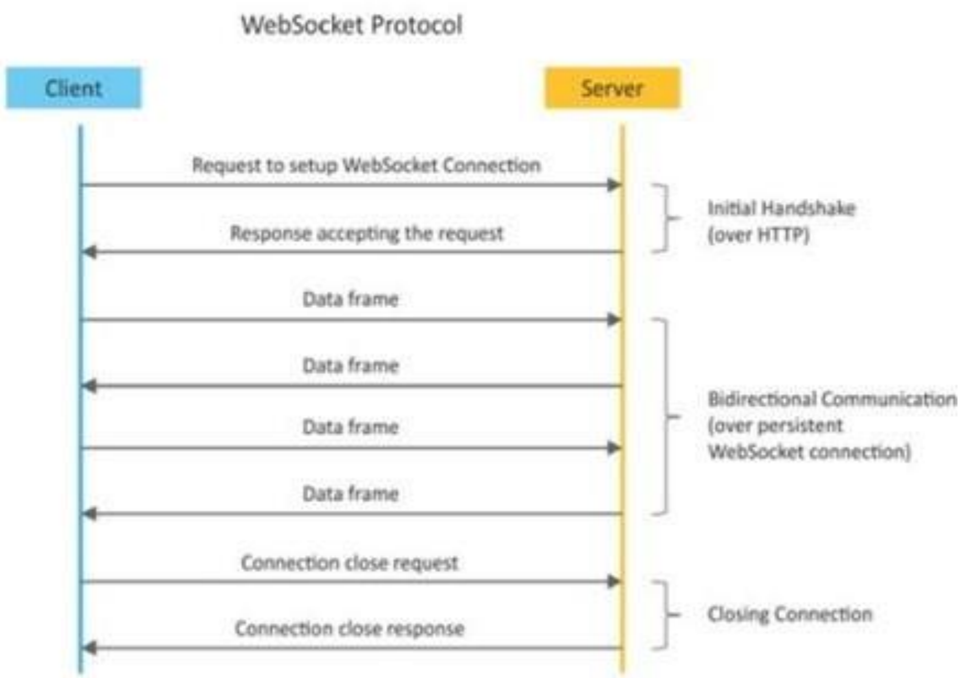
Request-Response model used by REST:

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



model.

1.4 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.

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

1.4.2 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.

1.4.3 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 Sensor data generated by IoT systems.

- Machine sensor data collected from sensors established in industrial and energy systems.
- Health and fitness data generated IoT devices.
- Data generated by IoT systems for location and tracking vehicles.
- Data generated by retail inventory monitoring systems.

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 characteristics 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 .

1.4.4 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.

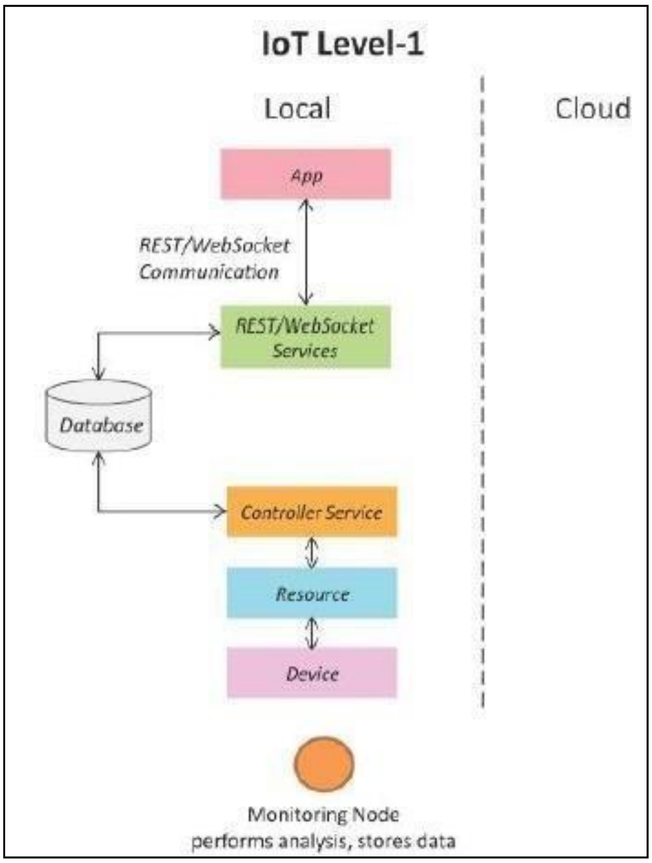
1.4.5 Embedded Systems:

Embedded Systemsis 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.,

1.5 IOT Levels and Deployment Templates.

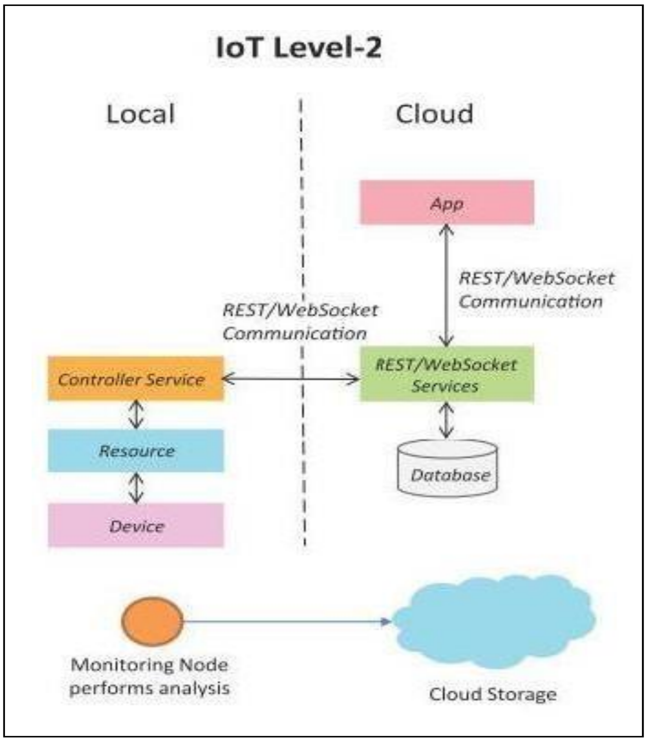
1.5.1 IoT Level-1

Level-1 IoT systems has a single node that performs sensing and/or actuation, stores data, performs analysis and host the application. 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 isHomeautomation.The system consist of a single node that allows controlling the lights and appliances in a home the device used in this system interfaces with the lights and appliances using electronic rely switches. The status information of each light or appliances is maintained in a local database. REST services deployed locally allow retrieving and updating the state of each lighter appliance in the status database. The controller service continuously monitors the state of each light or appliance by retrieving the light from the database.



1.5.2 IoT Level 2

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



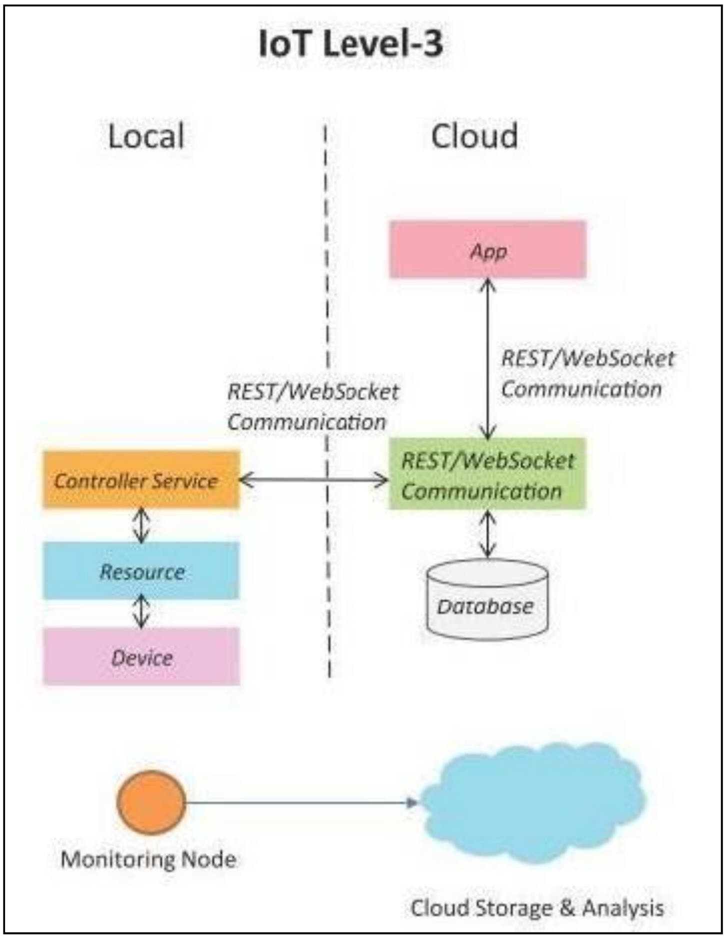
be done locally itself. An e,g., of Level2 IoT system for Smart Irrigation.

The system consists of a single node that monitors the soil moisture level and controls the irrigation system. The device used system collects soil moisture data from sensors. The controller service continuously monitors the moisture level. A cloud based REST web service is used for storing and retrieving moisture data which is stored in a cloud database. A cloud based application is used for visualizing the moisture level over a period of time which can help in making decision about irrigation schedule.

1.5.3 IoT Level 3

This 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.

The system consists of a single node that monitors the vibration levels for the package being shipped . The device in this system uses accelerometer and gyroscope sensor for monitoring vibration levels. The controller serves in the sensor data to the cloud in a real time using a websocket service. The data is stored in the cloud and also visualizing the cloud based applications . The analysis components in the cloud can trigger alerts if the vibration level becomes greater than the threshold.

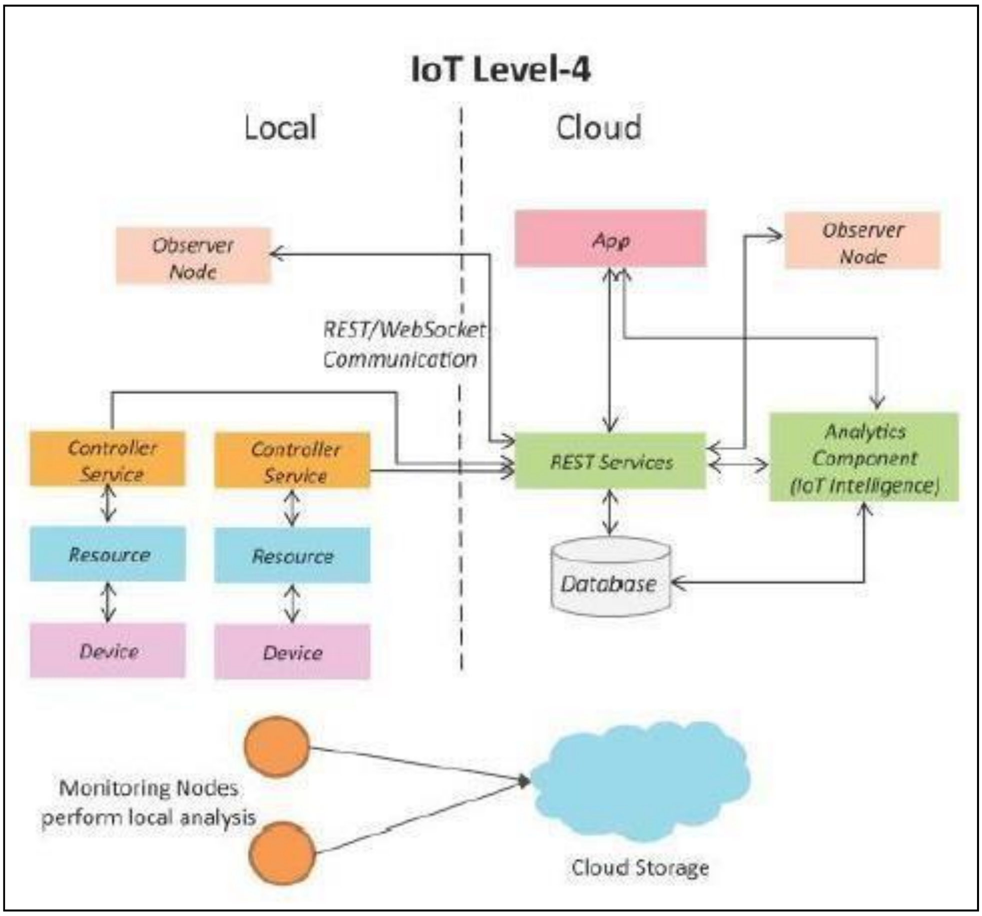


1.5.4 IoT Level 4

This 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. Level 4 IoT systems are suitable for solutions where multiple nodes are required, the data involved in big and the analysis requirements are computationally intensive.

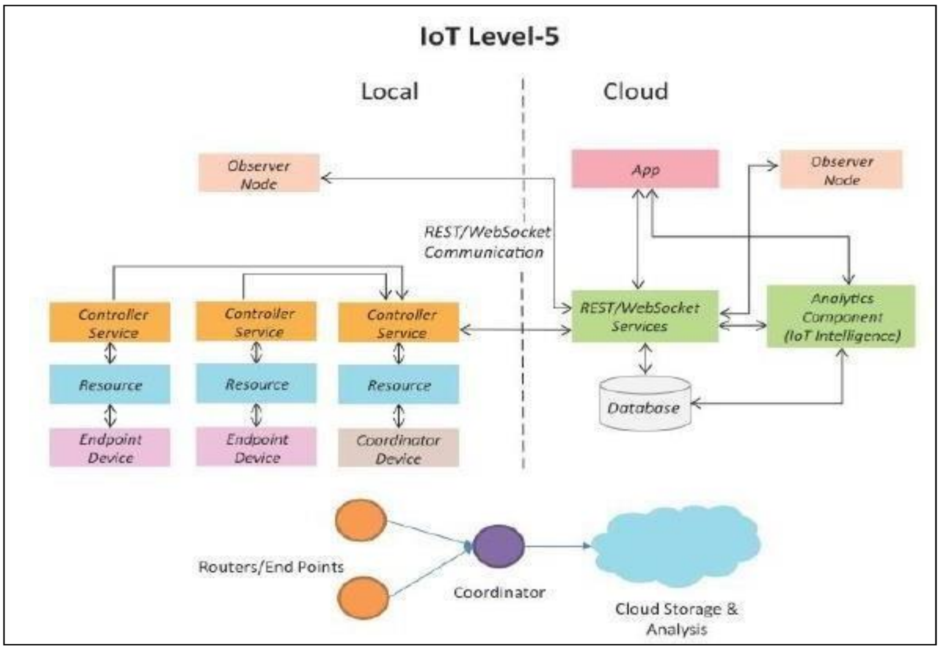
Example : IoT System for Noise Monitoring.

The system consists of multiple nodes placed in different locations for monitoring noise levels in an area. The nodes in this example are equipped with sound sensors. Nodes are independent of each other. Each nodes runs its owner controller service that sends the data to the cloud . The data is stored in cloud database. The analysis of data collected from a number of nodes is done in the cloud. A cloud based application is used for visualizing the aggregated data.



1.5.5 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 are high intensive.



Example :IoT system for Forest Fire Detection.

The system consists of multiple nodes placed in different locations for monitoring temperature, humidity and CO_2 levels in a forest. The end nodes in this example are equipped with various sensors such as temperature, humidity and CO_2. The coordinator node collects the data from the end nodes and act as a gateway that provides internet connectivity to the IoT system. The controller service on the coordinator device sends the collected data to the cloud. The data is stores in a cloud database. The analysis of data is done in the computing cloud to aggregate the data and make predictions. A cloud based applications is used for visualizing the data

1.5.6 IoT Level 6.

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 data base. The results are visualized with the cloud based applications. The centralized controller is aware of the status of all end nodes and sends control commands tothe nodes.
Example weather monitoring system

The system consists of multiple nodes placed in different locations for monitoring temperatures, humidity and pressure in an area. the end nodes are equipped with various sensors(such as temperature, humidity and pressure).the end nodes send the data to the cloud real time using a websocket service. the data is stored in a cloud database. The analysis of data is done in a cloud to aggregate a data and make predictions. A cloud based application is used for visualizing the data.

LEVELS	COST	COMPUTATION OF ANALYSIS	NODES	DATA STORAGE LOCATION	APPLICATION
1	Low	Low	Single	Local	Local
2	High	Low	Single	Cloud	Cloud
3	High	High	Single	Cloud	Cloud
4	High	Low	Multiple	Cloud	Cloud
5	High	High	Multiple	Cloud	Cloud
6	High	High	Multiple	Cloud	Cloud

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 also provide status information to the users remotely.

c) **Intrusion Detection:** use security cameras and sensors(PIR sensors and door sensors) to detect intrusion and raise alerts. Alerts can be in the form of SMS or email sent to the user.

d) **Smoke/Gas Detectors:** Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of fire. Alerts raised by smoke detectors can be in the form of signals to a fire alarm system. Gas detectors can detect the presence of harmful gases such as CO, 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 backends.

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(CO_2, CO, NO, NO_2 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 Measurment 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 RFIDreaders.

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 a 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 temp, humidity, to monitor the conditions and send data to cloud, where it can be analyzed to detect foods poilage.

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

Sensors:

- These form the front end of the IoT devices. These are the so-called “Things” of the system.
- Their main purpose is to collect data from its surroundings (sensors) or give out data to its surrounding (actuators).
- These have to be uniquely identifiable devices with a unique IP address so that they can be easily identifiable over a large network.
- These have to be active in nature which means that they should be able to collect real-time data.
- These can either work on their own (autonomous in nature) or can be made to work by the user depending on their needs (user-controlled).
- Examples of sensors are gas sensor, water quality sensor, moisture sensor, etc.

Different Types Of Sensors And Their Uses:

The following is a list of different types of sensors that are commonly used in various applications with examples. All these types are used for measuring one of the physical properties like Temperature, Resistance, Capacitance, Conduction, Heat Transfer etc.

Type of Sensor	**Used For**
Temperature Sensor	Controlling HVAC systems in homes and offices
Proximity Sensor	Detecting objects in automatic doors
Accelerometer Sensor	Screen orientation in smartphones
IR Sensor (Infrared Sensor)	Remote controls for TVs and other devices
Pressure Sensor	Monitoring tire pressure in vehicles
Light Sensor	Adjusting screen brightness on smartphones
Ultrasonic Sensor	Parking assistance in cars
Flow and Level Sensor	Managing water levels in tanks
Smoke, Gas and Alcohol Sensor	Detecting smoke and gas leaks in homes
Microphone (Sound Sensor)	Voice recognition in smart speakers
Touch Sensor	Touchscreens on smartphones and tablets
Color Sensor	Color detection in industrial sorting machines
Humidity Sensor	Controlling humidity levels in greenhouses

Magnetic Sensor (Hall Effect Sensor)	Detecting the position of a rotating object
Position Sensor	Tracking the position of machine parts
Tilt Sensor	Detecting the tilt of gaming controllers
PIR Sensor	Motion detection in security systems
Strain and Weight Sensor	Weighing items on digital scales
Gyroscope Sensor	Stabilizing drones during flight
Optical Sensor	Adjusting lighting in smart home systems
Capacitive Sensor	Touchpads on laptops
Piezoelectric Sensor	Detecting vibrations in musical instruments
Thermal Sensor	Temperature control in ovens
RFID Sensor	Tracking inventory in warehouses
Chemical Sensor	Monitoring air quality

Actuators:

- Actuators are devices that turn electrical signals into physical motions or movements.
- These devices are used to control and manipulate physical items in the real world using data from sensors in an IoT system.
- Actuators are essential to the operation of IoT devices because they enable the automation and control of physical systems and machinery.
- Actuators in IoT include motors, solenoids, hydraulic and pneumatic systems, and other devices that may control or manipulate physical things.

Examples of Actuators in Internet of Things

- **Smart Home Systems:** Actuators are an important part of smart home systems. They let customers remotely operate various equipment such as lights, heating systems, and security systems. A smart thermostat, for example, can use temperature sensors to change the temperature in a home, and an actuator can activate the heating or cooling system as needed.
- **Industrial Automation:** Actuators are frequently employed in industrial automation to control machines and other systems. Hydraulic actuators, for example, might be used to control the movement of robotic arms in a factory, while electric actuators could be used

to regulate the position of a conveyor belt.

- **Agriculture:** Actuators are rapidly being employed to automate numerous processes in agriculture, such as irrigation and harvesting. An actuator, for example, can control the flow of water in an irrigation system or the position of a robotic arm used to harvest crops.
- **Healthcare:** Actuators are employed in a variety of healthcare applications, including prostheses and medical equipment. An actuator, for example, can regulate the movement of a prosthetic limb or the location of a surgical tool during treatment.