Sensor Technology:

- A sensor can sense a change in physical parameters, such as temperature, pressure, light, smoke, and proximity to an object and also sense acceleration, orientation, location, vibrations.
- A microphone senses the voices and changes in the sound, and is used to record voice or music.
- A sensor converts physical energy like heat, sound, pressure, vibrations and motions into electrical energy.
- An electronic circuit connects to the input at a sensor.
- The circuit receives the output of the sensor.
- The circuit receives energy in form of variations through currents, voltages and frequencies.

1. Analog Sensors:

- They produce continuous analog output signals.
- Analog sensors measure the variations in the parameters with respect to a reference and provide the value of sensed parameter after appropriate calculations.
- It includes temperature, moisture, pressure, light, sound, etc.

2. Digital Sensors:

- Here data conversion and transmission takes place digitally.
- Signals are converted into digital format by the sensor itself.
- These signals are transmitted digitally through wire.
- In digital sensors, change of states is sensed in the form of 0s and 1s.
- It includes IR (infrared sensor), ultrasonic, float, moisture sensors, etc.

Point of difference	IOT	M2M
Full form	Internet of Things	Machine to Machine
Intelligence	IOT devices have objects that are responsible for decision making	Some degree of intelligence is observed in this.
Connection type used	The connection is via Network and using various communication types.	The connection is a point to point
Communication protocol used	Internet protocols are used such as HTTP, FTP, and Telnet.	Traditional protocols and communication technology techniques are used
Data Sharing	Data is shared between other applications that are used to improve the end-user experience.	Data is shared with only the communicating parties.
Internet	Internet connection is required for communication	Devices are not dependent on the Internet.
Type of Communication	It supports cloud communication	It supports point-to-point communication.
Computer System	Involves the usage of both Hardware and Software.	Mostly hardware-based technology
Scope	A large number of devices yet scope is large.	Limited Scope for devices.
Business Type used	Business 2 Business(B2B) and Business 2 Consumer(B2C)	Business 2 Business (B2B)
Open API support	Supports Open API integrations.	There is no support for Open APIs

c. Availability:

- It ensures that only authorized users can have access to the information as and when it is required. Including the fault tolerance.
- Fault tolerance can be built into the IOT architecture by ensuring that the backup components are present for each of the component (i.e. server, storage, networks).
- It also ensures that the **backup server** is an identical copy of the primary server so that backup server can immediately take over the role of primary server whenever they fail.
- **Storage backup** can be ensured by using highly scalable RAID (Redundant Array of Independent Disks) architecture where duplicate data is striped and mirrored across the multiple hard disk, so even if one disk fails the data would not be lost and be there on some other disk.
- Fault tolerance in **networks** can be ensured by providing multiple switches, ports and cables between the two connecting endpoints. This will ensure that the failure of any one network component will not harm the transfer of data over the network.

Security in IOT:

1. CIA Triad:

a. Confidentiality:

- It ensures that only authorized users will have the access to the underlying information.
- It ensures the privacy by preventing unauthorized access to the information which is stored and transmitted using the IOT infrastructure.

b. Integrity:

- It ensures that only authorized users are allowed to modify the stored information.
- It makes sure that unauthorized users will not be allowed to change (i.e. read, write, delete or update) the data in any manner at any time.

2. AAA Framework:

a. Authentication:

- It checks that a user's credentials are valid, so the users with invalid credentials will not be allowed to access the information.
- Most common form of authentication can be by using user names and passwords, but as the hacking techniques are evolving so the authentication techniques also have to be sophisticated.
- Thus **multi-factor authentication** comes into picture, where it uses a combination of parameters to authenticate user credentials.
- Ex: 1st factor: user name and password, 2nd factor: a secret random key is being generated which is only known to the user, 3rd factor: verifying biometrics (i.e. fingerprint scan, iris recognition, face recognition, voice detection, etc.)
- Multi-factor authentication could use multiple ways to verify user credentials.
- Sometimes it may be done using only two factors, and thus it is termed as **"two-factor authentication"**.

b. Authorization:

- It ensures that a specific user has rights to perform specific operations on a specific object, by providing different permissions.
- The permissions are granted to the user based on their role in the organization.
- The permissions could be as follows:
  - Read only: the user can only view/read the data.
  - Read & Write: the user can view, add, update and delete the data.

c. Audit Trial:

- It is an activity conducted periodically to assess the effectiveness of the security measures by keeping an audit log.
- **Audit log** keeps a track of the operations that are performed by the different users.

IOT enabling techniques:

- IOT enabling techniques are as follows:
  - Wireless Sensor Network (WSN)
  - Cloud Computing
  - Big Data Analytics
  - Communication Protocols
  - Embedded Systems

Characteristics of the Internet of Things :
There are the following characteristics of IoT as follows. Let's discuss it one by one.

1.Connectivity–
Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, connection between people through internet devices like mobile phones ,and other gadgets, also connection between Internet devices such as routers, gateways, sensors, etc.

2.Intelligence and Identity–

The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

3.Scalability–
The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.

4.Dynamic and Self-Adapting (Complexity) –

IoT devices should dynamically adapt themselves to the changing contexts and scenarios. Assume a camera meant for the surveillance. It should be adaptable to work in different conditions and different light situations (morning,afternoon,night).

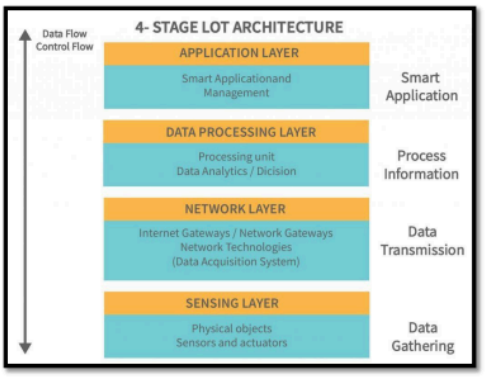
5.Architecture–
IoT architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturers ' products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.

6.Safety–
There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at the risk. Therefore, equipment safety is also critical.

7.Self Configuring –
This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

Component of IOT:

1. **Control Unit:**
   - A small computer containing processor, memory, programmable IO peripheral and the control unit responsible for main operation.
2. **Sensor:**
   - A device that can measure a physical quantity and convert it into a signal which will be read and interpreted by the microcontroller unit.
   - Most of the sensors are categorized into two categories: Digital Sensors or Analog Sensors.
3. **Communication Modules:**
   - These part of the device is responsible for communication with the rest of the IOT platform.
   - It provides connectivity depending on whether it is wired or wireless communication.
4. **Power Sources:**
   - It provides power to the device by passing current which generated by the sources like batteries, solar cells, etc.



. Sensing Layer –

- Sensors, actuators, devices are present in this Sensing layer.
- These Sensors or Actuators accepts data (physical/environmental parameters), processes data and then emits data over network.

. Network Layer –

- Internet gateways, Network gateways, Data Acquisition System (DAS) are present in this layer.
- DAS performs data aggregation and conversion function (i.e.collecting data and aggregating data then converting analog data of sensors to digital data etc.).
- Advanced gateways which mainly opens up connection between Sensor networks and Internet also performs many basic gateway functionalities like malware protection, and filtering also sometimes decision making based on inputted data and data management services, etc.

. Data processing Layer –

- This is processing unit of IOT ecosystem. Here data is analyzed and pre-processed before sending it to data center from where data is accessed by software applications often termed as business

1.4.2 IoT Communicational Models

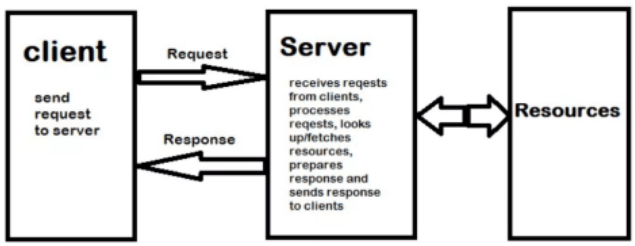
There are several different types of models available in an IoT system that is used to communicate between the system and server like the request-response model, publish-subscribe model, push-pull model, exclusive pair model, etc.

Request-Response Communication Model

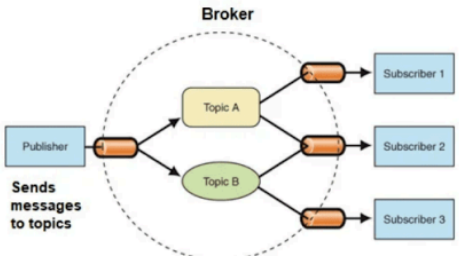
This model is a communication model in which a client sends the request for data to the server and the server responds according to the request. when a server receives a request it fetches the data, retrieves the resources and prepares the response, and then sends the data back to the client.

Publish-Subscribe Communication Model

In this communication model, we have a broker between publisher and consumer. here publishers are the source of data but they are not aware of consumers. they send the data managed by the brokers and when a consumer subscribes to a topic that is managed by the broker and when the broker receives data from the publisher it sends the data to all the subscribed consumers.



Request-Response Communication Model

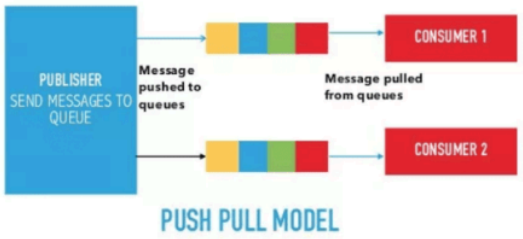


Push-Pull Communication Model

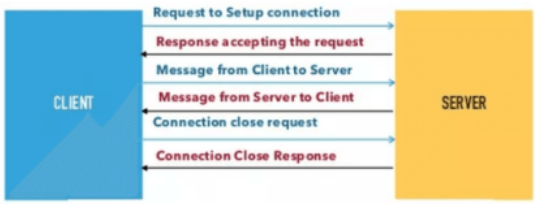
It is a communication model in which the data push by the producers in a queue and the consumers pull the data from the queues. here also producers are not aware of the consumers.

Exclusive Pair Communication Model

It is a bidirectional fully duplex communication model that uses a persistent connection between the client and server. here first set up a connection between the client and the server and remain open until the client sends a close connection request to the server.



PUSH PULL MODEL



EXCLUSIVE PAIR COMMUNICATION MODEL

3.2 Types of sensors and its usage (Temperature, Humidity, Gas Detector, Ultrasonic, Fire detector, Light, Sound, IR, Water Level)

Sensors are designed to respond to specific types of conditions in the physical world, and then generate a signal (usually electrical) that can represent the magnitude of the condition being monitored. Those conditions may be light, heat, sound, distance, pressure, or some other more specific situation, such as the presence or absence of a gas or liquid. The common IoT sensors that will be employed include:

- Temperature sensors
- Pressure sensors
- Motion sensors
- Level sensors
- Image sensors
- Proximity sensors
- Water quality sensors
- Chemical sensors
- Gas sensors
- Smoke sensors
- Infrared (IR) sensors
- Acceleration sensors
- Gyroscopic sensors
- Humidity sensors
- Optical sensors

A description of each of these sensors is provided below.

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.

Types of Actuators :

1. 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.

- 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.

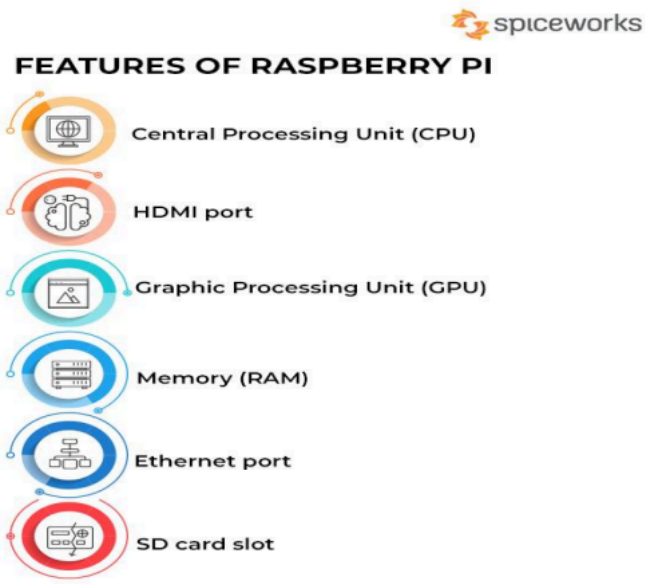
- **Mechanical Actuators –**

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	ACTUATOR
It converts physical characteristics into electrical signals.	It converts electrical signals into physical characteristics.
It takes input from environment.	It takes input from output conditioning unit of system.
It gives output to input conditioning unit of system.	It gives output to environment.
Sensor generated electrical signals.	Actuator generates heat or motion.
It is placed at input port of the system.	It is placed at output port of the system.
It is used to measure the physical quantity.	It is used to measure the continuous and discrete process parameters.
It gives information to the system about environment.	It accepts command to perform a function.
Example: Photo-voltaic cell which converts light energy into electrical energy.	Example: Stepper motor where electrical energy drives the motor.

4.4 Components of Raspberry pi



Basis	Arduino	Raspberry Pi
Software	Arduino boards are programmable using C/C++ languages.	Raspberry Pi supports its own Linux-based operating system Raspberry Pi OS. You can also install the OS you like.
Internet	Arduino does not have internet support. You need additional modules or shields to connect it to the internet.	Raspberry Pi has a built-in Ethernet port and WiFi support.
Cost	Arduino boards are cheaper.	Raspberry Pi boards are expensive.
How they handle power drop	Arduino devices begin executing code when they are turned on. Therefore, when power is turned off, abruptly, you won't end up with a corrupt operating system or errors. The code will simply start again when plugged in.	Raspberry Pi requires the same care as a PC. You have to shut the operating system down properly.
Current drive strength	Higher current drive strength	Lower current drive strength
Capability	Arduino is generally used to perform single (and simple) tasks repeatedly.	Raspberry Pi can perform multiple tasks simultaneously.
Wireless connectivity	Arduino does not support Bluetooth or WiFi.	Raspberry Pi supports Bluetooth and WiFi.
Applications	Traffic light countdown timer, Parking lot counter, Weighing machines, etc.	Robot controller, Game servers, Stop motion cameras, etc.