What is IoT?

The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools.

In other words, the internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business.

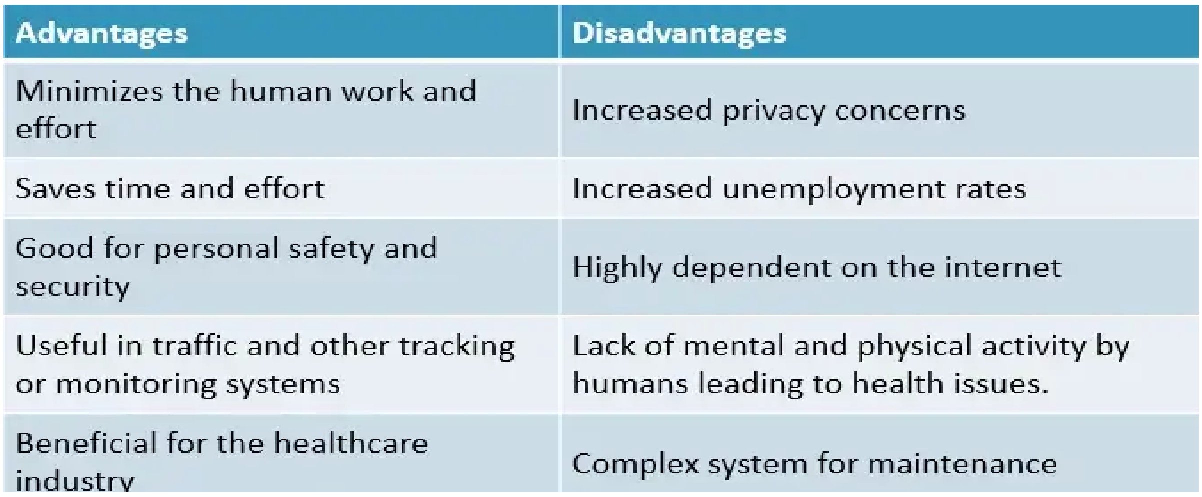
How does IoT work?

An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another. The devices do most of the work without human intervention, although people can interact with the devices to set them up, give them instructions or access the data.

The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

IoT can also make use of artificial intelligence (AI) and machine learning (ML) to aid in making data collecting processes easier and more dynamic.

Advantages & Disadvantages of IoT



Advantages	Disadvantages
Minimizes the human work and effort	Increased privacy concerns
Saves time and effort	Increased unemployment rates
Good for personal safety and security	Highly dependent on the internet
Useful in traffic and other tracking or monitoring systems	Lack of mental and physical activity by humans leading to health issues.
Beneficial for the healthcare industry	Complex system for maintenance

Advantages of IoT

- ability to access information from anywhere at any time on any device;
- improved communication between connected electronic devices;
- transferring data packets over a connected network saving time and money; and
- automating tasks helping to improve the quality of a business's services and reducing the need for human intervention.

Disadvantages of IoT

- As the number of connected devices increases and more information is shared between devices, the potential that a hacker could steal confidential information also increases.
- Enterprises may eventually have to deal with massive numbers of IoT devices, and collecting and managing the data from all those devices will be challenging.
- If there's a bug in the system, it's likely that every connected device will become corrupted.
- Since there's no international standard of compatibility for IoT, it's difficult for devices from different manufacturers to communicate with each other.

Characteristics of the Internet of Things

There are the following characteristics of IoT as follows:

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, the connection between people through internet devices like mobile phones, and other

gadgets, also a 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** – Being dynamic is one of the main characteristics of IoT because it needs to be self-adaptive to understand the changes around it and act accordingly. If we take an example of a camera, it was initially created just to take a photograph; however, later, it has got the feature of adjusting the quality of a photograph according to the light.
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** — The basic idea of IoT is to connect everything to the internet and make the system easier for the users. However, when things are connected to the internet in such a way there is always a danger of the sensitive personal details of the users getting compromised. So safety is undoubtedly a crucial characteristic of IoT.
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.

Physical Design of IoT

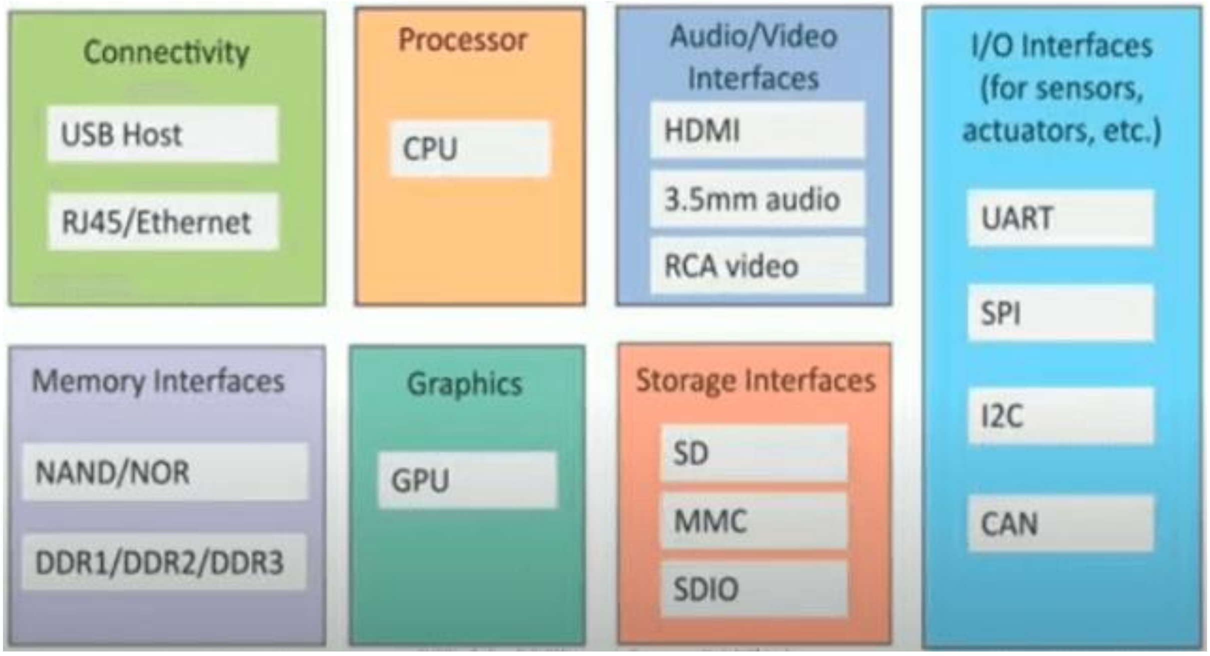
A physical design of an IoT system refers to the individual node devices and their protocols that are utilised to create a functional IoT ecosystem.

Each node device can perform tasks such as remote sensing, actuating, monitoring, etc., by relying on physically connected devices. It may also be capable of transmitting information through different types of wireless or wired connections.

The things/devices in the IoT system are used for:

- Building connections
- Data processing
- Providing storage
- Providing interfaces
- Providing graphical interfaces

The devices generate data, and the data is used to perform analysis and do operations for improving the system. For instance, a moisture sensor is used to obtain the moisture data from a location, and the system analyses it to give an output.



Connectivity: Devices like USB hosts and ETHERNET are used for connectivity between the devices and the server.

Processor: A processor like a CPU and other units are used to process the data. These data are further used to improve the decision quality of an IoT system.

Audio/Video Interfaces: An interface like HDMI and RCA devices is used to record audio and videos in a system.

Input/Output interface: To give input and output signals to sensors, and actuators we use things like UART, SPI, CAN, etc.

Storage Interfaces: Things like SD, MMC, and SDIO are used to store the data generated from an IoT device.

Other things like DDR and GPU are used to control the activity of an IoT system.

Logical Design of IoT

A logical design for an IoT system is the actual design of how its components (computers, sensors, and actuators) should be arranged to complete a particular function. It doesn’t go into the depth of describing how each component will be built with low-level programming specifics.

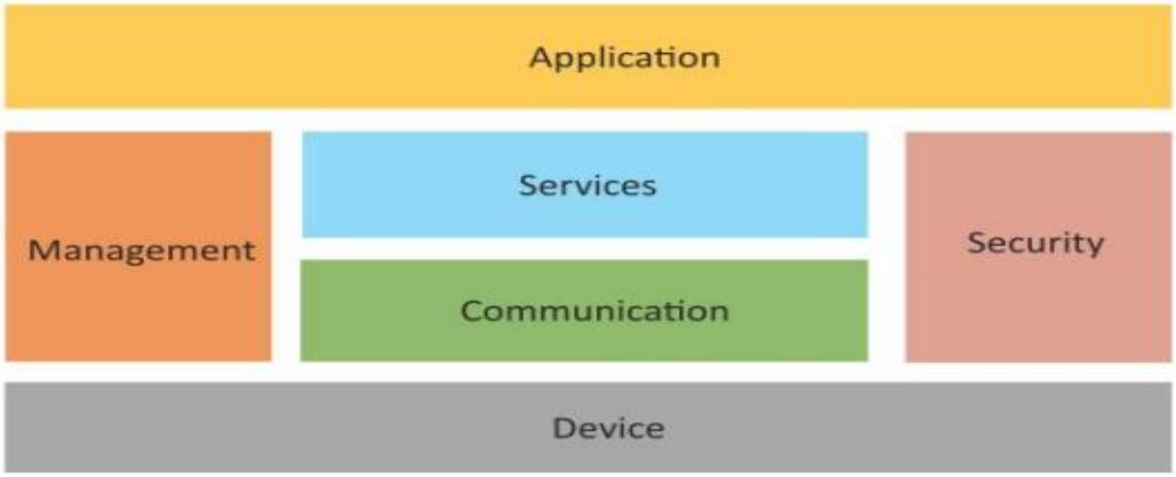
IoT logical design includes:

1. IoT functional blocks
2. IoT communications models
3. IoT communication APIs

1. IoT functional blocks

IoT systems include several functional blocks such as devices, communication, security, services, and application.

The functional blocks provide sensing, identification, actuation, management, and communication capability. These functional blocks consist of devices that handle the communication between the server and the host, enable monitoring control functions, manage the data transfer, secure the IoT system using authentication and different functions, and provide an interface for controlling and monitoring various terms.



The 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 block provides various functions to govern the IoT system.

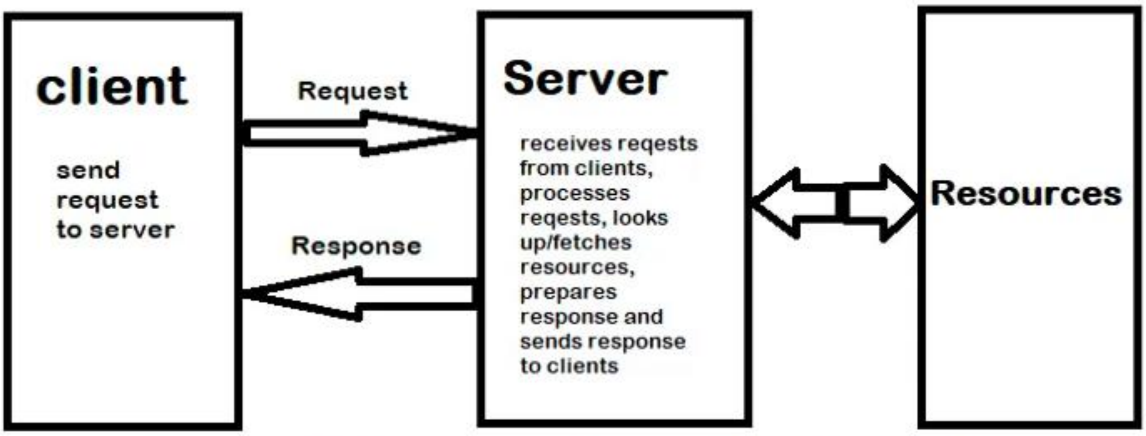
Security: This block secures the IoT system and by providing functions such as authentication, authorization, message and content integrity, and data security.

Application: This is an interface that the users can use to control and monitor various aspects of the IoT system. The application also allows users to view the system status and view or analyze the processed data.

2. IoT Communication Models

There are multiple kinds of models available in an Internet of Things system that is used for communicating between the system and server, such as:

- Request-Response Model

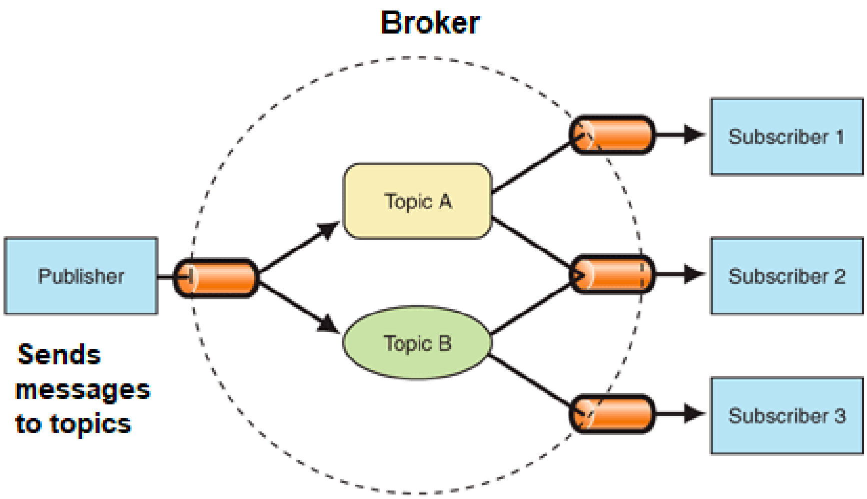

client
send request to server
Request
Response
Server
receives reqests from clients, processes reqests, looks up/fetches resources, prepares response and sends response to clients
Resources

Request-Response Communication Model

Request-response model 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 representation, prepares the response, and then sends the response to the client.

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.

- Publisher-Subscriber Model



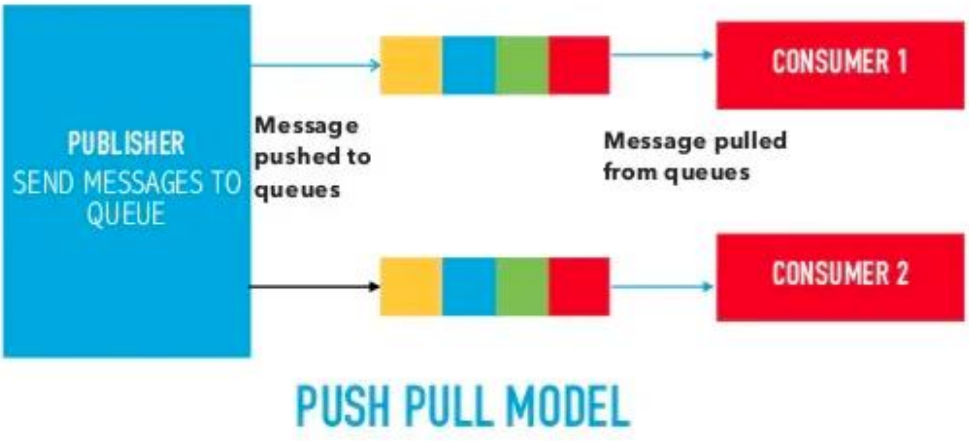
This model comprises three entities: Publishers, Brokers, and Consumers.

Publishers are the source of data. It sends the data to the topic which is managed by the broker. They are not aware of consumers.

Consumers subscribe to the topics which are managed by the broker.

Brokers' responsibility is to accept data from publishers and send it to the appropriate consumers. The broker only has the information regarding the consumer to which a particular topic belongs which the publisher is unaware.

- Push-Pull Model

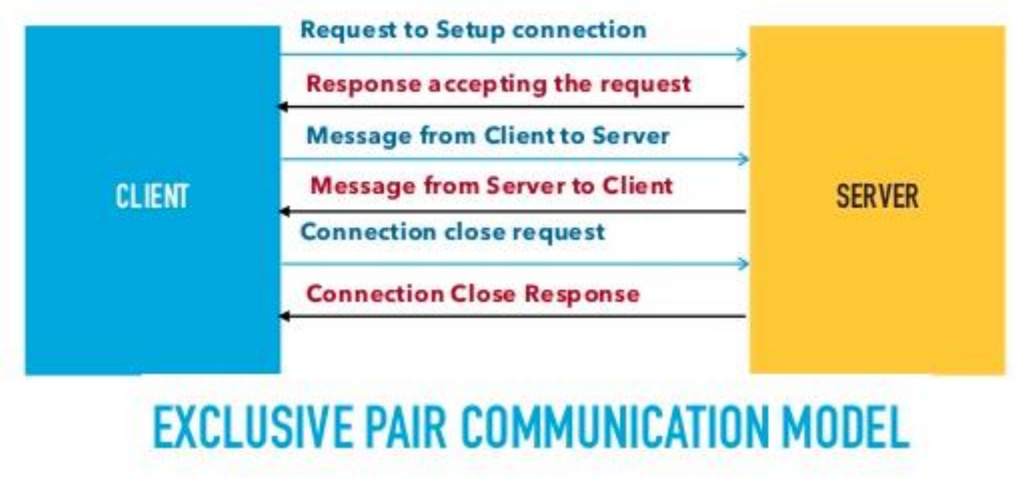


The push-pull model constitutes data publishers, data consumers, and data queues.

Publishers and Consumers are not aware of each other.

Publishers publish the message/data and push it into the queue. The consumers, present on the other side, pull the data out of the queue. Thus, the queue acts as the buffer for the message when the difference occurs in the rate of push or pull of data on the side of a publisher and consumer.

- Exclusive Pair


Request to Setup connection
Response accepting the request
Message from Client to Server
Message from Server to Client
Connection close request
Connection Close Response
CLIENT
SERVER
EXCLUSIVE PAIR COMMUNICATION MODEL

Exclusive Pair is the bi-directional model, including full-duplex communication between client and server. The connection is constant and remains open till the client sends a request to close the connection. The Server has the record of all the connections which has been opened.

3. IoT communication API

In IoT, there are 2 communication APIs –

1. REST-Based Communication API:

REpresentational State Transfer (REST) is a set of architectural principles by which you can design web services and web APIs that focus on a system’s resources and how resource states are addressed and transferred. REST APIs follow the request-response communication model. The REST architectural constraints apply to the components, connectors, and data elements, within a distributed hypermedia system.

2. Web Socket-Based Communication APIs:

Web Socket APIs allow bi-directional, full-duplex communication between clients and servers. It follows the exclusive pair communication model. This Communication API does not require a new connection to be set up for each message to be sent between clients and servers. Once the connection is set up the messages can be sent and received continuously without any interruption. WebSocket APIs are suitable for IoT Applications with low latency or high throughput requirements.

Examples of IoT Devices

- **Activity Trackers**

Smart home security cameras provide alerts and peace of mind. Activity trackers are sensor devices that can monitor and transmit key health indicators in real-time. You can track and manage your blood pressure, physical movement and oxygen levels.

- **Industrial Security and Safety**

IoT enabled detection systems, sensors and cameras can be placed in restricted areas to detect trespassers. They can also identify pressure buildups and small leaks of hazardous chemicals and fix them before they become serious problems.

- **Augmented Reality Glasses**

Augmented Reality (AR) glasses are wearable computer-enabled glasses that help you get extra information such as 3D animations and videos to the user's real-world scenes. The information is presented within the lenses of the glasses and can help users access Internet applications.

- **Motion Detection**

Motion sensors can detect vibrations in buildings, bridges, dams and other large-scale structures. These devices can identify anomalies (inconsistency) and disturbances in the structures that could lead to objectionable failures. They can also be used in areas susceptible to floods, landslides, and earthquakes.

- **Connected cars**

There are many ways vehicles, such as cars, can be connected to the internet. It can be through smart dashcams, infotainment systems, or even the vehicle's connected gateway. They collect data from the accelerator, brakes, speedometer, odometer, wheels, and fuel tanks to monitor both driver performance and vehicle health. Connected cars have a range of uses:

➢ Monitoring rental car groups to increase fuel efficiency and reduce costs.

➢ Helping parents track the driving behavior of their children.

➢ Notifying friends and family automatically in case of a car crash.

➢ Predicting and preventing vehicle maintenance needs.

- **Connected homes**

Smart home devices are mainly focused on improving the efficiency and safety of the house, as well as improving home networking. Home security systems like door locks, security cameras, and water leak detectors can detect and prevent threats, and send alerts to homeowners.

Connected devices for the home can be used for:

➢ Automatically turning off devices not being used.

➢ Rental property management and maintenance.

➢ Finding misplaced items like keys or wallets.

➢ Automating daily tasks like vacuuming, making coffee, etc.

- **Smart cities**

IoT applications have made urban planning and infrastructure maintenance more efficient. Governments are using IoT applications to tackle problems in infrastructure, health, and the environment. IoT applications can be used for:

➢ Measuring air quality and radiation levels.

➢ Reducing energy bills with smart lighting systems.

➢ Detecting maintenance needs for critical infrastructures such as streets, bridges, and pipelines.

➢ Increasing profits through efficient parking management.

- **Smart buildings**

Buildings such as college campuses and commercial buildings use IoT applications to drive greater operational efficiencies. IoT devices can be use in smart buildings for:

➢ Reducing energy consumption.

➢ Lowering maintenance costs.

➢ Utilizing work spaces more efficiently.