INTERNET OF THINGS CONCEPTS

Internet of Things (IoT)

- The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data.
- IoT devices—also known as “smart objects”—can range from simple “smart home” devices like smart thermostats, to wearables like smartwatches and RFID-enabled clothing, to complex industrial machinery and transportation systems.

The internet of things, or IoT, is a network of interrelated devices that connect and exchange data with other IoT devices and the cloud. IoT devices are typically embedded with technology such as sensors and software and can include mechanical and digital machines and consumer objects. IoT to operate more efficiently, deliver enhanced customer service, improve decision-making and increase the value of the business.

IoT enables these smart devices to communicate with each other and with other internet-enabled devices. Like smartphones and gateways, creating a vast network of interconnected devices that can exchange data and perform various tasks autonomously. This can include:

- monitoring environmental conditions in farms
- managing traffic patterns with smart cars and other smart automotive devices
- controlling machines and processes in factories
- tracking inventory and shipments in warehouses

IoT devices are used to monitor a wide range of parameters such as temperature, humidity, air quality, energy consumption, and machine performance.

Examples of IoT devices include:

- Smart home devices such as thermostats, lighting systems, and security systems.
- Wearables such as fitness trackers and smartwatches.
- Healthcare devices such as patient monitoring systems and wearable medical devices.
- Industrial systems such as predictive maintenance systems and supply chain management systems.
- Transportation systems such as connected cars and autonomous vehicles.
- The IoT is transforming various industries, from healthcare and manufacturing to transportation and energy. IoT devices generate vast amounts of data, which can be analyzed to improve operations, drive innovation, and create new business opportunities.

Characteristics of the Internet of Things

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 (Complexity)

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

8. Interoperability

- It helps in minimizing the human efforts in using the devices.
- It saves essential assets like time, electricity, etc.
- The resource is very efficiently used in IoT.

The Internet of Things (IoT) vision

The Internet of Things (IoT) vision revolves around the idea of connecting everyday objects and devices to the internet, enabling them to communicate, collect, and exchange data. This interconnected network of physical objects, equipped with sensors, actuators, and other technologies, creates a smart and dynamic environment.

The primary goals of the IoT vision include:

Interconnectivity: The IoT aims to connect a wide range of devices, from household appliances and industrial machinery to wearable devices and smart cities

infrastructure. This interconnectivity allows seamless communication and data exchange between devices.

Data Collection and Analysis: IoT devices generate vast amounts of data through sensors that monitor and measure various parameters. The vision involves collecting and analyzing this data to gain insights, make informed decisions, and optimize processes.

Automation: With IoT, devices can be programmed to perform specific actions correspond to particular conditions automatically. This automation enhances efficiency, reduces human intervention, and enables real-time adjustments based on the collected data.

Improved Efficiency and Productivity: By leveraging IoT, businesses and industries can optimize their operations, streamline processes, and improve overall efficiency. This can lead to cost savings, increased productivity, and enhanced resource utilization. Enhanced User Experience: IoT contributes to a more personalized and user-centric experience by enabling smart homes, wearables, and other devices to adapt to user preferences and behavior patterns.

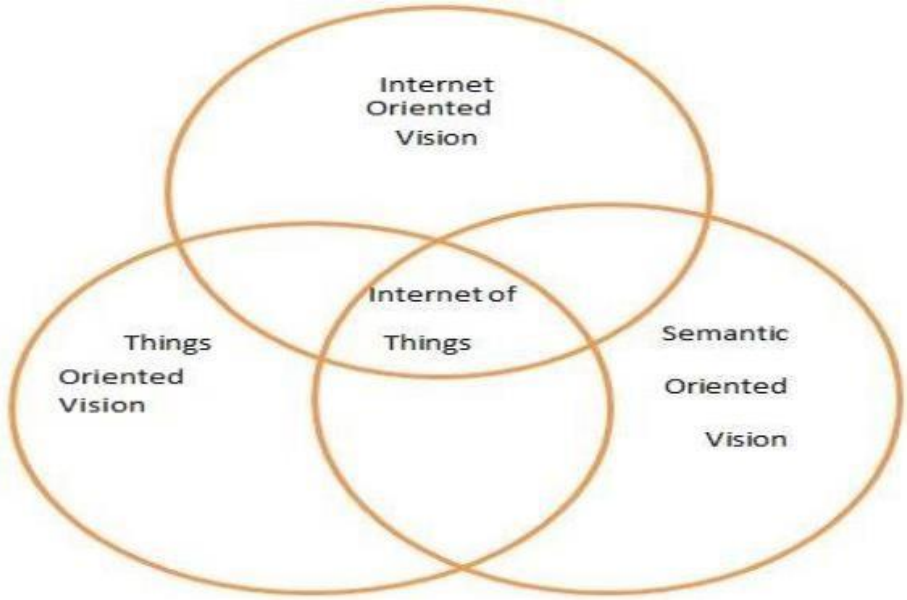
Smart Cities: The IoT vision extends to creating smart cities where various systems, such as transportation, energy, and public services, are interconnected to improve urban living conditions, sustainability, and resource management.

Security and Privacy: As the number of connected devices grows, ensuring the security and privacy of data becomes crucial. The IoT vision includes robust security measures to protect sensitive information and prevent unauthorized access.

Innovation and Collaboration: The IoT ecosystem fosters innovation by providing a platform for collaboration among different industries and stakeholders. This collaboration can lead to the development of new technologies and solutions that address complex challenges.

Environmental Sustainability: IoT can contribute to environmental sustainability by optimizing resource use, reducing energy consumption, and facilitating the development of eco-friendly technologies.

Healthcare Transformation: In healthcare, IoT devices can enable remote patient monitoring, personalized medicine, and more efficient healthcare delivery, leading to improved patient outcomes.



IoT Vision.

Emerging trends in IOT

Edge Computing: Edge computing involves processing data near the source of data generation, reducing latency and bandwidth usage. With the proliferation of IoT devices generating vast amounts of data, edge computing is becoming increasingly important for real-time processing and decision-making.

5G Connectivity: The rollout of 5G networks promises faster speeds, lower latency, and increased network capacity, enabling more IoT devices to connect and communicate seamlessly. This advancement facilitates the growth of IoT applications in various sectors, including smart cities, healthcare, and manufacturing.

AI and Machine Learning Integration: AI and machine learning algorithms are being integrated into IoT systems to analyze large volumes of data generated by connected devices. This integration enables predictive analytics, anomaly detection, and automation, enhancing the efficiency and effectiveness of IoT applications.

Security and Privacy Concerns: As the number of connected devices continues to rise, so do concerns about security and privacy. IoT security vulnerabilities can expose

sensitive data and pose risks to infrastructure and individuals. Addressing these concerns through robust security measures, such as encryption, authentication, and access control, is crucial for the widespread adoption of IoT technologies.

Interoperability Standards: The development and adoption of interoperability standards are essential for ensuring seamless communication and integration among different IoT devices and platforms. Standards such as MQTT, CoAP, and OPC UA facilitate interoperability and compatibility, enabling IoT ecosystems to operate efficiently and effectively.

Blockchain Technology: Blockchain technology is increasingly being explored for enhancing the security, transparency, and integrity of IoT data and transactions. By providing a decentralized and tamper-proof ledger, blockchain can mitigate risks associated with data manipulation and unauthorized access in IoT applications.

Edge AI: Edge AI involves deploying AI algorithms directly on IoT devices or at the edge of the network, enabling real-time data analysis and decision-making without relying on cloud connectivity. Edge AI reduces latency, conserves bandwidth, and enhances privacy by processing data locally.

Sustainability and Energy Efficiency: With growing concerns about environmental sustainability, IoT solutions are being designed to optimize energy usage and promote sustainability. Smart energy management systems, environmental monitoring devices, and efficient resource utilization are examples of IoT applications aimed at addressing sustainability challenges.

Digital Twins: Digital twins are virtual representations of physical objects, processes, or systems that enable monitoring, analysis, and simulation. IoT devices and sensors collect real-time data from physical assets, which is then used to create and update digital twins. This technology is particularly valuable in industries such as manufacturing, healthcare, and infrastructure management.

Vertical-Specific Solutions: Increasingly, IoT solutions are being tailored to specific verticals or industries, addressing unique requirements and challenges. Whether it's precision agriculture, remote patient monitoring in healthcare, or predictive maintenance in manufacturing, vertical-specific IoT solutions are driving innovation and efficiency in various sectors.

Economic Significance of IoT

IoT can significantly impact the economy by improving productivity, increasing competitiveness, and generating additional tax revenue. IoT is a revolutionary technology that both individuals and companies cannot afford to overlook

Productivity and New Business Models: IoT technology enhances productivity through automation, machine downtime reduction, and energy savings, leading to increased efficiency and profits for businesses.

Environmental Impact: IoT can optimize waste management, reduce energy consumption, and contribute to sustainability efforts by saving electricity and fuel consumption

Job Market Changes: While automation may lead to job losses in the short term, strategic adoption of IoT technologies is crucial for economic growth and competitiveness in the long run.

Global Economic Inequality: The benefits of IoT adoption may not accrue equitably across all nations or industries, potentially reinforcing inequalities in global markets

Societal Benefits of IoT

Efficient Resource Management:

IoT enables better utilization of resources by providing real-time data on various parameters. For example, in agriculture, smart sensors can monitor soil conditions and crop health, allowing farmers to optimize water and fertilizer usage.

Smart Cities:

IoT contributes to the development of smart cities by enhancing urban infrastructure and services. Connected devices can be used for intelligent traffic management, waste management, energy consumption optimization, and public safety improvements.

Healthcare Advancements:

IoT applications in healthcare can lead to remote patient monitoring, smart medical devices, and improved healthcare delivery. Wearable devices and sensors can track vital signs, send alerts, and provide valuable data for preventive care.

Environmental Monitoring:

IoT can be used to monitor and manage environmental conditions. For instance, sensors can track air and water quality, detect pollution, and contribute to conservation efforts. This data can be used to make informed decisions for sustainable resource management.

Improved Safety and Security:

IoT enhances safety and security through applications like smart surveillance systems, smart home security, and industrial safety monitoring. Connected devices can detect and respond to potential threats in real-time.

Energy Efficiency:

IoT plays a crucial role in optimizing energy consumption. Smart grids, connected appliances, and energy management systems can help reduce energy wastage, lower costs, and contribute to a more sustainable energy future.

Enhanced Transportation:

IoT applications in transportation lead to smarter and safer systems. Intelligent traffic management, predictive maintenance for vehicles, and real-time monitoring of public transport contribute to a more efficient and reliable transportation network.

Improved Quality of Life for Individuals:

IoT devices contribute to improved quality of life for individuals through applications such as smart homes, wearable health devices, and assistive technologies for people with disabilities.

Supply Chain Optimization:

IoT enhances supply chain visibility and efficiency by providing real-time tracking of goods, monitoring inventory levels, and optimizing logistics. This can lead to reduced costs and improved overall performance.

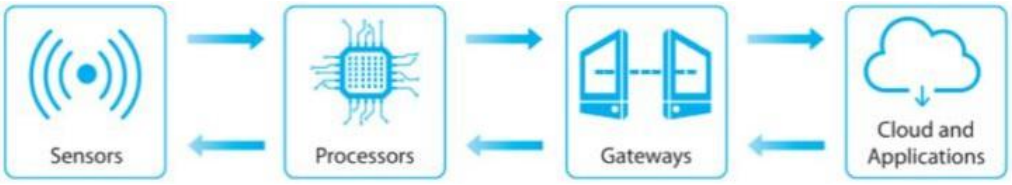
Business Productivity:

In the industrial sector, IoT helps improve productivity and efficiency by enabling predictive maintenance, monitoring equipment performance, and automating routine tasks.

Data-Driven Decision Making:

The wealth of data generated by IoT devices allows businesses, governments, and individuals to make informed decisions based on real-time insights, fostering innovation and better outcomes.

Technical Building Blocks



The Internet of Things denotes the connection of devices, machines, and sensors to the Internet. An IoT system comprises four basic building blocks: sensors, processors, gateways, and applications

The architecture of IoT components:

1. **Sensors** convert a non-electrical input to an electrical signal. Sensors are the front end of the IoT devices. They really mean "things" in IoT. Their main task is to get necessary data from surroundings and pass it further to database or processing systems. They must be uniquely findable from there IP address because they are basic front end interface in the large network of other devices. Sensors collect real time data and can either work autonomous or can be user controlled.

   Examples of sensors are: gas sensor, water quality sensor, moisture sensor, etc.

   Sensors are classified into two types: active and passive sensors. Whereas active sensors use and emit their own energy to collect real-time data (ex.: GPS, X-ray, radars), passive sensors use energy from external sources (ex: cameras). Additionally, sensors differentiate themselves by position, occupancy, and motion, velocity and acceleration, force, pressure, flow, humidity, light, radiation, temperature, etc.

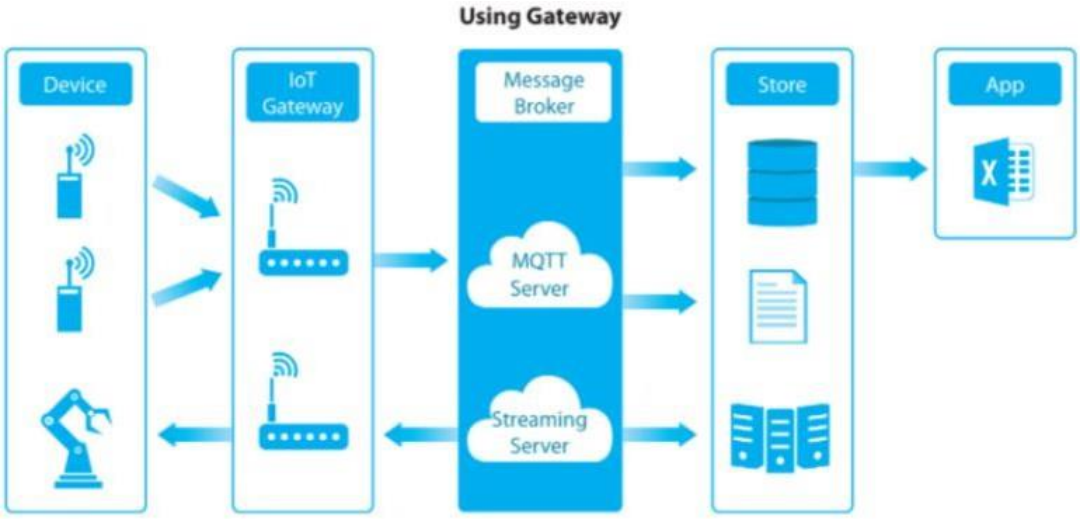
2. **Processors**

   As computer and other electrical systems, processors are the brain of the IoT system. The main job of processors it to process raw data collected by the

sensors and transforms them to some meaningful information and knowledge. In short, we can say that its job is to give intelligence to the data. Processors are easily controllable by applications and their one more important job is to securing data. They perform encryption and decryption of data. Microcontroller, embedded hardware devices, etc can process the data using processors attached within the devices.

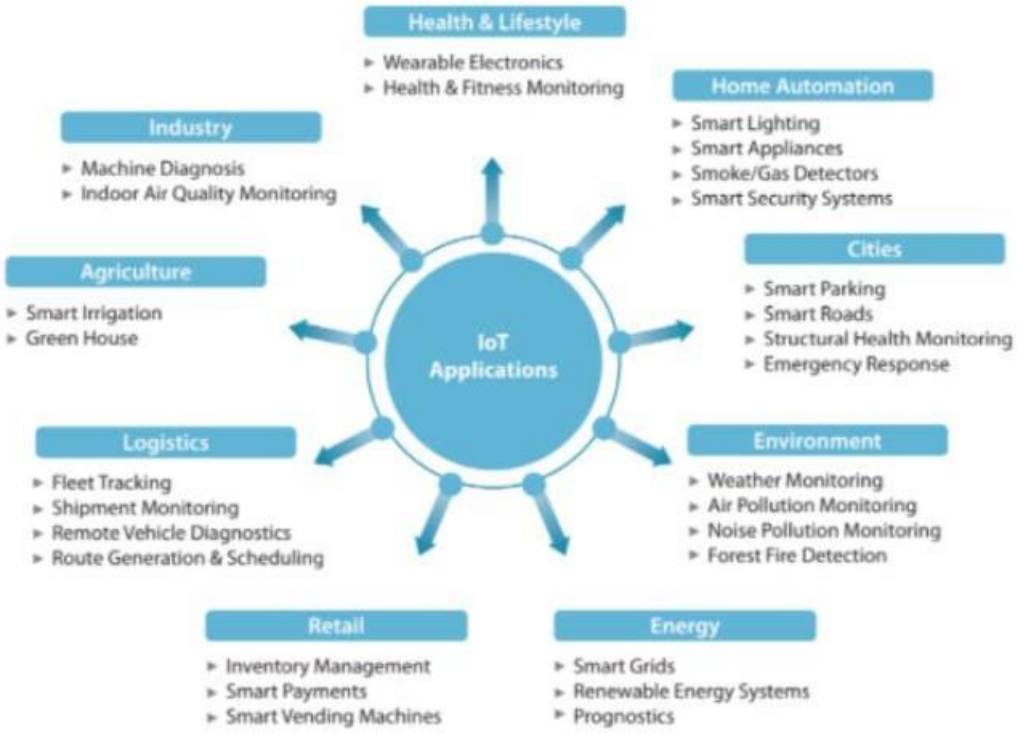
Examples of processors are microcontrollers and microcomputers.

3. **Gateways** are the combination of hardware and software used to connect one network to another. Gateways are responsible for bridging sensor nodes with the external Internet or World Wide Web. Main task of gateways is to route the processed data and transfer it to proper databases or network storage for proper utilization. In other words, gateway helps in communication of the data. Communication and network connectivity are essentials for IoT systems. Examples of gateways are LAN, WAN, PAN, etc. The figure below depicts how using gateways works.

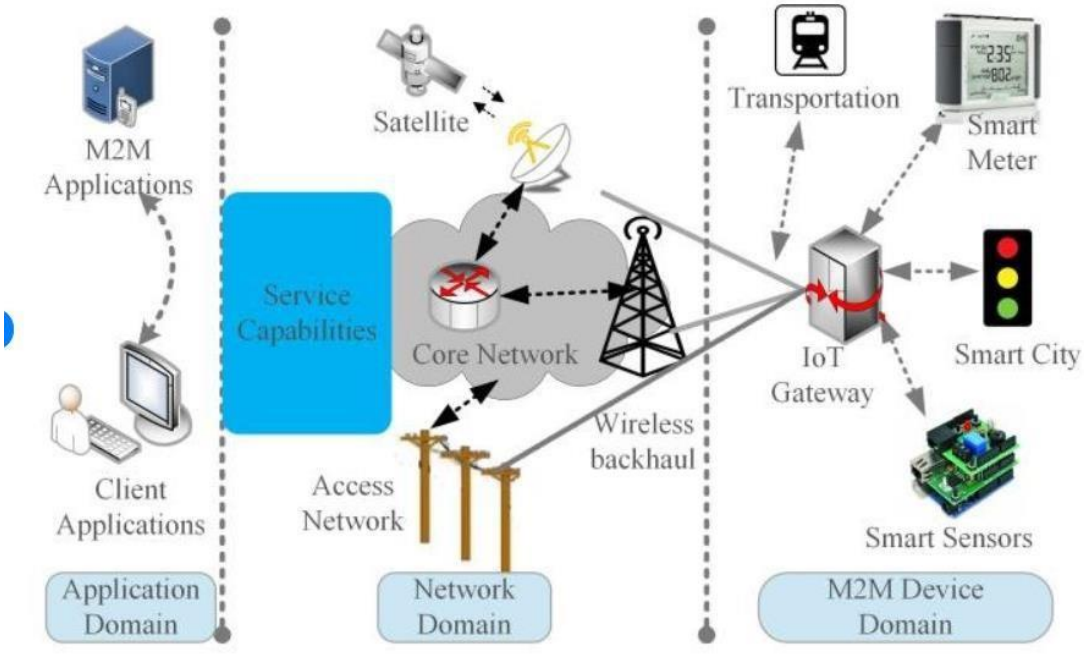


4. **Applications** provide a user interface and effective utilization of the data collected. Applications are another end of an IoT system. Applications do proper utilization of all the data collected and provide interface to users to interact with that data. These applications could be cloud based applications which are responsible for rendering data collected. Applications are user controllable and are delivery points of particular services. Examples of applications are: smart

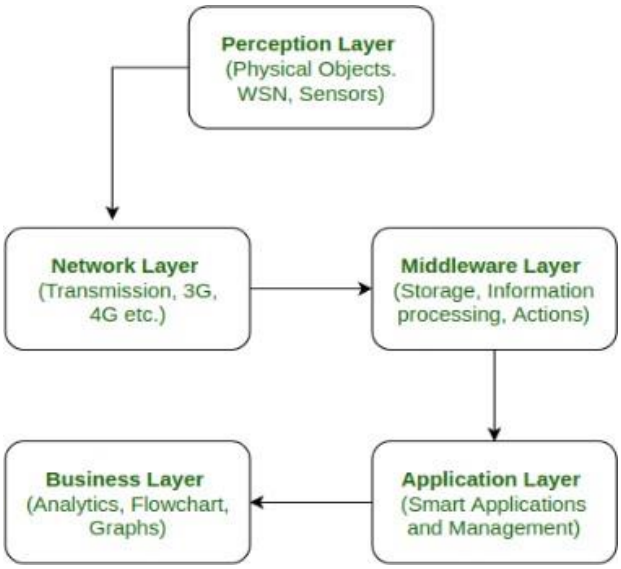
home apps, security system control applications, industrial control hub applications, etc. The figure above illustrates some examples of IoT applications.



High-level Architecture of IoT



High-level IoT architecture



- **Perception Layer :** This is the first layer of IoT architecture. In the perception layer, number of sensors and actuators are used to gather useful information like temperature, moisture content, intruder detection, sounds, etc. The main function of this layer is to get information from surroundings and to pass data to another layer so that some actions can be done based on that information.
- **Network Layer :** As the name suggests, it is the connecting layer between perception and middleware layer. It gets data from perception layer and passes data to middleware layer using networking technologies like 3G, 4G, UTMS, WiFI, infrared, etc. This is also called communication layer because it is responsible for communication between perception and middleware layer. All the transfer of data done securely keeping the obtained data confidential. It includes protocols and technologies for both local area networks (LANs) and wide area networks (WANs), such as Wi-Fi, Bluetooth, Zigbee, RFID, cellular networks (3G/4G/5G), LoRaWAN, and others.
- **Middleware Layer :** Middleware Layer has some advanced features like storage, computation, processing, action taking capabilities. It stores all data-set and based on the device address and name it gives appropriate data to that device. It can also take decisions based on calculations done on data-set obtained from sensors. The middleware layer serves as a bridge between the lower layers (perception and network) and the higher

layers (application and business layers). It provides services such as data normalization, protocol translation, device management, security, and authentication. MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), and AMQP (Advanced Message Queuing Protocol) are examples of protocols often used in this layer.

- **Application Layer :** The application layer manages all application process based on information obtained from middleware layer. This application involves sending emails, activating alarm, security system, turn on or off a device, smartwatch, smart agriculture, etc.
- **Business Layer :** The success of any device does not depend only on technologies used in it but also how it is being delivered to its consumers. Business layer does these tasks for the device. It involves making flowcharts, graphs, analysis of results, and how device can be improved, etc.

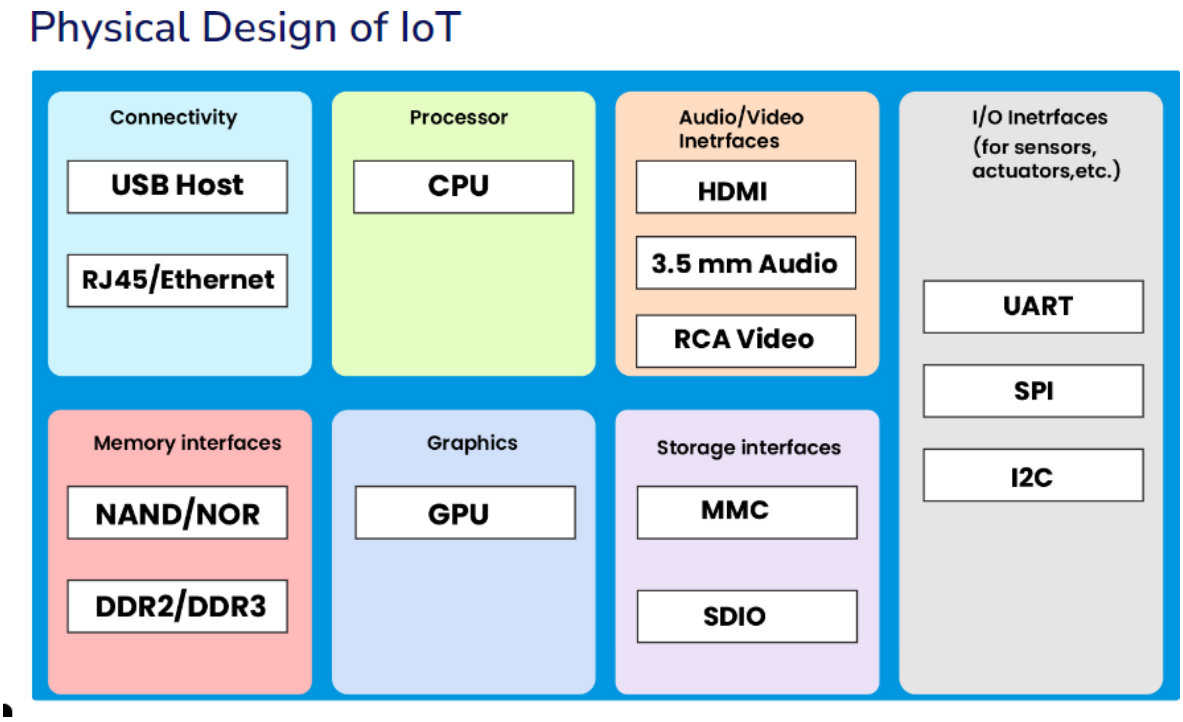
- **Edge Computing Layer:** In many IoT architectures, especially those involving real-time data processing and low-latency requirements, there's a layer called edge computing. Edge computing involves processing data closer to the data source (i.e., at the network edge or on IoT devices themselves) to reduce latency, minimize bandwidth usage, enhance security, and support offline operation. Edge computing can involve deploying computing resources such as microcontrollers, edge gateways, or edge servers at the network edge.
- **Cloud Platform:** While not always a distinct layer, cloud platforms play a crucial role in many IoT architectures by providing scalable storage, computing resources, and services for data storage, processing, analytics, and machine learning. Cloud platforms enable centralized management, remote access, and global scalability for IoT deployments.

Physical Design of IoT

The physical design of Internet of Things (IoT) devices encompasses various aspects including form factor, hardware components, power source, connectivity options, sensors, and environmental considerations.

The Internet of Things (IoT) is the physical devices that are connected to a network. These physical devices are called node devices. These are embedded with sensors, software, and other technologies to exchange data with other devices and systems

over the Internet. With IoT, digital systems can record, monitor, and adjust each interaction between connected things. Hence now we can connect everyday objects like kitchen appliances, cars, thermostats, etc to the internet via embedded devices. This makes communication streamlined between people, processes, and things.to understand IoT properly we need to understand the Logical and Physical Designs of IOT in detail.



Form Factor: IoT devices come in various shapes and sizes depending on their intended use case and deployment environment. They can range from small, compact sensors to larger industrial equipment. Form factor considerations include factors such as portability, mounting options, and ease of installation.

Hardware Components: The hardware components of an IoT device typically include a microcontroller or microprocessor, memory (both volatile and non-volatile), communication interfaces (such as Wi-Fi, Bluetooth, Zigbee, cellular, etc.), power management circuitry, and sometimes specialized hardware for specific functionalities (e.g., sensors, actuators, cameras).

Power Source: Power considerations are critical for IoT devices, especially those intended for remote or battery-powered operation. Devices can be powered through various means including batteries, solar panels, energy harvesting techniques, or

through wired power sources. Power efficiency is a key consideration to maximize device uptime and minimize maintenance requirements.

Connectivity Options: IoT devices need to connect to the internet or other devices to exchange data. Connectivity options vary based on factors such as range, data rate, power consumption, and cost. Common connectivity options include Wi-Fi, Bluetooth, Zigbee, LoRaWAN, cellular (2G/3G/4G/5G), and Ethernet.

Sensors and Actuators: Sensors are crucial for gathering data in IoT applications. These can include temperature sensors, humidity sensors, motion sensors, light sensors, GPS modules, accelerometers, gyroscopes, etc. Actuators are devices used to perform physical actions based on data received from sensors, such as motors, relays, and valves.

Environmental Considerations: IoT devices may be deployed in harsh environments or exposed to extreme conditions, so they need to be designed to withstand factors like temperature variations, humidity, dust, water, vibration, and physical impacts. Enclosures and ruggedized designs are often employed to protect the internal electronics.

Security Considerations: Physical security of IoT devices is essential to prevent tampering, unauthorized access, and data breaches. This includes measures such as secure enclosures, tamper-evident seals, secure boot mechanisms, hardware-based encryption, and secure communication protocols.

Manufacturing Considerations: The physical design of IoT devices must also consider manufacturability, including factors like ease of assembly, testing, and scalability of production. Design for Manufacturing (DFM) and Design for Assembly (DFA) principles are often employed to optimize the manufacturing process.

IoT (Internet of Things)

IoT (Internet of Things) protocols are a set of rules and standards that govern communication between IoT devices, gateways, and cloud platforms. These protocols ensure interoperability, security, and efficient data exchange in IoT ecosystems.

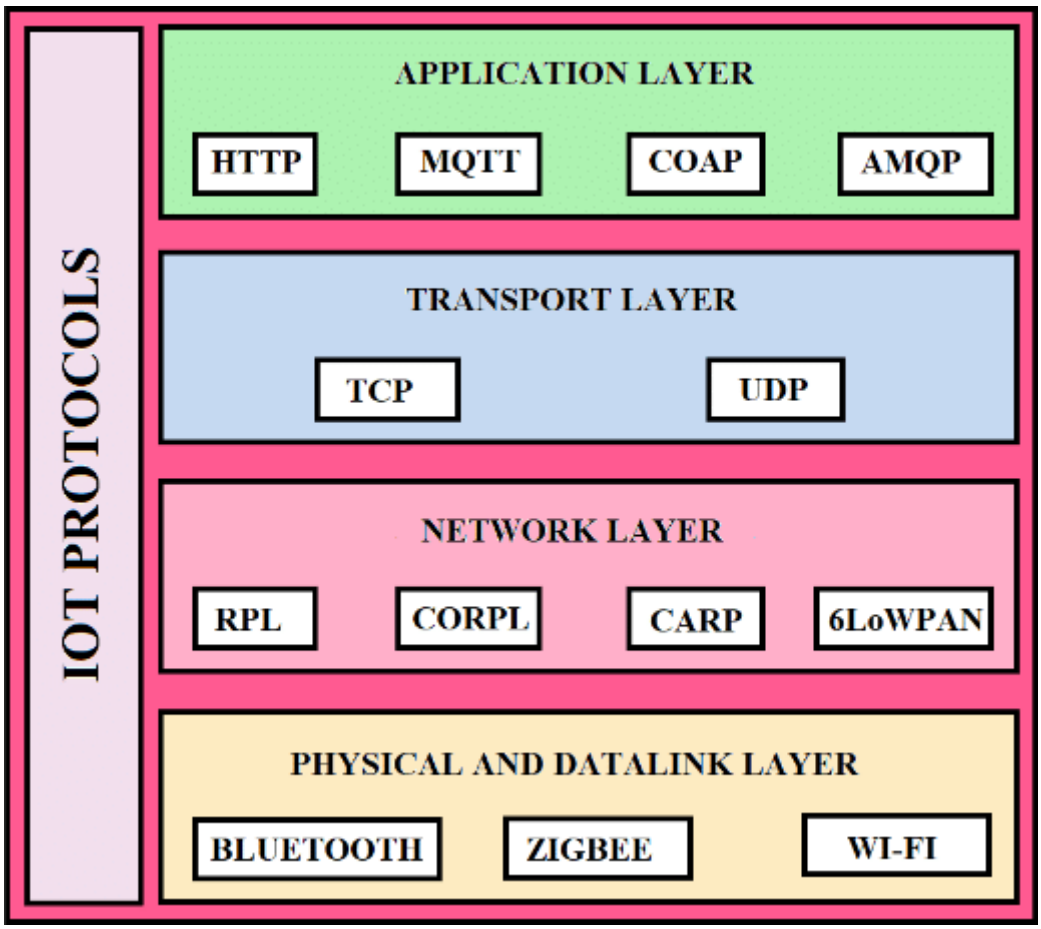


Table 1 protocols in different layers

Application layer	HTTP, CoAP, EBHTTP, LTP, SNMP, IPfix, DNS, NTP, SSH, DLMS, COSEM, DNP, MODBUS
Network/Communication layer	IPv6/IPv4, RPL, TCP/UDP, uIP, SLIP, 6LoWPAN,
PHY/MAC layer	IEEE 802.11 Series, 802.15 Series, 802.3, 802.16, WirelessHART, Z-WAVE, UWB, IrDA, PLC, LonWorks, KNX

Link Layer protocol

- IEEE 802.15.4: A low-rate wireless personal area network (LR-WPAN) standard that provides the physical and data link layer specifications for low-power devices and sensors.
- Bluetooth Low Energy (BLE): A wireless personal area network technology designed for short-range communication with low power consumption, commonly used in wearable devices, smart home appliances, and healthcare devices.

- Zigbee: A low-power, low-data-rate wireless mesh networking standard designed for applications such as home automation, smart lighting, and industrial automation.
- Z-Wave: A wireless communication protocol primarily used for home automation applications. It operates on the sub-1 GHz band and is known for its interoperability among devices from different manufacturers.

The IoT Data Link communication protocol provides service to the Network Layer. There are various protocols and standard technologies specified by the different organization for data link protocols.

Bluetooth

Bluetooth is a short-range wireless communication network over a radio frequency. Bluetooth is mostly integrated into smartphones and mobile devices. The Bluetooth communication network works within 2.4 ISM band frequencies with data rate up to 3Mbps.

There are three categories of Bluetooth technology:

1. Bluetooth Classic
2. Bluetooth Low Energy
3. Bluetooth SmartReady

Properties of Bluetooth network

- **Standard:** Bluetooth 4.2
- **Frequency:** 2.4GHz
- **Range:** 50-150m
- **Data transfer rates:** 3Mbps

Advantages of Bluetooth network

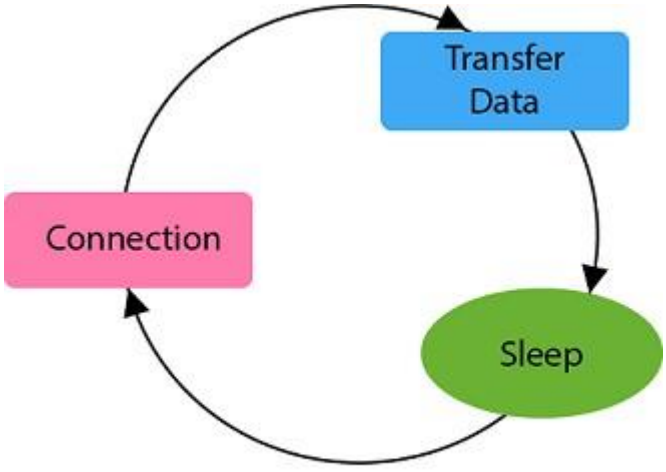
- It is wireless.
- It is cheap.
- It is easy to install.
- It is free to use if the device is installed with it.

Disadvantages of Bluetooth network

- It is a short-range communication network.
- It connects only two devices at a time.

Bluetooth Low Energy

Bluetooth low energy (BLE) is a short-range communication network protocol with PHY (physical layer) and MAC (Medium Access Control) layer. It is designed for low-power devices which uses less data. BLE always remain in sleep mode except when the connection between devices is initiated and data transmission occurs, due to this it conserves power of the device. Bluetooth low energy follows the master/slave architecture and offers two types of frames that are adverting and data frames. Slave node sent the advertising frame to discover one or more dedicated advertisement channels. Master nodes sense this advertisement channels to find slaves and connect them.



BLE Technology

Z-Wave

Z-Wave is a wireless communication protocol with the frequency of 900MHz. The ranges of Z-Wave lies between 30 meters to 100 meters with the data transfer rate of 100kbps so that it is suitable for small messages in IoT applications for home automation. This communication protocol operates on mesh network architecture with one and several secondary controllers.

Properties of Z-Wave protocol

- **Standard:** Z-Wave Alliance ZAD12837 / ITU-T G.9959
- **Frequency:** 908.42GHz
- **Range:** 30-100m
- **Data transfer rate:** 100kbps

Advantages of Z-Wave protocol

- Low power consumption
- Remote or local control
- Simple installation
- Interoperability

Application of Z-Wave protocol

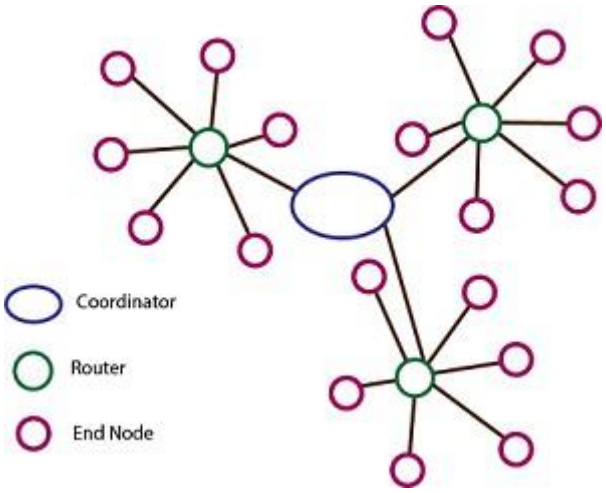
- Smart product and IoT based application
- Energy saving
- Home security

ZigBee Smart Energy

ZigBee is a low power, low data rate wireless personal area network communication protocol. It is mostly used in home automation and industrial settings. Since ZigBee is a low power communication protocol, the IoT power devices used with ZigBee technology. The ZigBee communication protocol is based on the IEEE 802.15.4 standard operating at the 2.4GHz frequency. The ZigBee protocol supports star, cluster or wireless mesh technology topology.

ZigBee uses the following devices in its network:

- Zigbee Coordinator
- Zigbee End Device
- Zigbee Router



Properties of ZigBee protocol

- **Standard:** ZigBee 3.0 based on IEEE802.15.4
- **Frequency:** 2.4GHz
- **Range:** 10-100m
- **Data transfer rate:** 250kbps

Advantages of ZigBee protocol

- Wireless
- Mesh networking
- Direct communication
- Low power consumption

Disadvantages of ZigBee protocol

- Costly
- Works with low speed within a small distance

Application of ZigBee protocol

- Commercial and residential control
- Personal and healthcare
- Home networking
- Industrial control and management

- Consumer electronics

LoRaWAN

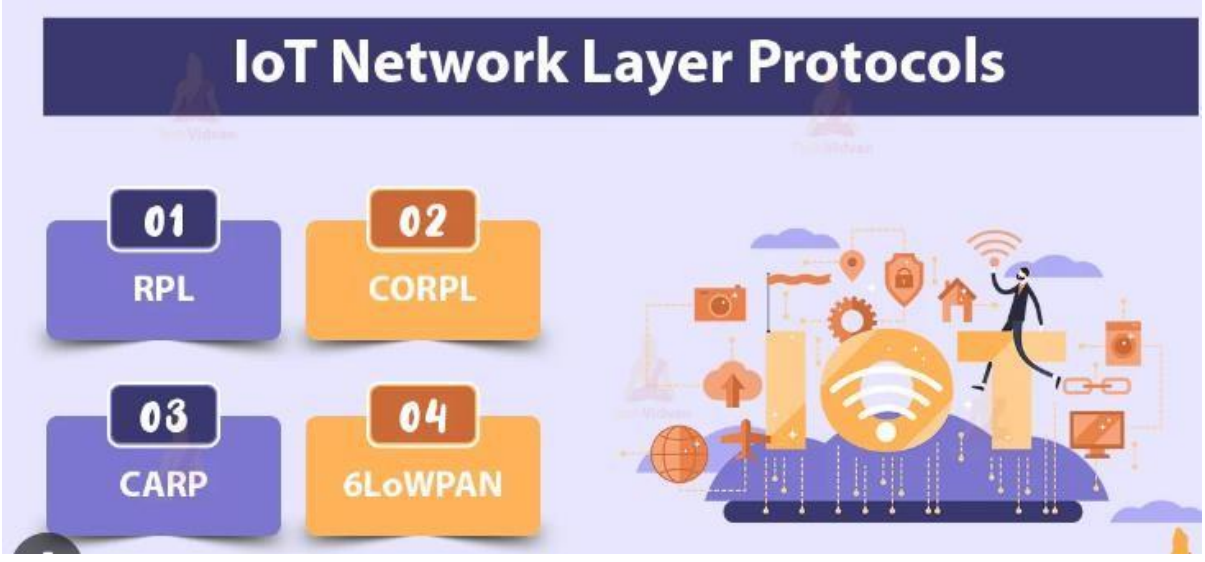
LoRaWAN refers to Long Rage Wide Area Network which is a wide area network protocol. It is an optimized low-power consumption protocol design to support large-scale public networks with millions of low-power devices. A single operator operates the LoRaWAN. The LoRaWAN network is a bi-directional communication for IoT application with low cost, mobility, and security.

Properties of LoRaWAN protocol

- **Standard:** LoRaWAN
- **Frequency:** Various
- **Range:** 2-5km (urban environment), 15km (suburban environment)
- **Data Rates:** 0.3-50 kbps.

Network Layer Protocols

The network layer is divided into two sublayers: routing layer which handles the transfer of packets from source to destination, and an encapsulation layer that forms the packets.



CORPL Protocol

CORPL protocol is the extension of the **RPL protocol**, which is termed as **cognitive RPL**. This network protocol is designed for cognitive networks and uses DODAG topology. CORPL protocol makes two new modifications in the RPL protocol. It uses opportunistic forwarding to forward a packet between the nodes. Each node of CORPL protocol keeps the information of forwarding set rather than parents only maintaining it. Each node updates its changes to its neighbor using DIO messages. On the basis of this updated message, each node frequently updates its neighbor for constant forwarder set.

CARP Protocol

CARP (Channel-Aware Routing Protocol) is a distributed routing protocol. It is designed for underwater communication. It has lightweight packets so that it can be used for Internet of Things (IoT). It performs two different functionalities: network initialization and data forwarding. CARP protocol does not support previously collected data. Hence, it is not beneficial for those IoT or other application where data is changed frequently. The upgradation of CARP is done in E-CARP which overcomes the limitation of CARP. The E-CARP allows the sink node to save previously received sensory data.

6LoWPAN

The 6LoWPAN protocol refers to IPv6 Low Power Personal Area Network which uses a lightweight IP-based communication to travel over low data rate networks. It has limited processing ability to transfer information wirelessly using an internet protocol. So, it is mainly used for home and building automation. The 6LoWPAN protocol operates only within the 2.4 GHz frequency range with 250 kbps transfer rate. It has a maximum length of 128-bit header packets.

IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): Allows IPv6 packets to be transmitted over low-power wireless networks, enabling IPv6 connectivity for IoT devices.

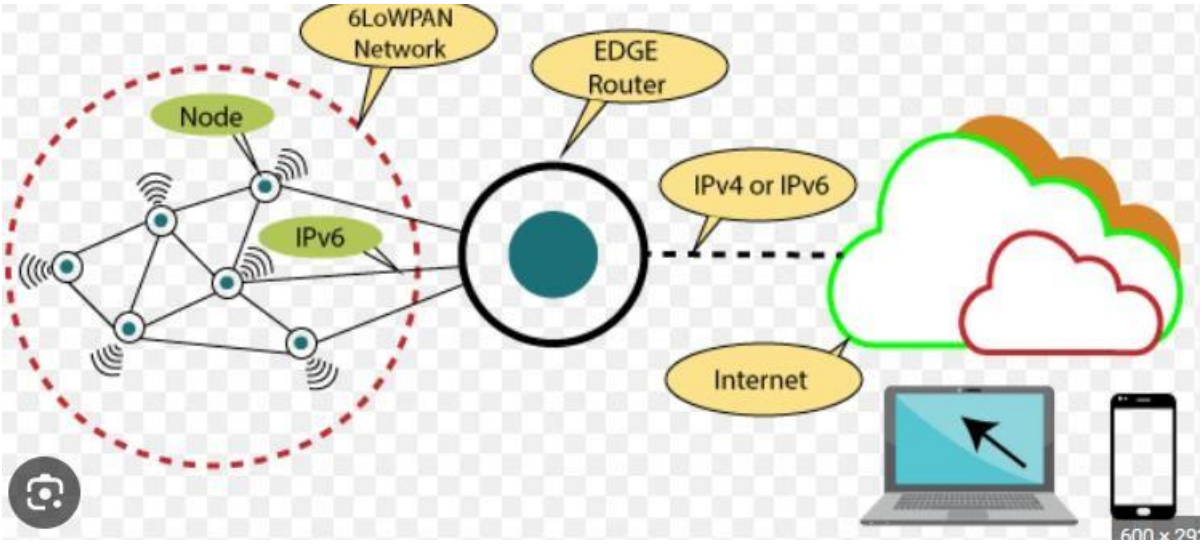
6LowPAN Security Measure

Security is a major issue for 6LowPAN communication Protocol. There are several attacks issues at the security level of 6LoWPAN which aim is to direct destruction of

the network. Since it is the combination of two systems, so, there is a possibility of attack from two sides that targets all the layer of the 6LoWPAN stack (Physical layer, Data link layer, Adaptation layer, Network layer, Transport layer, Application layer).

Properties of 6LowPAN protocol

- **Standard:** RFC6282
- **Frequency:** Used over a variety of other networking media including Bluetooth Smart (2.4GHz) or ZigBee or low-power RF (sub-1GHz)
- **Range:** NA
- **Data Rates:** NA



Transport Layer Protocols

MQTT (Message Queuing Telemetry Transport):

- MQTT is a lightweight messaging protocol designed for constrained devices and low-bandwidth, high-latency, or unreliable networks.
- It follows a publish-subscribe messaging pattern, where clients (devices) publish messages to topics, and other clients subscribe to those topics to receive messages.
- MQTT is widely used in IoT applications due to its efficiency, low overhead, and support for asynchronous communication.

CoAP (Constrained Application Protocol):

- CoAP is a specialized web transfer protocol designed for resource-constrained devices and networks.
- It is designed to be simple and lightweight, making it suitable for IoT devices with limited processing power and memory.
- CoAP is built on top of UDP (User Datagram Protocol) and provides features like reliable delivery, multicast support, and low overhead for efficient communication.

HTTP (Hypertext Transfer Protocol):

- While not specifically designed for IoT, HTTP is commonly used in IoT applications, especially for communication with IoT gateways and web servers.
- HTTP is a request-response protocol, where clients send requests to servers, and servers respond with data.
- In IoT scenarios, HTTP APIs (Application Programming Interfaces) are often used for accessing and managing IoT devices and data over the web.

AMQP (Advanced Message Queuing Protocol):

- AMQP is a messaging protocol that supports message-oriented middleware for distributed systems.
- It provides features like message queuing, routing, reliability, and security, making it suitable for IoT scenarios where reliable and secure communication is essential.
- AMQP is designed to be transport-agnostic, meaning it can work over different underlying transport protocols such as TCP/IP, WebSocket, or TLS.

DDS (Data Distribution Service):

- DDS is a standardized middleware protocol for real-time, scalable, and reliable data distribution in distributed systems.
- It is often used in IoT applications where real-time data sharing and communication between devices and systems are critical.
- DDS provides features like publish-subscribe communication, Quality of Service (QoS) settings, and data-centric communication, making it suitable for a wide range of IoT use cases, including industrial IoT and smart grids.

WebSockets:

WebSockets provide full-duplex communication channels over a single, long-lived connection. This protocol is commonly used for real-time communication between IoT devices and servers.

Use Case: Suitable for scenarios where low-latency, bidirectional communication is required.

Application Layer Protocols:

HTTP/HTTPS: The Hypertext Transfer Protocol and its secure variant are widely used for communication between IoT devices and web servers or cloud platforms, especially in IoT applications with web-based interfaces.

DDS (Data Distribution Service): A publish-subscribe middleware protocol designed for real-time data distribution and communication in distributed systems, including IoT applications in industrial automation and healthcare.

AMQP (Advanced Message Queuing Protocol): A messaging protocol for reliable communication between IoT devices and applications, ensuring message delivery, security, and interoperability.

Modbus: A serial communication protocol commonly used in industrial IoT applications for communication between PLCs, sensors, and other devices.

MQTT (Message Queuing Telemetry Transport):

- MQTT is a lightweight publish-subscribe messaging protocol designed for constrained devices and low-bandwidth, high-latency, or unreliable networks.
- It's widely used in IoT for its simplicity, efficiency, and support for both real-time and intermittent connections.

HTTP (Hypertext Transfer Protocol):

- Although primarily known for web browsing, HTTP is also used in IoT applications for communication between devices and servers.
- It's easy to implement and widely supported but may not be as efficient as MQTT in terms of overhead.

CoAP (Constrained Application Protocol):

- CoAP is a lightweight protocol designed for resource-constrained devices and low-power, lossy networks.
- It's RESTful, similar to HTTP, but optimized for IoT environments.

AMQP (Advanced Message Queuing Protocol):

- AMQP is an open standard application layer protocol for message-oriented middleware.
- It's used for reliable, message-oriented communication in IoT systems, particularly in scenarios where message queuing and routing are essential.

DDS (Data Distribution Service):

- DDS is a protocol for real-time data exchange between IoT devices and applications.
- It's designed for highly scalable, high-performance, and fault-tolerant systems, often used in industrial IoT (IIoT) and critical infrastructure applications.

Websockets:

- Websockets enable full-duplex communication channels over a single TCP connection.
- They're commonly used in IoT applications requiring real-time, bidirectional communication, such as remote control or monitoring.

AMQP (Advanced Message Queuing Protocol):

- AMQP is an open standard application layer protocol for message-oriented middleware.
- It's used for reliable, message-oriented communication in IoT systems, particularly in scenarios where message queuing and routing are essential.

DDS (Data Distribution Service):

- DDS is a protocol for real-time data exchange between IoT devices and applications.
- It's designed for highly scalable, high-performance, and fault-tolerant systems, often used in industrial IoT (IIoT) and critical infrastructure applications.