# Unit-1

**Contents** **pg.no**

# INTRODUCTION

"Internet of Things" was coined by Kevin Ashton in 1999, and it has recently become more relevant to the practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics.

Imagine a world where billions of objects can sense, communicate and share information, all interconnected over public or private Internet Protocol (IP) networks. These interconnected objects have data regularly collected, analyzed and used to initiate action, providing a wealth of intelligence for planning, management and decision making. This is the world of the Internet of Things.


## DEFINITION AND CHARACTERISTICS OF IOT

Definition :

IOT can be defined as a global infrastructure that enables advanced services by interconnecting physical and virtual things based on existing information and communication technology .

The Internet of Things (IoT) refers to a system of interrelated, internet-connected objects that are able to collect and transfer data over a wireless network without human intervention.

### Characteristics of IoT:

Various characteristics of IoT are:

- Dynamic and self-adapting
- Self-configuring
- Interoperable Communication protocols
- Unique identity

- Integrated into information network

## Dynamic and self-adapting:

The IoT devices can dynamically adapt with sensed environment, their operating conditions, and user's context and take actions accordingly. For ex: Surveillance System

## Self-configuring:

I. IoT devices can be able to upgrade the software with minimal intervention of user, whenever they are connected to the internet

. II. They can also setup the network i.e a new device can be easily added to the existing network. For ex: Whenever there will be free wifi access one device can be connected easily.

**Interoperable Communication**: IoT allows different devices (different in architecture) to communicate with each other as well as with different network. For ex: MI Phone is able to control the smart AC and smart TV of different manufacturer.

## Unique identities:

I. The devices which are connected to the internet have unique identities i.e IP address through which they can be identified throughout the network

. II. The IoT devices have intelligent interfaces which allow communicating with users. It adapts to the environmental contexts.

III. It also allows the user to query the devices, monitor their status, and control them remotely, in association with the control, configuration and management infrastructure.

## Integrated into information network:

I. The IoT devices are connected to the network to share some information with other connected devices. The devices can be discovered dynamically in the network by other devices. For ex. If a device has wifi connectivity then that will be shown to other nearby devices having wifi connectivity

II. The devices ssid will be visible though out the network. Due to these things the network is also called as information network.

III. The IoT devices become smarter due to the collective intelligence of the individual devices in collaboration with the information network. For Ex: weather monitoring system. Here the information collected from different monitoring nodes (sensors, arduino devices) can be aggregated and analysed to predict the weather.

# Physical Design of IoT

**Physical Design of IoT** refers to IoT Devices and IoT Protocols. Things are Node device which have unique identities and can perform remote sensing, actuating and monitoring capabilities. Communication established between things and cloud based server over the Internet by various IoT protocols.

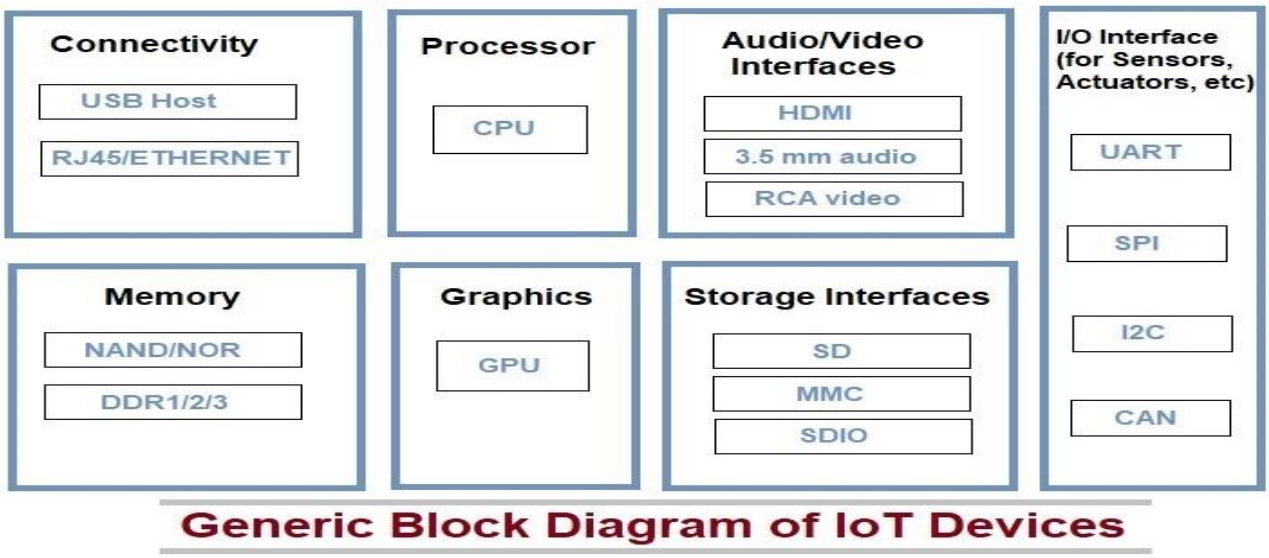
# Things

Basically Things refers to IoT Devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities. Things are is main part of IoT Application. IoT Devices can be various type, Sensing Devices, Smart Watches, Smart Electronics appliances, Wearable Sensors, Automobiles, and industrial machines.

IoT devices can:

Exchange data with other connected devices and applications (directly or indirectly).

- Collect data from other devices and process the data locally .
- Send the data to centralized servers or cloud-based application back-ends for processing the data, or
- Perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints.



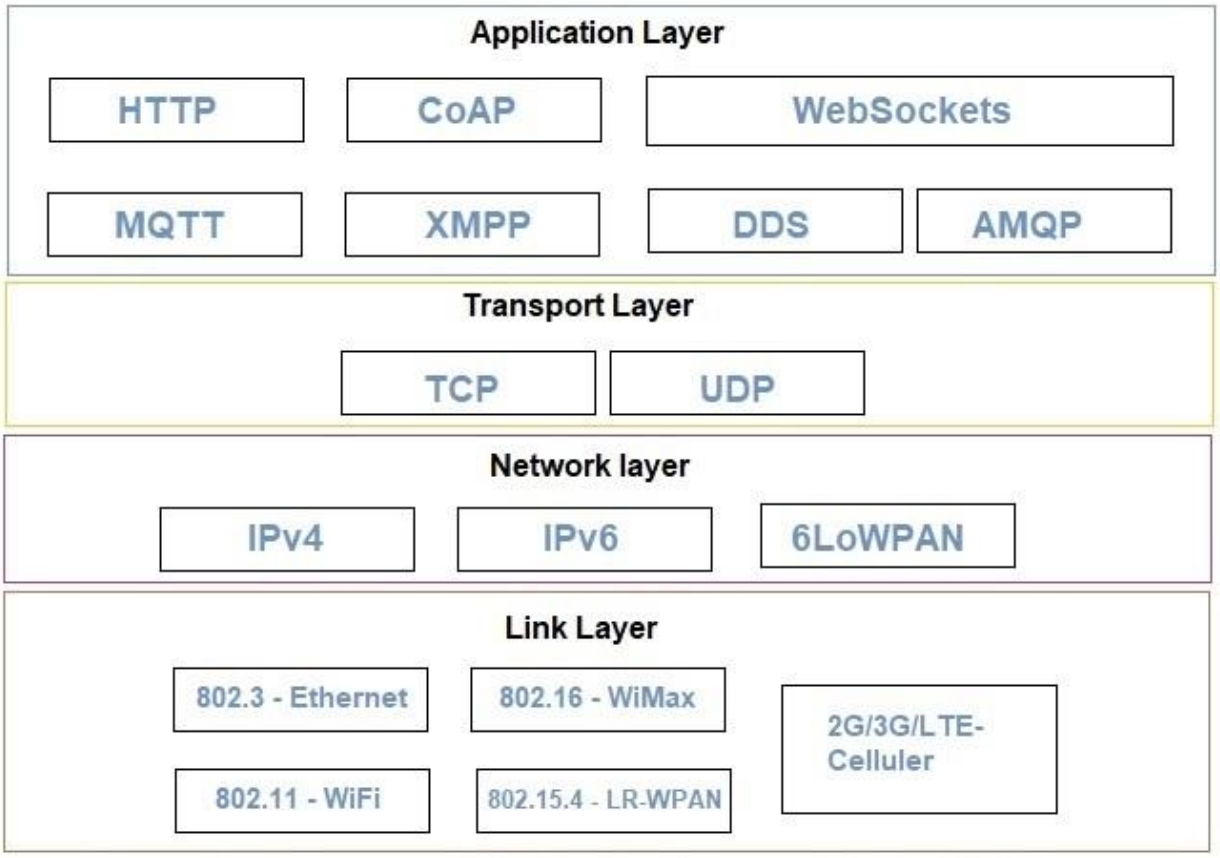

Generic Block Diagram of IoT Devices

As shown in above diagram 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 interface

# 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. An image is given below. By this image you can understand which protocols used.




# *1.Link Layer*

Link layer protocols determine how data is physically sent over the network's physical layer or medium (Coxial calbe or other or radio wave). This Layer determines how the packets are coded and signaled by the hardware device over the medium to which the host is attached (eg. coxial cable).

Here we explain some Link Layer Protocols:

**1. 802.3 – Ethernet :** Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s by IEEE 802.3 standard. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.
802.3i – is IEEE standard for 10Base5 that uses coaxial cable as shared medium .

802.3j-- is IEEE standard for 10BaseT uses copper twisted pair connection .

802.3ae -- is IEEE standard for 10Gbs/Ethernet over fiber.

**2. 802.11 – WiFi** : IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 60 GHz frequency bands.

Forex:

802.11a – operates in 5GHZ band.

802.11b,802.11g—operates in2.4GHZ band

802..11n---operates in 2.4/2.5GHZ band

3. 802.16 – Wi-Max : The standard for WiMAX technology is a standard for Wireless Metropolitan Area Networks (WMANs) that has been developed by working group number 16 of IEEE 802, specializing in point-to-multipoint broadband wireless access.

2G/3G/4G- Mobile Communication : These are different types of telecommunication generations. IoT devices are based on these standards can communicate over the celluer networks.

# *2.Network Layer*

---

Responsible for sending of IP datagrams from the source network to the destination network. Network layer performs the host addressing and packet routing. We used IPv4 and IPv6 for Host identification. IPv4 and IPv6 are hierarchical IP addrssing schemes.

1.IPv4 :
IPv4 is the most deployed intrnet protocol used to identify the device on a network using hierarchical addressing scheme.ipv4 uses 32 bit addressing scheme which allows to identify 26^32 addresses . But more and more addresses got connected to the inntenet addresses got exhausted by year 2011 .IPV6 succeeded this .

2.IPV6 : it is the newest version in nternet protocol which uses 2^128 addresses .

**3.6LoWPAN :** It is an acronym of *IPv6 over Low-Power Wireless Personal Area Networks*. 6LoWPAN is the name of a concluded working group in the Internet area of the IETF. This protocol allows for the

smallest devices with limited processing ability to transmit information wirelessly using an internet protocol. 6LoWPAN can communicate with 802.15.4 devices as well as other types of devices on an IP network link like WiFi.

# *Transport Layer*

---

This layer provides functions such as error control, segmentation, flow control and congestion control. So this layer protocols provide end-to-end message transfer capability independent of the underlying network.

**1.TCP :** TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other.

**UDP :** User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is unreliable and connectionless protocol. So, there is no need to establish connection prior to data transfer.

# *Application Layer*

---

Application layer protocols define how the applications interface with the lower layer protocols to send over the network.

**HTTP :** *Hypertext Transfer Protocol (HTTP)* is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes. HTTP follows a classical client-server model, with a client opening a connection to make a request, then waiting until it receives a response. HTTP is a stateless protocol, meaning that the server does not keep any data (state) between two requests.
**CoAP :** CoAP-Constrained Application Protocol is a specialized Internet Application Protocol for constrained devices, as defined in RFC 7252. It enables devices to communicate over the Internet. The protocol is especially targeted for constrained hardware such as 8-bits microcontrollers, low power sensors and similar devices that can't run on HTTP or TLS

**WebSocket :** The WebSocket Protocol enables two-way communication between a client running untrusted code in a controlled environment to a remote host that has opted-in to communications from that code. The security model used for this is the origin-based security model commonly used by web browsers.

**MQTT :** MQTT is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport and useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium

**XMPP : Extensible Messaging and Presence Protocol** (**XMPP**) is a communication protocol for message-oriented middleware based on XML (Extensible Markup Language). It enables the near-real-time exchange of structured yet extensible data between any two or more network entities.

**DDS :** The Data Distribution Service (DDS™) is a middleware protocol and API standard for data-centric connectivity from the Object Management Group® (OMG®). It integrates the components of a system together, providing low-latency data connectivity, extreme reliability, and a scalable architecture that business and mission-critical Internet of Things (IoT) applications need.

**AMQP :** The AMQP – IoT protocols consist of a hard and fast of components that route and save messages within a broker carrier, with a set of policies for wiring the components together. The AMQP protocol enables patron programs to talk to the dealer and engage with the AMQP model.

# Logical Design of IoT

In this article we discuss Logical design of Internet of things. Logical design of IoT system refers to an abstract representation of the entities & processes without going into the low-level specifies of the implementation. For understanding Logical Design of IoT, we describes given below terms.

- IoT Functional Blocks
- IoT Communication Models
- IoT Communication APIs

# IoT Functional Blocks

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:

**Device:** An IoT system comprises of devices that provide sensing, actuation, monitoring and control functions.

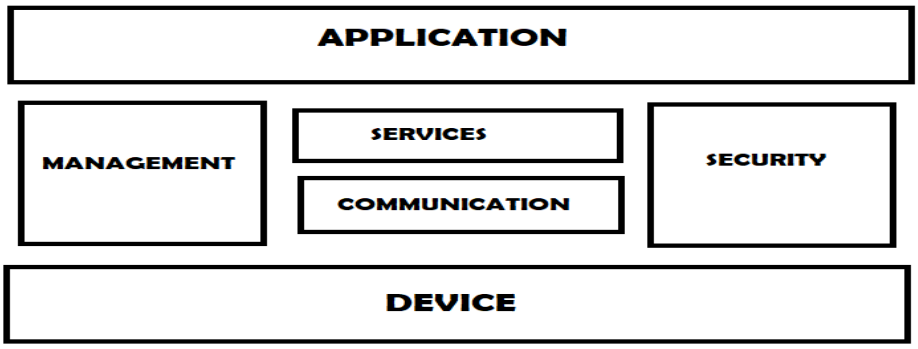
**Communication:** Handles the communication for the IoT system.

**Services:** services for device monitoring, device control service, data publishing services and services for device discovery.

**Management:** this blocks provides various functions to govern the IoT system.

**Security:** this block secures the IoT system and by providing functions such as authentication , authorization, message and content integrity, and data security.

**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

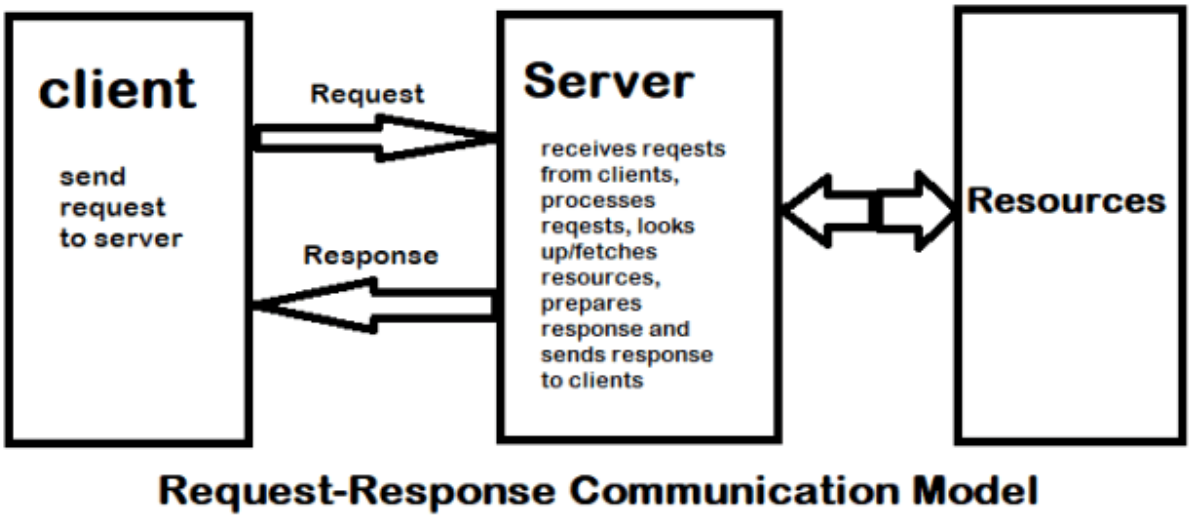
---

# Request-Response Model

Request-response model is 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 representation, prepares the response, and then sends the response to the client. Request-response is a stateless communication model and each request-response pair is independent of others.

HTTP works as a request-response protocol between a client and server. A web browser may be the client, and an application on a computer that hosts a web site may be the server.

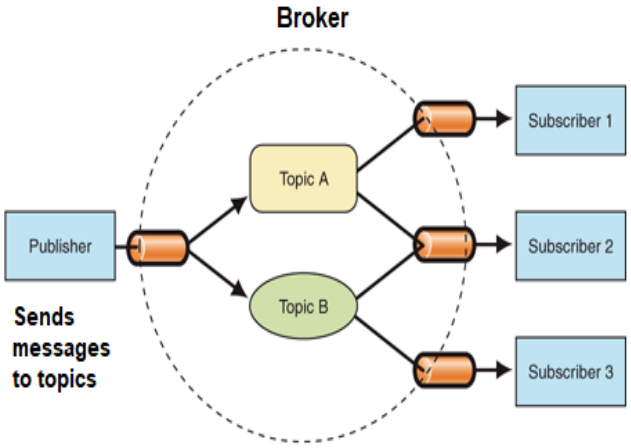
Example: A client (browser) submits an HTTP request to the server; then the server returns a response to the client. The response contains status information about the request and may also contain the requested content.




Request-Response Communication Model

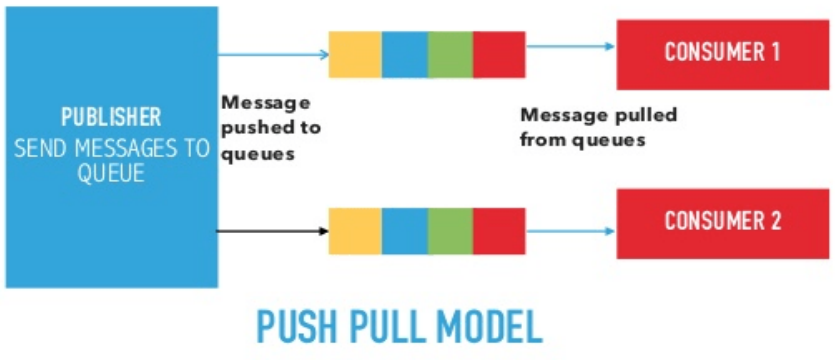
# Publish-Subscribe Model

Publish-Subscribe is a communication model that involves publishers, brokers and consumers. 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. Consumers subscribe to the topics which are managed by the broker. When the broker receive data for a topic from the publisher, it sends the data to all the subscribed consumers.



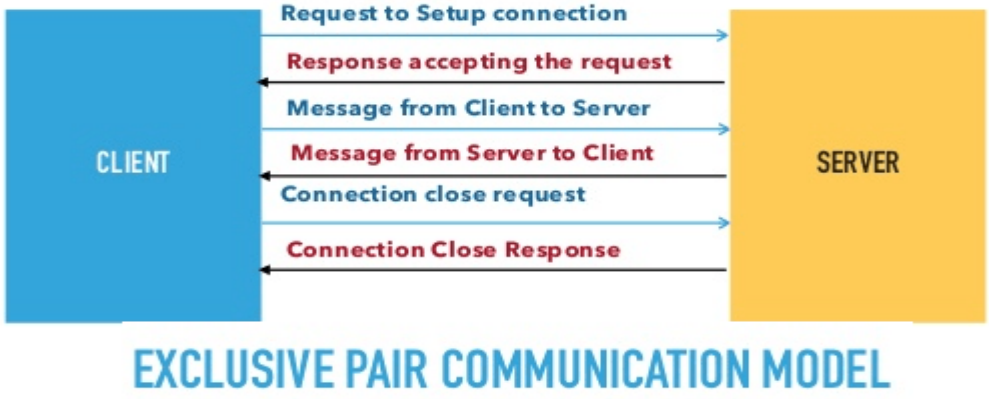
# Push-Pull Model

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. Queues help in decoupling the messaging between the Producers and Consumers. 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 rate at which the consumer pull data.




# Exclusive Pair Model

Exclusive Pair is a bidirectional, fully duplex communication model that uses a persistent connection between the client and server. Connection is setup it remains open until the client sends a request to close the connection. Client and server can send messages to each other after connection setup. Exclusive pair is stateful communication model and the server is aware of all the open connections.




# IoT Communication APIs

Generally we used Two APIs For IoT Communication. These IoT Communication APIs are:

- REST-based Communication APIs
- WebSocket-based Communication APIs

# REST-based Communication APIs

Representational state transfer (REST) is a set of architectural principles by which you can design Web services the Web APIs that focus on systems's resources and how resource states are addressed and transferred. REST APIs that follow the request response communication model, the rest architectural constraint apply to the components, connector and data elements, within a distributed hypermedia system. The rest architectural constraint are as follows:

**Client-server –** The principle behind the client-server constraint is the separation of concerns. for example clients should not be concerned with the storage of data which is concern of the serve. Similarly the server should not be concerned about the user interface, which is concern of the clien. Separation allows client and server to be independently developed and updated.

**Stateless** – Each request from client to server must contain all the information necessary to understand the request, and cannot take advantage of any stored context on the server. The session state is kept entirely on the client.

**Cache-able** – Cache constraints requires that the data within a response to a request be implicitly or explicitly leveled as cache-able or non cache-able. If a response is cache-able, then a client cache is given the right to reuse that repsonse data for later, equivalent requests. caching can partially or completely eliminate some instructions and improve efficiency and scalability.

**Layered system** – layered system constraints, constrains the behavior of components such that each component cannot see beyond the immediate layer with they are interacting. For example, the client cannot tell whether it is connected directly to the end server or two an intermediaryalong the way. System scalability can be improved by allowing intermediaries to respond to requests instead of the end server, without the client having to do anything different.

**Uniform interface** – uniform interface constraints requires that the method of communication between client and server must be uniform. Resources are identified in the requests (by URIsin web based systems) and are themselves is separate from the representations of the resources data returned to the client. When a client holds a representation of resources it has all the information required to update or delete the resource you (provided the client has required permissions). Each message includes enough information to describe how to process the message.

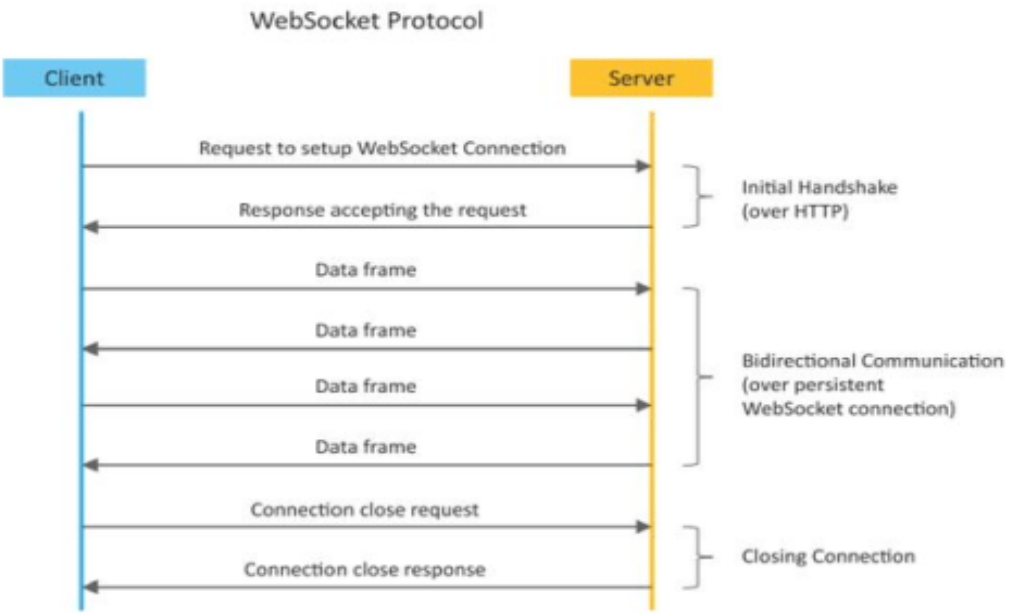
**Code on demand** – Servers can provide executable code or scripts for clients to execute in their context. this constraint is the only one that is optional.
A RESTful web service is a " Web API " implemented using HTTP and REST principles. REST is most popular IoT Communication APIs.

**HTTP METHODS/COMMANDS SHOWN IN ABOVE TABLE :**

| HTTP Method | Action | Examples |
|---|---|---|
| GET | Obtain information about a resource | http://example.com/api/orders (retrieve order list) |
| GET | Obtain information about a resource | http://example.com/api/orders/123 (retrieve order #123) |
| POST | Create a new resource | http://example.com/api/orders (create a new order, from data provided with the request) |
| PUT | Update a resource | http://example.com/api/orders/123 (update order #123, from data provided with the request) |
| DELETE | Delete a resource | http://example.com/api/orders/123 (delete order #123) |

# WebSocket based communication API

Websocket APIs allow bi-directional, full duplex communication between clients and servers. Websocket APIs follow the exclusive pair communication model. Unlike request-response model such as REST, the WebSocket APIs allow full duplex communication and do not require new coonection to be setup for each message to be sent. Websocket communication begins with a connection setup request sent by the client to the server. The request (called websocket handshake) is sent over HTTP and the server interprets it is an upgrade request. If the server supports websocket protocol, the server responds to the websocket handshake response. After the connection setup client and server can send data/mesages to each other in full duplex mode. Websocket API reduce the network traffic and letency as there is no overhead for connection setup and termination requests for each message. Websocket suitable for IoT applications that have low latency or high throughput requirements. So Web socket is most suitable IoT Communication APIs for IoT System.


WebSocket Protocol
Client
Server
Request to setup WebSocket Connection
Response accepting the request
Initial Handshake
(over HTTP)
Data frame
Data frame
Data frame
Data frame
Bidirectional Communication
(over persistent
WebSocket connection)
Connection close request
Connection close response
Closing Connection

# SENSING

A **sensor** is a device that is able to detect changes in an environment. By itself, a **sensor** is useless, but when we use it in an electronic system, it plays a key role. A **sensor** is able to measure a physical phenomenon (like temperature, pressure, and so on) and transform it into an electric signal.

## What is a Sensor? ¬

A device that receives and responds to a signal or stimulus.

The sensor converts any type of energy into electrical energy.

Example: A pressure sensor detects pressure (a mechanical form of energy) and converts it to electrical signal for display.

¬ A sensor is a device that receives a stimulus (measurand) and responds with an electrical signal.

¬ A sensor may have several energy conversion steps before it produces and outputs an electrical signal, since most of stimuli are not electrical.

## Transducers:

**What is a Transducer**:

♣ A device that converts a signal from one physical form to a corresponding signal having a different physical form.

♣ Transducer is a converter of any one type of energy into another.

♣ Transducers may be used as actuators in various systems.

♣ An example of a transducer is a loudspeaker, which converts an electrical signal into a variable magnetic field (acoustic waves).

## Actuators

Another type of transducer that you will encounter in many IoT systems is an actuator. In simple terms, an actuator operates in the reverse direction of a sensor. It takes an electrical input and turns it into physical action. For instance, an electric motor, a hydraulic system, and a pneumatic system are all different types of actuators.

### Transducers: sensors and actuators

### Sensor: an input transducer (i.e., a microphone)

### Actuator: an output transducer (i.e., a loudspeaker)

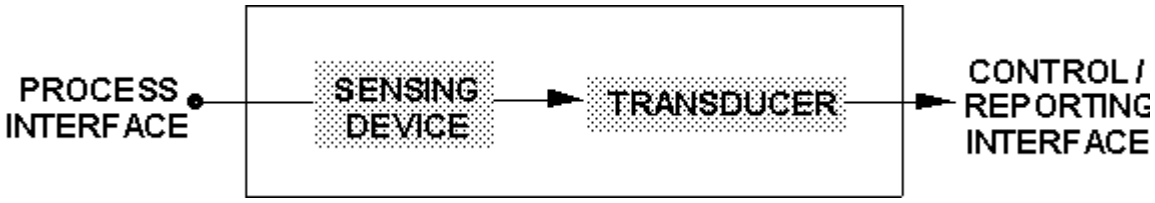
# Sensing in IoT

### Definition

A **sensor detects** (senses) changes in the **ambient conditions** or in the state of another device or a system, and forwards or processes this information in a certain manner.
"A device which detects or measures a physical property and record, indicates, or otherwise responds to it"

## Sensors

They perform some input functions by sensing or feeling the physical changes in characteristics of a system in response to a stimuli.
For example heat is converted to electrical signals in a temperature sensor, or atmospheric pressure is converted to electrical signals in a barometer.




The structure of a sensor

## Transducers

Transducers convert or transduce energy of one kind into another.
For example, in a sound system, a microphone (input device) converts sound waves into electrical signals for an amplifier to amplify (a process), and a loudspeaker (output device) converts these electrical signals back into sound waves.

## Sensor vs. Transducer

The word "Transducer" is the collective term used for both **Sensors** which can be used to sense a wide range of different energy forms such as movement, electrical signals, radiant energy, thermal or magnetic energy etc., And **Actuators** which can be used to switch voltages or current.

### Sensor Features

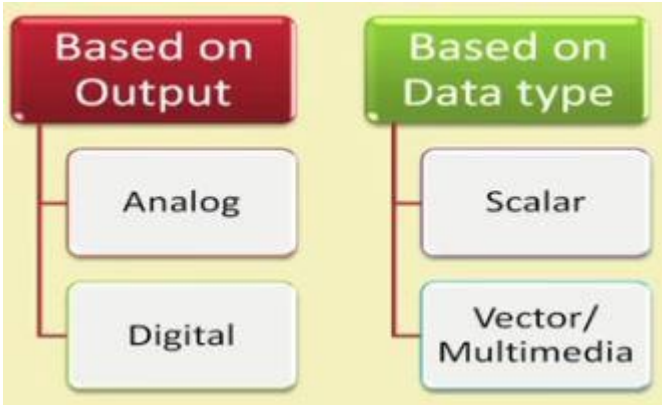
**It is only sensitive to the measured property (e.g., A temperature sensor senses the ambient temperature of a room.)**

- **It is insensitive to any other property likely to be encountered in its application (e.g., A temperature sensor does not bother about light or pressure while sensing the temperature.)**
- **It does not influence the measured property (e.g., measuring the temperature does not reduce or increase the temperature).**

## Sensor Resolution

- The resolution of a sensor is the smallest change it can detect in the quantity that it is measuring.
- The resolution of a sensor with a digital output is usually the smallest resolution the digital output it is capable of processing.
- The more is the resolution of a sensor, the more accurate is its precision.
- A sensor's accuracy does not depend upon its resolution.

# Sensor Classes




### Analog Sensors

- Analog Sensors produces a continuous output signal or voltage which is generally proportional to the quantity being measured.
- Physical quantities such as Temperature, speed, Pressure, Displacement, Strain etc. are all analog quantities as they tend to be continuous in nature.
- For example, the temperature of a liquid can be measured using a thermometer or thermocouple (e.g. in geysers) which continuously responds to temperature changes as the liquid is heated up or cooled down.

### Digital Sensors

- Digital Sensors produce discrete output voltages that are a digital representation of the quantity being measured.

- Digital sensors produce a binary output signal in the form of a logic "1" or a logic "0" , ("ON" or "OFF).
- Digital signal only produces discrete (non-continuous) values, which may be output as a signal "bit" (serial transmission), or by combing the bits to produce a signal "byte" output (parallel transmission).

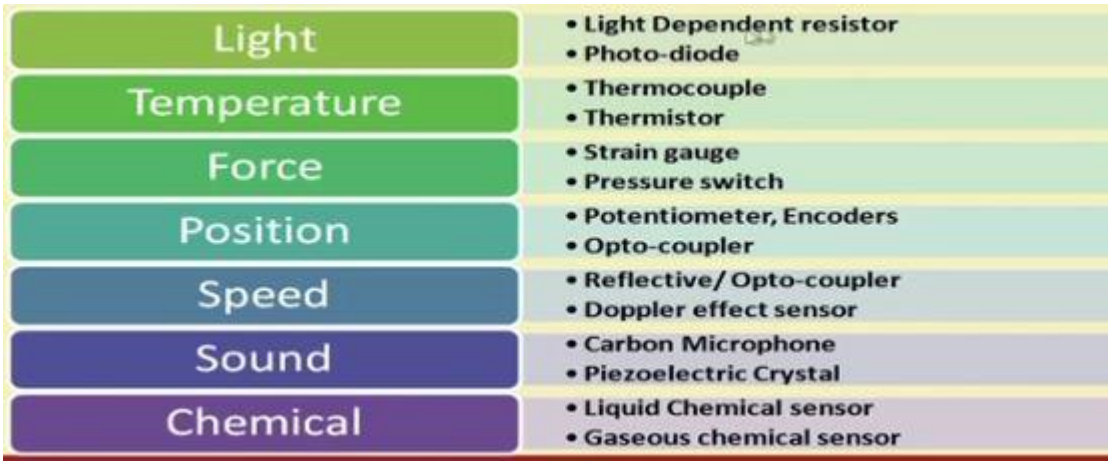
## Scalar Sensors

- Scalar Sensors produce output signal or voltage which generally proportional to the magnitude of the quantity being measured.
- Physical quantities such as temperature, color, pressure, strain, etc. are all scalar quantities as only their magnitude is sufficient to convey an information.
- For example the temperature of a room can be measured using thermometer or thermocouple, which responds to temperature changes irrespective of the orientation of the sensor or its direction.

## Vector Sensors

- Vector Sensors produce output signal or voltage which generally proportional to the magnitude, direction, as well as the orientation of the quantity being measured.
- Physical quantities such as sound, image, velocity, acceleration, orientation, etc. are all vector quantities, as only their magnitude is not sufficient to convey the complete information.
- For example, the acceleration of a body can be measured using an accelerometer, which gives the components of acceleration of the body with respect to the x,y,z coordinate axes.

## Types of sensors :




### Temperature sensors

Temperature sensors detect the temperature of the air or a physical object and concert that temperature level into an electrical signal that can be calibrated accurately reflect the measured temperature. These sensors could monitor the temperature of the soil to help with agricultural output or the temperature of a bearing operating in a critical piece of equipment to sense when it might be overheating or nearing the point of failure.

### Pressure sensors

Pressure sensors measure the pressure or force per unit area applied to the sensor and can detect things such as atmospheric pressure, the pressure of a stored gas or liquid in a sealed system such as tank or pressure vessel, or the weight of an object.

### Image sensors

Image sensors function to capture images to be digitally stored for processing. License plate readers are an example, as well as facial recognition systems. Automated production lines can use image sensors to detect issues with quality such as how well a surface is painted after leaving the spray booth.

### Proximity sensors

Proximity sensors can detect the presence or absence of objects that approach the sensor through a variety of different technology designs. These approaches include:

- Inductive technologies which are useful for the detection of metal objects
- Capacitive technologies, which function on the basis of objects having a different dielectric constant than that of air
- Photoelectric technologies, which rely on a beam of light to illuminate and reflect back from an object, or

- Ultrasonic technologies, which use a sound signal to detect an object nearing the sensor

### Chemical sensors

Chemical sensors are designed to detect the presence of specific chemical substances which may have inadvertently leaked from their containers into spaces that are occupied by personnel and are useful in controlling industrial process conditions.

### Smoke sensors

Smoke sensors or detectors pick up the presence of smoke conditions which could be an indication of a fire typically using optical sensors (photoelectric detection) or ionization detection.

### Infrared (IR) sensors

Infrared sensor technologies detect infrared radiation that is emitted by objects. Non-contact thermometers make use of these types of sensors as a way of measuring the temperature of an object without having to directly place a probe or sensor on that object. They find use in analyzing the heat signature of electronics and detecting blood flow or blood pressure in patients

# Characteristics of Sensors

It is the minimum step size within the range of measurement of a sensor in a wire-wound potentiometer, it will be equal to resistance of one turn of wire. In digital devices with _n‘bits, resolution is _Full range/2n

**Sensitivity:**

It is defined as the change in output response divided by the change in input response.

Highly sensitive sensors show larger fluctuations in output as a result of fluctuations in input.

**Linearity:**

It represents the relationship between input variations and output variations.

In a sensor with linear output, any change in input at any level within the range will produce the same change in output.

**Range:**

It is the difference between the smallest and the largest outputs that a sensor can provide, or the difference between the smallest and largest inputs with which it can operate properly.

**Response time:**

It is the time that a a certainsensor‘spercentage output of total change.

It is also defined as the time required to observe the change in output as a result of change in input for example, ordinary mercury thermometer response time and digital thermometer response time.

**Frequency response:**

The frequency response is the range i to the input remains relatively high.

The larger the range of frequency response, the better the ability of the system to respond to varying input.

**Reliability:**

It is the ratio between the number of times a system operates properly and the number of times it is tried.

For continuous satisfactory operation, it is necessary to choose reliable sensors that last long while considering the cost as well as other requirements.

**Accuracy:**

It shows how close the output of the sensor is to the expected value.

For a given input, certain expected output value is related to how close the sensor‘s output value is to this value.

**Repeatability:**

is poor.

Also, a specific range is desirable for operational performance as the performance of robots depends on sensors.

Repeatability is a random phenomenon and hence there is no compensation.

**Interfacing:**

Direct interfacing of the sensor to the microcontroller/microprocessor is desirable while some add-on circuit may be necessary in certain special sensors.

The type of the sensor output is equally important. An ADC is required for analogue output sensors for example, potentiometer output to microcontroller.

**Size, weight and volume:**

Size is a critical consideration for joint displacement sensors.

When robots are used as dynamic machines, weight of the sensor is important.

Volume or spaces also critical to micro robots and mobile robots used for surveillance.

Cost is important especially when quantity involved is large in the end application.

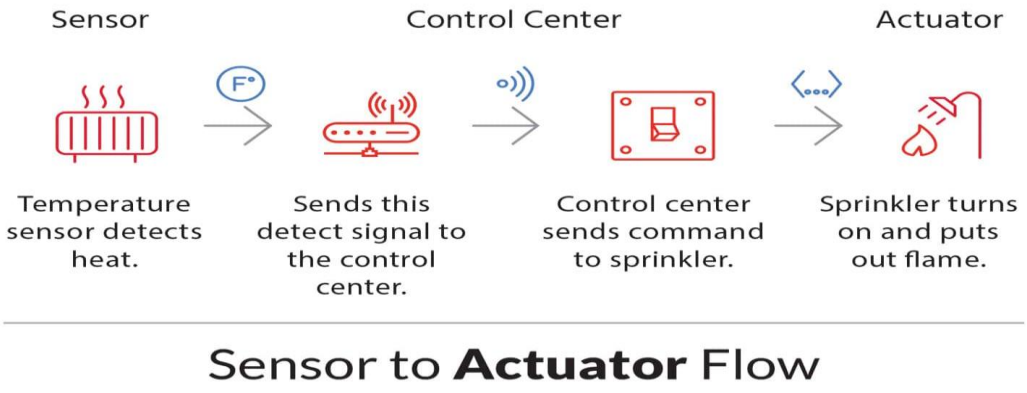
# ACTUATORS

## Actuators

Another type of transducer that you will encounter in many IoT systems is an actuator. In simple terms, an actuator operates in the reverse direction of a sensor. It takes an electrical input and turns it into physical action. For instance, an electric motor, a hydraulic system, and a pneumatic system are all different types of actuators.

## Controller

In a typical IoT system, a sensor may collect information and route to a control center. There, previously defined logic dictates the decision. As a result, a corresponding command controls an actuator in response to that sensed input. Thus, sensors and actuators in IoT work together from opposite ends. Later, we will discuss where the control center resides in the greater IoT system.

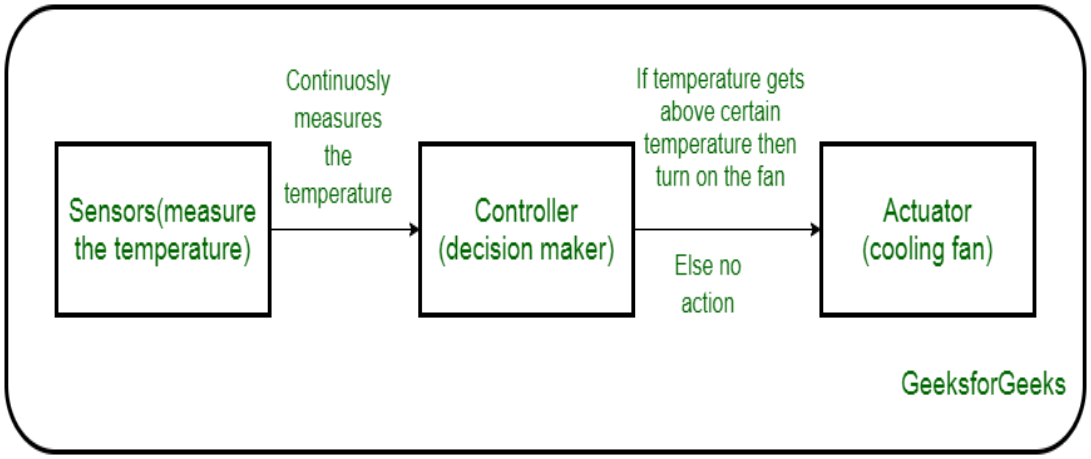



Sensor to **Actuator** Flow

**An IoT device is made up of a Physical object (“thing”) + Controller (“brain”) + Sensors + Actuators + Networks (Internet). An actuator is a machine component or system that moves or controls the mechanism or the system. Sensors in the device sense the environment, then control signals are generated for the actuators according to the actions needed to perform.**

**A servo motor is an example of an actuator. They are linear or rotatory actuators, can move to a given specified angular or linear position. We can use servo motors for IoT applications and make the motor rotate to 90 degrees, 180 degrees, etc., as per our need.**

**The following diagram shows what actuators do, the controller directs the actuator based on the sensor data to do the work.**




*Working of IoT devices and use of Actuators*

The control system acts upon an environment through the actuator. It requires a source of energy and a control signal. When it receives a control signal, it converts the source of energy to a mechanical operation. On this basis, on which form of energy it uses, it has different types given below.

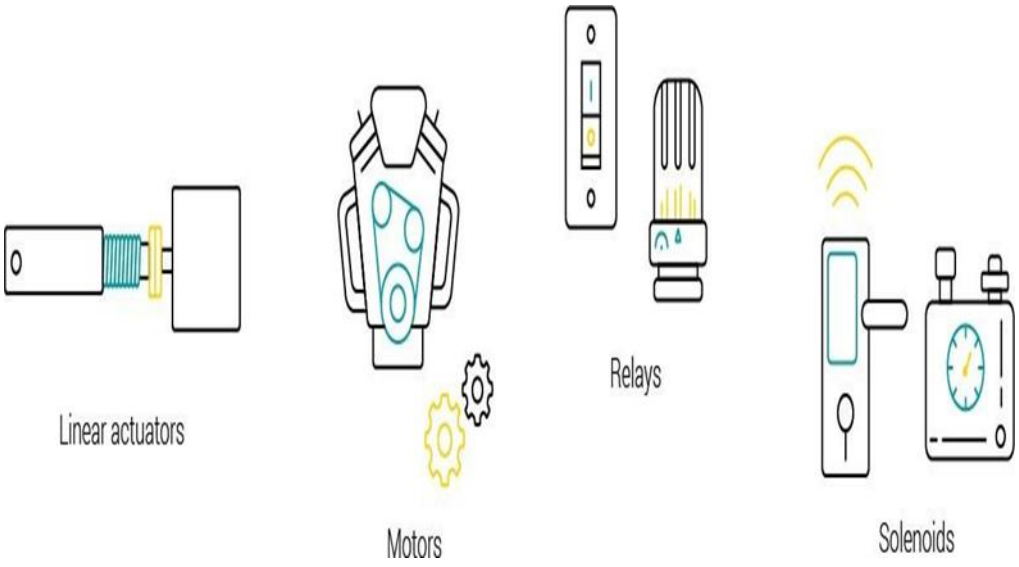
# IoT actuator types

Actuators, as the name itself suggests, can act on their immediate environment toenable correct operation of the machines or devices they are embedded into.
Small as they are, they are rarely visible during operation, but the effects of theirwork can be felt in vehicles, industrial machines or any other electronic equipment involving automation technologies. They can be separated into four main categories based on their construction pattern and the role they play in a specific IoT environment:

- **Linear actuators** – these are used to enable motion of objects or elements in a straight line.
- **Motors** – they enable precise rotational movements of device components or whole objects.
- **Relays** – this category includes electromagnet-based actuators to

operate power switches in lamps, heaters or even smart vehicles.

- **Solenoids** – most widely used in home appliances as part of locking or triggering mechanisms, they also act as controllers in IoT-based gas and water leak monitoring systems.



## Types of Actuators :

**. Hydraulic Actuators –**

A hydraulic actuator uses hydraulic power to perform a mechanical operation. They are actuated by a cylinder or fluid motor. The mechanical motion is converted to rotary, linear, or oscillatory motion, according to the need of the IoT device. Ex- construction equipment uses hydraulic actuators because hydraulic actuators can generate a large amount of force.

**Advantages :**

- Hydraulic actuators can produce a large magnitude of force and high speed.
- Used in welding, clamping, etc.
- Used for lowering or raising the vehicles in car transport carriers.

**Disadvantages :**

- Hydraulic fluid leaks can cause efficiency loss and issues of cleaning.
- It is expensive.
- It requires noise reduction equipment, heat exchangers, and high maintenance systems.

**2. Pneumatic Actuators –**

A pneumatic actuator uses energy formed by vacuum or compressed air at high pressure to convert into either linear or rotary motion. Example- Used in robotics, use sensors that work like human fingers by using compressed air.

**Advantages :**

- They are a low-cost option and are used at extreme temperatures where using air is a safer option than chemicals.
- They need low maintenance, are durable, and have a long operational life.
- It is very quick in starting and stopping the motion.

**Disadvantages :**

- Loss of pressure can make it less efficient.
- The air compressor should be running continuously.
- Air can be polluted, and it needs maintenance.

**3. Electrical Actuators –**

An electric actuator uses electrical energy, is usually actuated by a motor that converts electrical energy into mechanical torque. An example of an electric actuator is a solenoid based electric bell.

**Advantages :**

- It has many applications in various industries as it can automate industrial valves.
- It produces less noise and is safe to use since there are no fluid leakages.
- It can be re-programmed and it provides the highest control precision positioning.

**Disadvantages :**

- It is expensive.
- It depends a lot on environmental conditions.

**Other actuators are** –

- **Thermal/Magnetic Actuators –**
  These are actuated by thermal or mechanical energy. Shape Memory Alloys (SMAs) or Magnetic

Shape-Memory Alloys (MSMAs) are used by these actuators. An example of a thermal/magnetic actuator can be a piezo motor using SMA.

- **Mechanical Actuators –**
  A mechanical actuator executes movement by converting rotary motion into linear motion. It involves pulleys, chains, gears, rails, and other devices to operate. Example – A crankshaft.
- Soft Actuators
- Shape Memory Polymers
- Light Activated Polymers
- With the expanding world of IoT, sensors and actuators will find more usage in commercial and domestic applications along with the pre-existing use in industry

# SENSOR NETWORKS

A wireless **sensor network** (WSN) is a **network** formed by a large number of **sensor** nodes where each node is equipped with a **sensor** to detect physical phenomena such as light, heat, pressure, etc. ... With the rapid technological development of **sensors**, WSNs will become the key technology for **IoT**.

## Applications of wireless sensor network

Wireless sensor networks have gained considerable popularity due to their flexibility in solving problems in different application domains and have the potential to change our lives in many different ways. WSNs have been successfully applied in various application domains

**Military applications**: Wireless sensor networks be likely an integral part of military command, control, communications, computing, intelligence, battlefield surveillance, reconnaissance and targeting systems.

**Area monitoring**: In area monitoring, the sensor nodes are deployed over a region where some phenomenon is to be monitored. When the sensors detect the event being monitored (heat, pressure etc), the event is reported to one of the base stations, which then takes appropriate action.

**Transportation**: Real-time traffic information is being collected by WSNs to later feed transportation models and alert drivers of congestion and traffic problems.

**Health applications**: Some of the health applications for sensor networks are supporting interfaces for the disabled, integrated patient monitoring, diagnostics, and drug administration in hospitals, tele-monitoring of human physiological data, and tracking & monitoring doctors or patients inside a hospital.

**Environmental sensing**: The term Environmental Sensor Networks has developed to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests etc. Some other major areas are listed below:

- Air pollution monitoring
- Forest fires detection
- Greenhouse monitoring

- Landslide detection

**Structural monitoring**: Wireless sensors can be utilized to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc enabling Engineering practices to monitor assets remotely with out the need for costly site visits.

**Industrial monitoring**: Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring.

**Agricultural sector**: using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Irrigation automation enables more efficient water use and reduces waste.

## Structure of a wireless sensor network

Structure of a Wireless Sensor Network includes different topologies for radio communications networks.

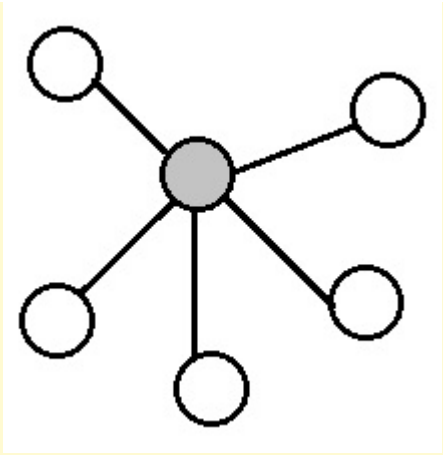
1.Star Network

2.MeshNetwork

3.HybridStar-MeshNetwork

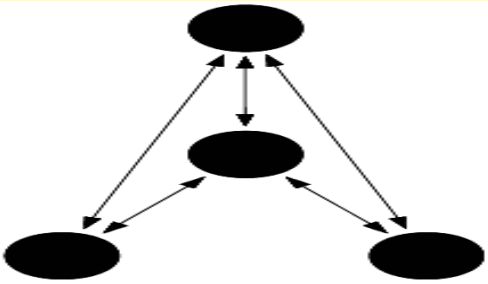
### 1.Star network (single point-to-multipoint)

A star network is a communications topology where a single base station can send and/or receive a message to a number of remote nodes. The remote nodes are not permitted to send messages to each other. The advantage of this type of network for wireless sensor networks includes simplicity, ability to keep the remote node's power consumption to a minimum. It also allows low latency communications between the remote node and the base station. The disadvantage of such a network is that the base station must be within radio transmission range of all the individual nodes and is not as robust as other networks due to its dependency on a single node to manage the network.



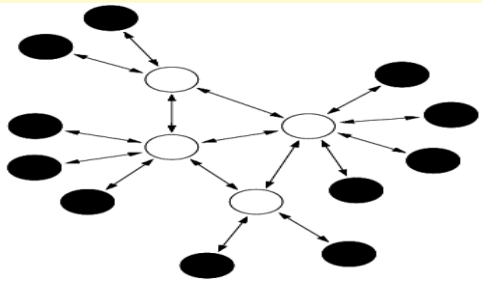
**2.**Mesh network **:**

A mesh network allows transmitting data to one node to other node in the network that is within its radio transmission range. This allows for what is known as multi-hop communications, that is, if a node wants to send a message to another node that is out of radio communications range, it can use an intermediate node to forward the message to the desired node. This network topology has the advantage of redundancy and scalability. If an individual node fails, a remote node still can communicate to any other node in its range, which in turn, can forward the message to the desired location. In addition, the range of the network is not necessarily limited by the range in between single nodes; it can simply be extended by adding more nodes to the system. The disadvantage of this type of network is in power consumption for the nodes that implement the multi-hop communications are generally higher than for the nodes that don't have this capability, often limiting the battery life. Additionally, as the number of communication hops to a destination increases, the time to deliver the message also increases, especially if low power operation of the nodes is a requirement.



## 3.Hybrid star – Mesh network

A hybrid between the star and mesh network provides a robust and versatile communications network, while maintaining the ability to keep the wireless sensor nodes power consumption to a minimum. In this network topology, the sensor nodes with lowest power are not enabled with the ability to forward messages. This allows for minimal power consumption to be maintained. However, other nodes on the network are enabled with multi-hop capability, allowing them to forward messages from the low power nodes to other nodes on the network. Generally, the nodes with the multi-hop capability are higher power, and if possible, are often plugged into the electrical mains line. This is the topology implemented by the up and coming mesh networking standard known as ZigBee.

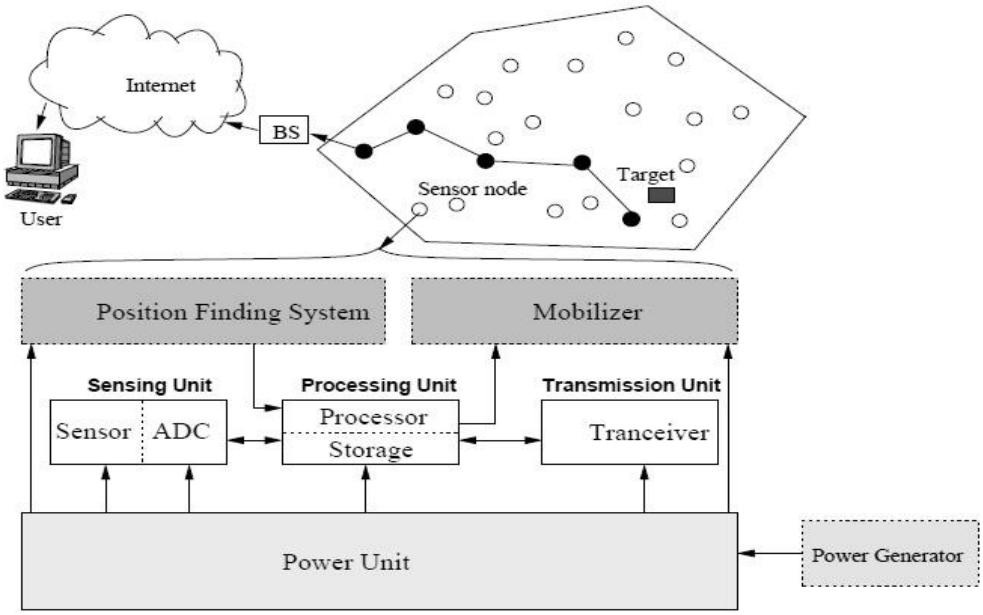


## Structure of a wireless sensor node

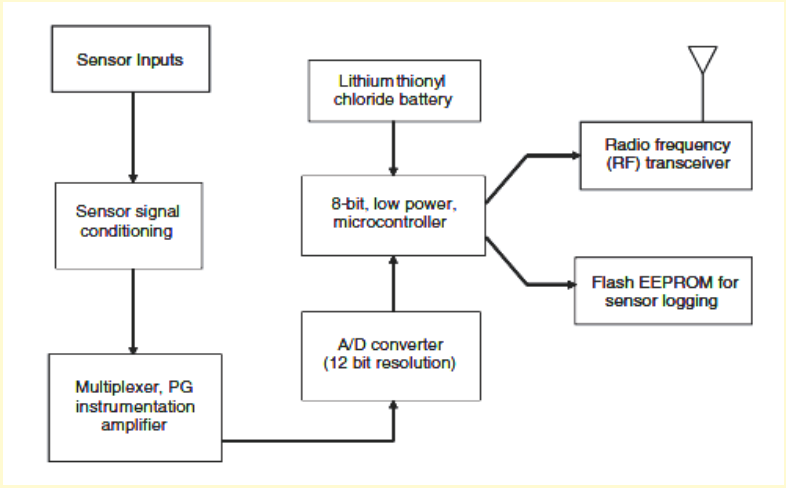
A sensor node is made up of four basic components such as sensing unit, processing unit, transceiver unit and a power unit which is shown in Fig. 5. It also has application dependent additional components such as a location finding system, a power generator and a mobilizer. Sensing units are usually composed of two subunits: sensors and analogue to digital converters (ADCs) (Akyildiz et al., 2002). The analogue signals produced by the sensors are converted to digital signals by the ADC, and then fed into the processing unit. The processing unit is generally associated with a small storage unit and it can manage the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to the network. One of the most important components of a sensor node is the power unit. Power units can be supported by a power scavenging unit such as solar cells. The other subunits, of the node are application dependent.

A functional block diagram of a versatile wireless sensing node is provided in Fig. 6. Modular design approach provides a flexible and versatile platform to address the needs of a wide variety of applications. For example, depending on the sensors to be deployed, the signal conditioning block can be re-programmed or replaced. This allows for a wide variety of different sensors to be used with the wireless sensing node. Similarly, the radio link may be swapped out as required

for a given applications' wireless range requirement and the need for bidirectional communications.




The components of a sensor node




Functional block diagram of a sensor node

Using flash memory, the remote nodes acquire data on command from a base station, or by an event sensed by one or more inputs to the node. Moreover, the embedded firmware can be upgraded through the wireless network in the field.

The microprocessor has a number of functions including:

- Managing data collection from the sensors
- performing power management functions
- interfacing the sensor data to the physical radio layer
- managing the radio network protocol

A key aspect of any wireless sensing node is to minimize the power consumed by the system. Usually, the radio subsystem requires the largest amount of power. Therefore, data is sent over the radio network only when it is required. An algorithm is to be loaded into the node to determine when to send data based on the sensed event. Furthermore, it is important to minimize the power consumed by the sensor itself. Therefore, the hardware should be designed to allow the microprocessor to judiciously control power to the radio, sensor, and sensor signal conditioner

# BASICS OF NETWORKING

Switches, routers, and wireless access points are the essential **networking basics**. Through them, devices connected to your **network** can communicate with one another and with other **networks**, like the Internet. Switches, routers, and wireless access points perform very different functions in a **network**.

## switches

**Switches** are the foundation of most business networks. A switch acts as a controller, connecting computers, printers, and servers to a network in a building or acampus.

Switches allow devices on your network to communicate with each other, as well aswith other networks, creating a network of shared resources. Through information sharing and resource allocation, switches save money and increase productivity.

There are two basic types of switches to choose from as part of your networkingbasics: on-premises and cloud-managed.

- A managed on-premises switch lets you configure and monitor your LAN, giving youtighter control of your network traffic.
- Have a small IT team? A cloud-managed switch can simplify your network management. You get a simple user interface, multisite full-stack management, and automatic updatesdelivered directly to the switch.

### ROUTERS

- Routers connect multiple networks together. They also connect computers on those networks to the Internet. Routers enable all networked computers to share a single Internet connection, which saves money.
- A router acts a dispatcher. It analyzes data being sent across a network, chooses the best route for data to travel, and sends it on its way.
- Routers connect your business to the world, protect information from security threats, and can even decide which computers receive priority over others.
- Beyond those basic networking functions, routers come with additional features to make networking easier or more secure. Depending on your security needs, for example, you can choose a router with a firewall, a virtual private network (VPN), or an Internet Protocol (IP) communications system.

## ACCESS POINT

An access point* allows devices to connect to the wireless network without cables. A wireless network makes it easy to bring new devices online and provides flexible support to mobile workers.

An access point acts like an amplifier for your network. While a router provides the bandwidth, an access point extends that bandwidth so that the network can support many devices, and those devices can access the network from farther away.

## WIRELESS NETWORKING

To create your wireless network, you can choose between three types of deployment: centralized deployment, converged deployment, and cloud-based deployment

### 1. Centralized deployment

The most common type of wireless network system, centralized deployments are traditionally used in campuses where buildings and networks are in close proximity. This deployment consolidates the wireless network, which makes upgrades easier and facilitates advanced wireless functionality. Controllers are based on-premises and are installed in a centralized location.

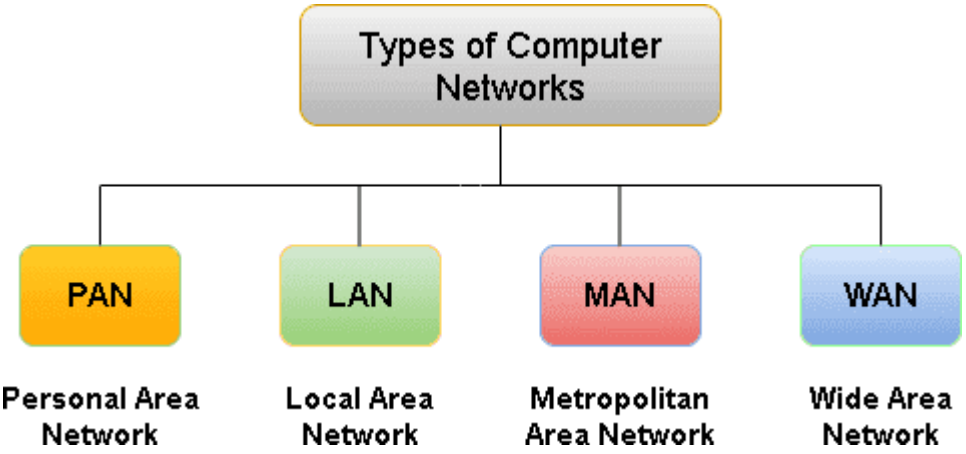
### 2. Converged deployment

For small campuses or branch offices, converged deployments offer consistency in wireless and wired connections. This deployment converges wired and wireless on one network device—an access switch—and performs the dual role of both switch and wireless controller.

### 3. Cloud-based deployment

This system uses the cloud to manage network devices deployed on-premises at different locations. The solution requires Cisco Meraki cloud-managed devices, which provide full visibility of the network through their dashboards.

## Types of Networks in Use Today




### 1. Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and aremanaged by one person or organization from a single device.

### 2. Local Area Network (LAN)

LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximityto each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidlyand safely transfer data.

### 3. Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either asingle person or company (a local council, a large company, etc.).

**Wide Area Network (WAN)**

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're milesapart.

This concepts also related to Basics of Networking

| |
|---|
| IOT protocols |
| Communication models |
| Communication Api's |