Introduction to IOT
Unit-1 (AIDS-309)

Prepared By: Dr. Ankita Sharma

Assistant Professor

Department of Computer Science

GTBIT, GGSIPU

AGENDA

Internet Principles

Agenda

- **Internet Communication- An overview**
- **Physical design of IOT**
- **Logical design of IOT**
- **IOT standards**
- **IOT generic architectures and IOT protocols {MQTT, CoAP, HTTP}**
- **IOT future trends**
- **Understand various IOT architectures based on applications.**

IOT

- The Internet of things is a connecting bridge between the physical world and the cyber world and Machine to Machine communication
- Any physical object can be transformed into an IoT device if it can be connected to the internet to be controlled or communicate information.
- A lightbulb that can be switched on using a smartphone app is an IoT device.

Internet Communication- An overview

- **Communication on the internet is done with the help of a network protocol.**
- A network protocol is a set of rules used to set up communication between two or more than two entities.
- A protocol defines the format and the order of messages exchanged between two or more communicating entities as well as action taken on the transmission and receipt of a message or other events.
- A network protocol is similar to human protocol except that entities exchanging the messages are taking action are hardware or software components for some device like a mobile, tablet, computer, etc.
- The Internet and network make extensive use of various protocols. Different protocols used to carry out various communication tasks.

There are many different protocols for Internet

- **FTP:** FTP is a file transfer protocol used to transfer computer files between client and server. It uses port no 21 to send the data.
- **ISDN:** ISDN is an integrated service digital network. It used to transfer voice, data, audio, or video over the telephone cabling or landline connection.
- **SMTP:** SMTP is a simple mail transfer protocol. It used to transfer mail from one user to another user. Many of system uses SMTP to transfer mail.

There are many different protocols for Internet

- **HTTP:** HTTP is a hypertext transfer protocol. It allows the user to communicate data on the world wide web. It is an application protocol for distributed, collaborative, hypermedia information systems.
- **telnet:** telnet is a network protocol. It is used to connect your computer to a remote computer. It has a command-line interface to communicate with the device.
- **HTTPS:** HTTPS is a hypertext transfer protocol secure. It is the same as HTTP except that communication of data on the world wide web is done in an encrypted format. It secures communications between two computers, one using the browser and other fetching data from the webserver.

Physical Design: Constructing the IoT Ecosystem

- The physical IoT design transforms the logical framework into a functional IoT ecosystem.
- In this phase, the system should be tailored to meet the users' specific needs.
- Physical design deals with the actual implementation of devices and infrastructure. It is about figuring out the best methods of storing, accessing, and managing the data generated by IoT devices.
- Physical design encompasses the individual nodes and the protocols used for creating an enterprise's IoT ecosystem.
- With the right nodes, devices can perform tasks like sensing, actuating, monitoring, and data transmission. These tasks operate through wired or wireless connections.

Physical Design: Constructing the IoT Ecosystem

The physical design links devices that are essential for:

- Creating connections
- Processing and storing data
- Offering interfaces
- Facilitating graphical interfaces

❑ *Data generated by these devices is the essential facet of IoT systems. For example: a moisture sensor collects moisture data. The system analyses the data to yield actionable insights, such as when to irrigate crops or monitor the soil's health.*

Physical design of IOT

- A physical design of an IoT system refers to the individual node devices and their protocols that are utilized 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.

Physical design of IOT

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.

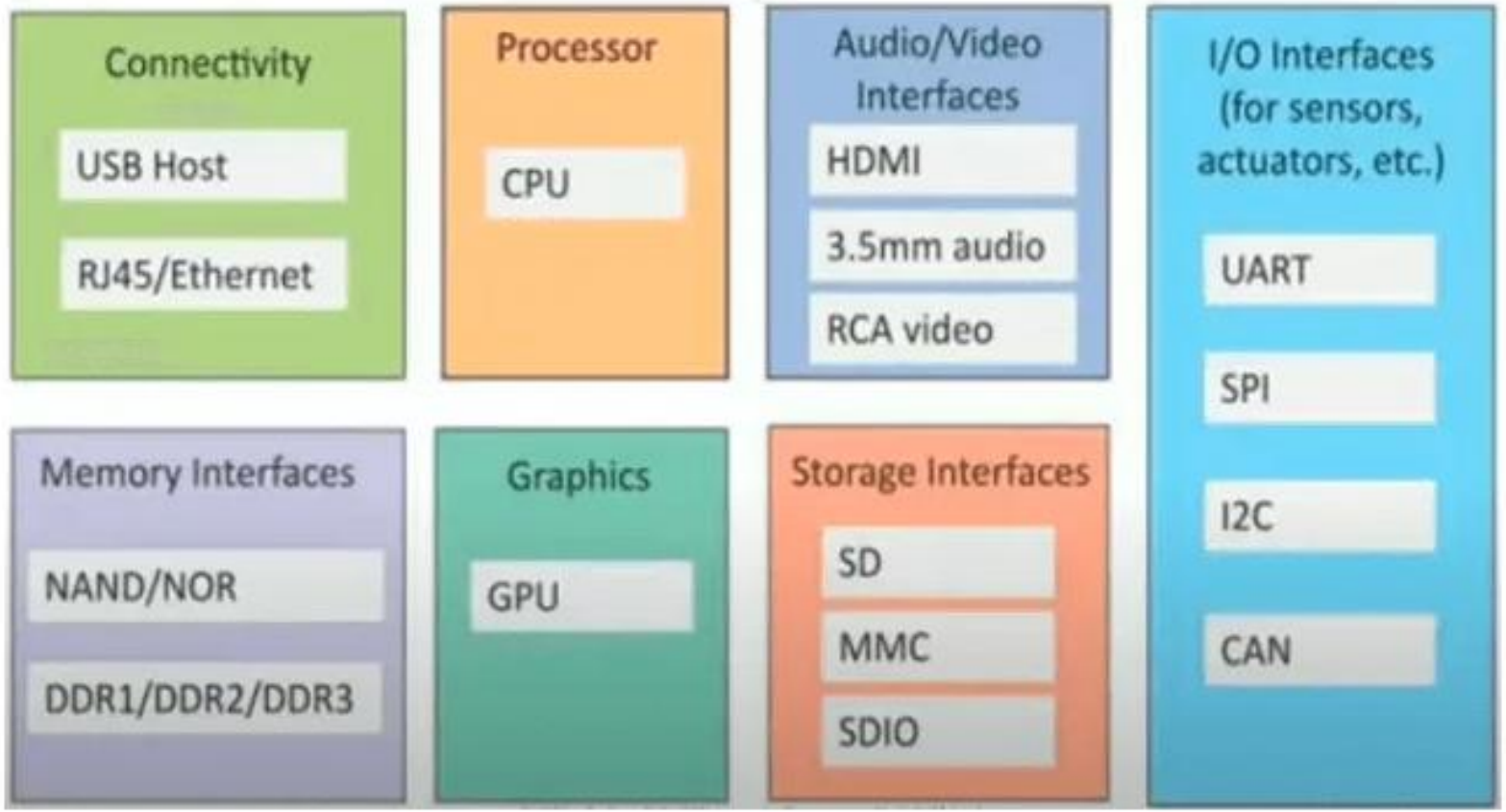
Things/Devices

- Things/Devices are used to build a connection, process data, provide interfaces, provide storage, and provide graphics interfaces in an IoT system.
- All these generate data in a form that can be analyzed by an analytical system and program to perform operations and used to improve the system.
- For example temperature sensor that is used to analyze the temperature generates the data from a location and is then determined by algorithms.

“Things” in IoT: The Heart of the System

- IoT devices are often referred to as Things. These are the central components of IoT applications.
- Some examples of these devices are smartwatches, smart appliances, automobiles, wearable sensors, and industrial machinery. They are fitted with monitoring and remote sensing capabilities. They generate data when in operation.
- This data is a resource that can be analyzed and acted upon to improve operations, enhance efficiency, and deliver real-world insights.
- Businesses can make informed decisions, optimize processes, and even offer new services by processing the data collected by IoT devices.

Things/Devices



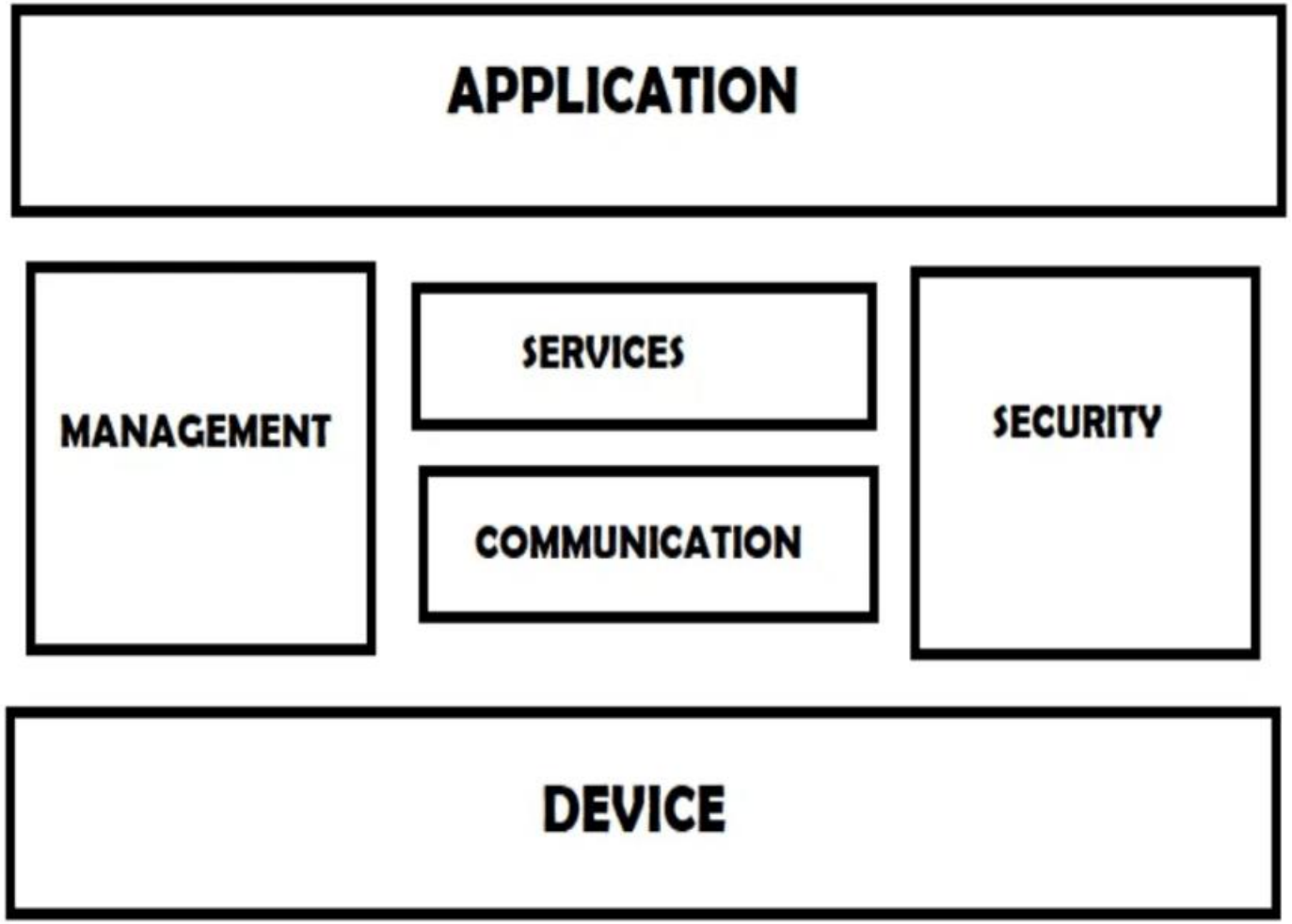
Things/Devices

- **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: Navigating the Framework

- The logical design of an organisation’s IoT system deals with how components such as computers and sensors should be arranged to perform specific functions.
- It focuses on high-level structures and functionality, without delving into the specifics of each component.

Logical design of IOT



The key components of the logical design include:

- **IoT Functional Blocks:** An enterprise's IoT systems comprise distinct functional blocks. These can be divided into devices and communication, along with security, services, and applications. These functional blocks are responsible for providing capabilities such as sensing, identification, actuation, management, and communication.
- **IoT Communication Models:** IoT systems employ a variety of communication models, each with its distinct characteristics. These models include models such as request-response, push-pull, publish-subscribe, and exclusive pairs. They define how information is exchanged within the IoT ecosystem.

The key components of the logical design include:

- **IoT Communication APIs:** Application Programming Interfaces (APIs) play a pivotal role in facilitating communication via the server and the IoT system. Some examples of these APIs include client-server models, stateless communication, and cacheable interfaces, each offering unique functionalities.
- **IoT Protocols:** IoT protocols serve as the guiding principles for data exchange between devices within a network. They enable interoperability across designs and operations. They facilitate the transmission of commands as well as data across different network layers.

Difference Between Physical and Logical Design of IoT

Physical Design	Logical Design
Physical design is highly detailed.	Logical design is a high-level design and doesn't provide any detail.
Physical design is more graphical than textual; however, it can comprise both.	Logical design can be textual, graphic, or both.
A physical design focuses on specific solutions explaining how they are assembled or configured.	A logical design focuses on satisfying the design factors, including risks, requirements, constraints, and assumptions.

What are IoT Standards?

- IoT standards define the requirements for IoT devices and systems. They can cover a wide range of topics, such as security, interoperability, and data formats.
- IoT standards are developed and maintained by various organizations and consortia that specialize in setting technical guidelines, frameworks, and best practices for the Internet of Things.
- Some of the prominent organizations involved in the development of IoT standards include:

IoT Standards

- **International Electrotechnical Commission (IEC):** The IEC is a global organization that develops and publishes international standards for electrical, electronic, and related technologies. They play a crucial role in shaping IoT standards related to areas such as communication protocols, security, and energy efficiency.
- **Institute of Electrical and Electronics Engineers (IEEE):** IEEE is a leading professional association that focuses on advancing technology in various fields, including IoT. They develop standards under the IEEE 802 family, which cover areas such as wireless communication, network protocols, and energy efficiency.

IoT Standards

- **Industrial Internet Consortium (IIC):** The IIC is a consortium of industry leaders, academic institutions, and technology companies working together to accelerate the adoption of the Industrial Internet of Things (IIoT). They develop reference architectures, testbeds, and best practices to promote interoperability and security in industrial IoT deployments.
- **Open Connectivity Foundation (OCF):** The OCF is a consortium that aims to create a standard IoT connectivity framework to enable seamless interoperability across devices, platforms, and ecosystems. They develop specifications and certification programs for IoT devices and applications.

IoT Standards

- **Thread Group:** The Thread Group is an industry alliance focused on developing the Thread networking protocol for IoT devices in the smart home and commercial sectors. They work on defining the technical specifications and certification programs for Thread-enabled products.
- **Connectivity Standards Alliance:** Formerly known as the the Zigbee Alliance is an organization that develops and promotes the Zigbee wireless communication standard, which is widely used in IoT applications such as home automation, smart energy, and lighting control.

Future Trends of IoT

1. Edge Computing

Description: Shifting data processing closer to the source of data (the edge) rather than relying solely on cloud computing.

Impact: Reduces latency, increases speed and efficiency, and enhances data privacy by keeping sensitive data local.

2. AI and Machine Learning Integration

Description: Incorporating artificial intelligence and machine learning algorithms to analyze data and automate decision-making processes.

Impact: Enables predictive maintenance, advanced analytics, and intelligent automation across industries.

Future Trends of IoT

3. 5G Connectivity

Description: The rollout of 5G networks providing higher speeds, lower latency, and greater capacity.

Impact: Facilitates real-time data processing and communication, supporting more sophisticated IoT applications such as autonomous vehicles and smart cities.

4. IoT in Healthcare

Description: Expansion of IoT devices in healthcare, including wearable health monitors, remote patient monitoring, and smart medical devices.

Impact: Improves patient care, enables remote diagnostics, and enhances health management and personalized medicine.

Future Trends of IoT

5. Smart Cities

Description: Development of urban areas that leverage IoT technologies to improve infrastructure, public services, and quality of life.

Impact: Enhances traffic management, energy efficiency, waste management, and public safety.

6. Enhanced Security Measures

Description: Increasing focus on securing IoT devices and networks to protect against cyber threats.

Impact: Implementation of advanced encryption, blockchain, and AI-driven security solutions to safeguard data and privacy.

Future Trends of IoT

7. Industrial IoT (IIoT)

Description: Expansion of IoT applications in manufacturing and industrial settings.

Impact: Optimizes production processes, improves supply chain management, and enables predictive maintenance and asset tracking.

8. Sustainability and Environmental Monitoring

Description: Using IoT to monitor and manage environmental conditions and resources.

Impact: Supports efforts in sustainability, resource conservation, and climate change mitigation through smart agriculture, water management, and air quality monitoring.

Future Trends of IoT

9. Interoperability and Standardization

Description: Development of common standards and protocols for IoT devices to ensure compatibility and seamless integration.

Impact: Facilitates the growth of IoT ecosystems by allowing diverse devices to work together efficiently.

10. IoT in Retail

Description: Utilization of IoT technologies in the retail sector to enhance customer experience and streamline operations.

Impact: Enables personalized shopping experiences, inventory management, and real-time data analytics to optimize sales and marketing strategies.

Future Trends of IoT

11. IoT in Smart Homes

Description: Growth in smart home devices and systems that automate and control home functions.

Impact: Improves convenience, energy efficiency, and home security through interconnected devices like smart thermostats, lighting, and security systems.

12. Blockchain for IoT

Description: Leveraging blockchain technology to enhance security, transparency, and trust in IoT networks.

Impact: Ensures secure and tamper-proof data transactions and enhances device authentication and identity management.

13. Wearable Technology

Description: Proliferation of wearable devices that monitor health, fitness, and other personal metrics.

Impact: Provides real-time health insights, encourages healthy lifestyles, and enables continuous health monitoring.

14. IoT for Supply Chain Management

Description: Using IoT to improve visibility and efficiency in supply chains.

Impact: Enhances tracking, inventory management, and demand forecasting, reducing costs and improving delivery times.

15. Energy Management

Description: Implementation of IoT for optimizing energy use and integrating renewable energy sources.

Impact: Supports smart grids, energy-efficient buildings, and renewable energy management, contributing to sustainability goals.

IoT Protocols

- These protocols are used to establish communication between a node device and a server over the internet.
- It helps to send commands to an IoT device and receive data from an IoT device over the internet.
- We use different types of protocols that are present on both the server and client side.
- These protocols are managed by network layers like application, transport, network, and link layer.

Application Layer protocols

In this layer, protocols define how the data can be sent over the network with the lower layer protocols using the application interface.

HTTP

Hypertext transfer protocol is a protocol that presents in an application layer for transmitting media documents. It is used to communicate between web browsers and servers. It makes a request to a server and then waits till it receives a response and in between the request server does not keep any data between the two requests.

WebSocket

This protocol enables two-way communication between a client and a host that can be run on an untrusted code in a controlled environment. This protocol is commonly used by web browsers.

MQTT

It is a machine-to-machine connectivity protocol that was designed as a publish/subscribe messaging transport and it is used for remote locations where a small code footprint is required.

Transport Layer Protocols

This layer is used to control the flow of data segments and handle error control. Also, these layer protocols provide end-to-end message transfer capability independent of the underlying network.

TCP

The transmission control protocol is a protocol that defines how to establish and maintain a network that can exchange data in a proper manner using the internet protocol.

UDP

A user datagram protocol is a part of an internet protocol called the connectionless protocol. this protocol is not required to establish the connection to transfer data.

Network Layer Protocols

This layer is used to send datagrams from the source network to the destination network. We use IPv4 and IPv6 protocols as host identification that transfers data in packets.

IPv4

This is a protocol address that is a unique and numerical label assigned to each device connected to the network. An IP address performs two main functions host and location addressing. IPv4 is an IP address that is 32-bit long.

IPv6

It is a successor of IPv4 that uses 128 bits for an IP address.

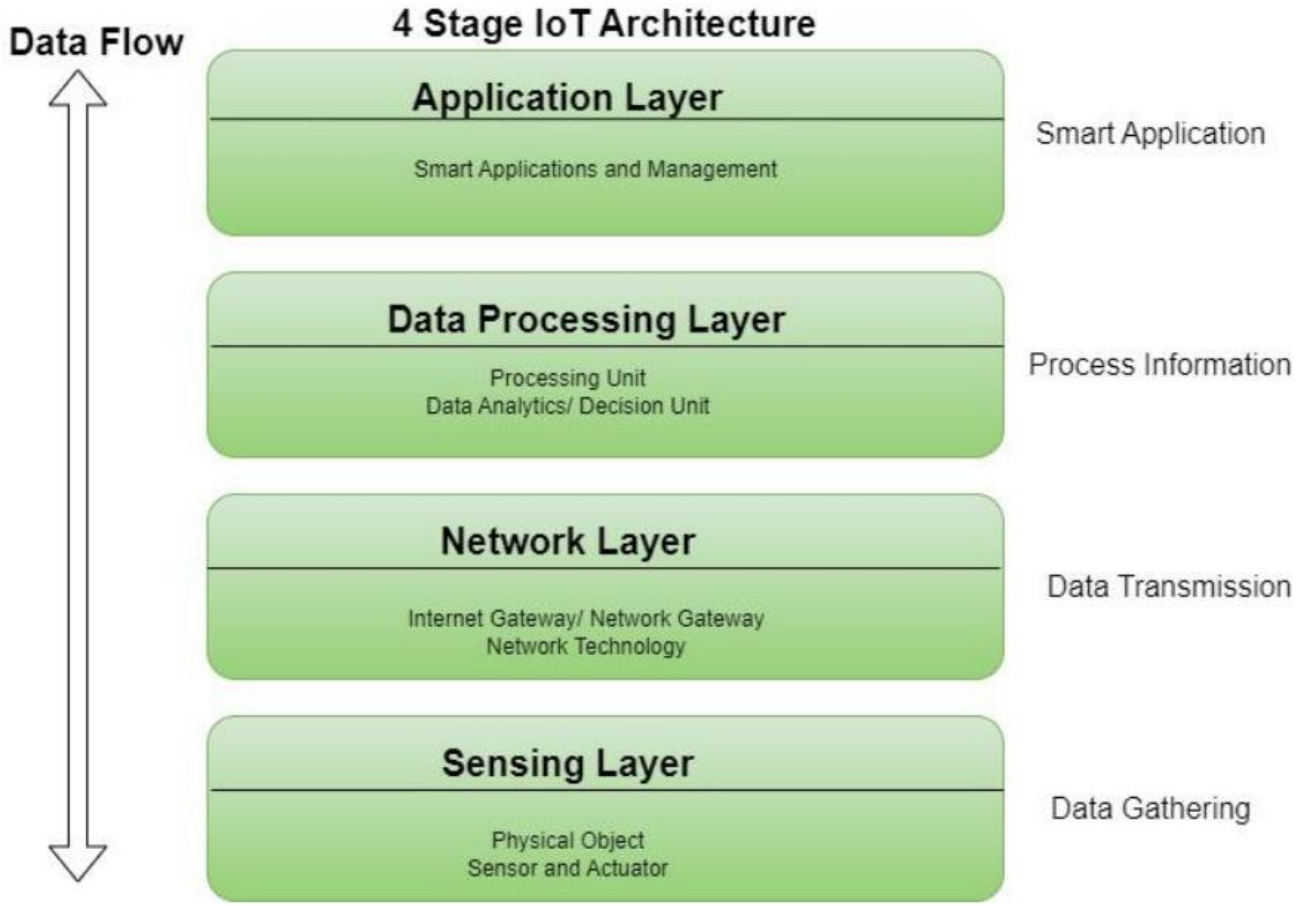
Link Layer Protocols

Link-layer protocols are used to send data over the network's physical layer. It also determines how the packets are coded and signaled by the devices.

Ethernet: It is a set of technologies and protocols that are used primarily in LANs. It defines the physical layer and the medium access control for wired ethernet networks.

WiFi: It is a set of LAN protocols and specifies the set of media access control and physical layer protocols for implementing wireless local area networks.

IoT Architecture



IoT Architecture

1. Sensing Layer:

- The sensing layer is the first layer of the Internet of Things architecture and is responsible for collecting data from different sources.
- This layer includes sensors and actuators that are placed in the environment to gather information about temperature, humidity, light, sound, and other physical parameters.
- Wired or wireless communication protocols connect these devices to the network layer.

IoT Architecture

2. Network Layer:

- The network layer of an IoT architecture is responsible for providing communication and connectivity between devices in the IoT system.
- It includes protocols and technologies that enable devices to connect and communicate with each other and with the wider internet.
- Examples of network technologies that are commonly used in IoT include WiFi, Bluetooth, Zigbee, and cellular networks such as 4G and 5G technology. Additionally, the network layer may include gateways and routers that act as intermediaries between devices and the wider internet, and may also include security features such as encryption and authentication to protect against unauthorized access.

IoT Architecture

3. Data processing Layer:

- The data processing layer of IoT architecture refers to the software and hardware components that are responsible for collecting, analyzing, and interpreting data from IoT devices.
- This layer is responsible for receiving raw data from the devices, processing it, and making it available for further analysis or action.
- The data processing layer includes a variety of technologies and tools, such as data management systems, analytics platforms, and machine learning algorithms.
- These tools are used to extract meaningful insights from the data and make decisions based on that data.
- Example of a technology used in the data processing layer is a data lake, which is a centralized repository for storing raw data from IoT devices.

IoT Architecture

4. Application Layer:

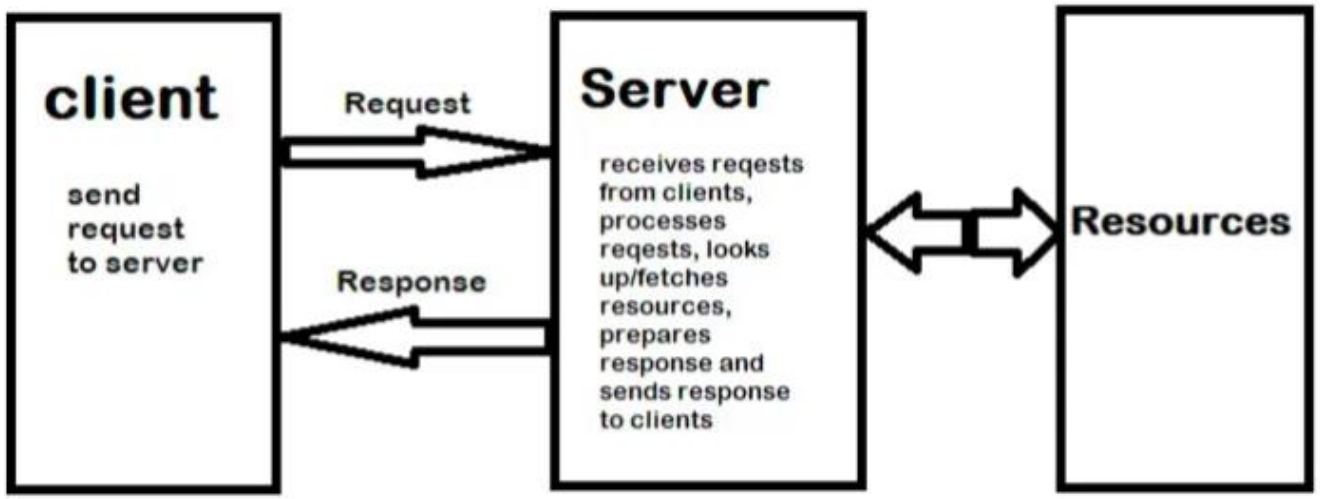
- The application layer of IoT architecture is the topmost layer that interacts directly with the end-user.
- It is responsible for providing user-friendly interfaces and functionalities that enable users to access and control IoT devices.
- This layer includes various software and applications such as mobile apps, web portals, and other user interfaces that are designed to interact with the underlying IoT infrastructure.
- It also includes middleware services that allow different IoT devices and systems to communicate and share data seamlessly.
- The application layer also includes analytics and processing capabilities that allow data to be analyzed and transformed into meaningful insights. This can include machine learning algorithms, data visualization tools, and other advanced analytics capabilities.

IoT Communication Models

1. Request-Response 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.
- Request-response is a stateless communication model and each request-response pair is independent of the others.
- HTTP works as a request-response protocol between a client and a server.
- A web browser may be the client, and an application on a computer that hosts a website 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

IoT Communication Models

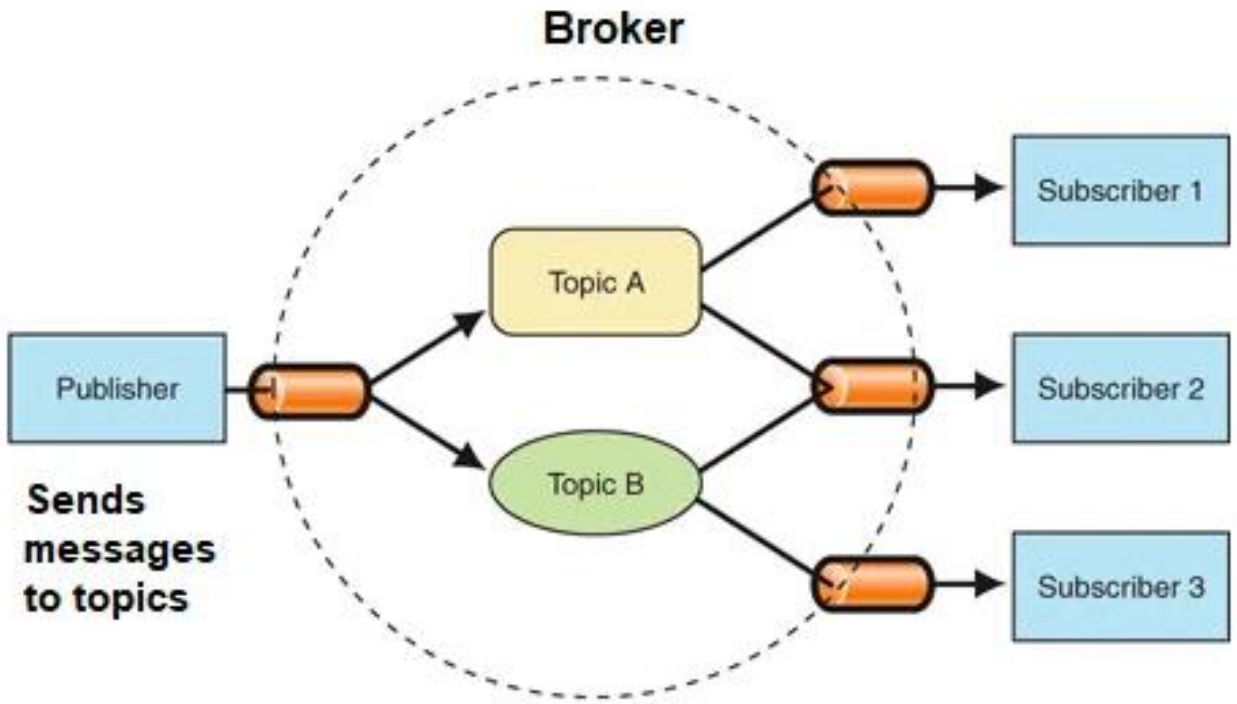
2. Publisher-Subscriber Model —

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.

IoT Communication Models

2. Publisher-Subscriber Model —



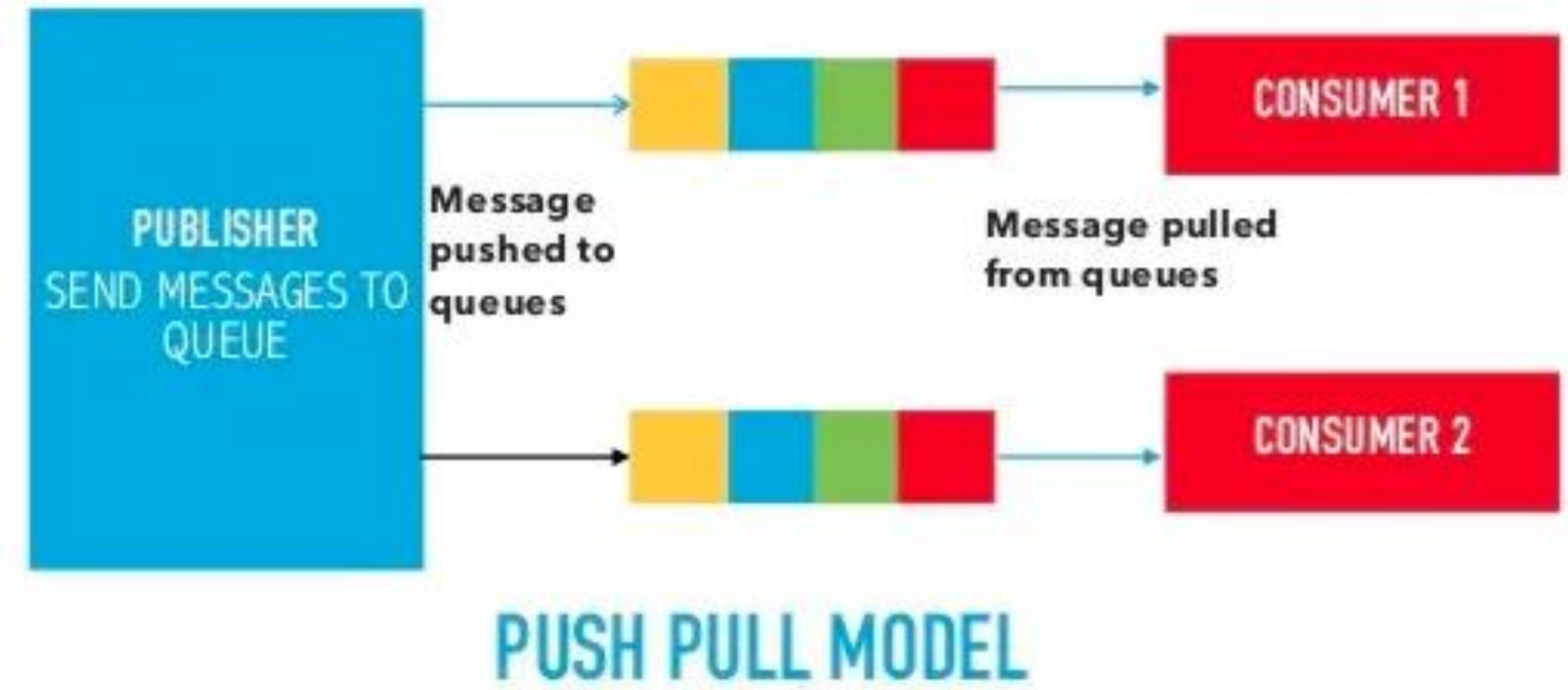
IoT Communication Models

3. 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.
- Queues help in decoupling the messaging between the producer and consumer. Queues also act as a buffer which helps in situations where there is a mismatch between the rate at which the producers push the data and consumers pull the data.

IoT Communication Models

3. Push-Pull Model —



IoT Communication Models

4. Exclusive Pair –

- 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.
- This is a state-full connection model and the server is aware of all open connections.
- WebSocket-based communication API is fully based on this model.

IoT Communication Models

4. Exclusive Pair –

IoT Levels

IoT level 1

- A level-1 IoT system has a single node/device that performs sensing and/or actuation, stores data, performs analysis, and hosts the application
- It is suitable for modeling low-cost and low-complexity solutions where the data involved are not big and the analysis requirements are not computationally intensive.

IoT Level-2

- It has a single node that performs sensing and/or actuation and local analysis (IoT Device and collected data).
- At this, IoT Level Databases and applications establish in Cloud.
- It is useful for solutions where the data involved is big, however, the primary analysis requirement is not computationally intensive and can be done locally itself.

IoT Level-3

- It has a single node.
- Database and applications established in the cloud.
- It is suitable for solutions where the data involved is big and the analysis requirements are computationally intensive.

IoT Level-4

- It has multiple nodes that perform local analysis. It has a Cloud-based application and database.
- This IoT System contains local and cloud-based observer nodes which can subscribe to and receive information collected in the cloud from IoT node devices.
- It is suitable for solutions where we are using multiple nodes, the data involved is big and the analysis requirements are computationally intensive.

IoT Level-5

- It has multiple end nodes and one coordinator node. The end nodes use for sensing and/or actuation.
- In this model, the Coordinator node collects data from the end nodes and transfers it to the cloud.
- In this model, we used a Cloud-based Database for storing and Analyzing data.
- It is suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive.

IoT Level-6

- It has multiple independent end nodes that are used for sensing and/or actuation and transferring data to the cloud.
- We used a Cloud-based database. The analytics component analyzes the data and stores the results in the cloud database and the results are visualized with the cloud-based application.
- The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes

Real-World IoT Architecture Example: Smart Cities

- The utilization of IoT architecture is a key factor in the construction of smart cities, which are designed to use technology for enhancing quality life within urban areas.
- Through various networks and sensors being integrated together, such as IoT sensors. Data can be collected from these cities and services such as transportation, safety regulations or energy optimization can be managed more effectively.
- IoT architectures work towards improving how city living works by managing traffic flow better with monitored signals that respond quickly to changes according to real-time analysis done through deployed IoT systems.
- Monitoring air pollution levels while also optimizing power consumption this allows conditions at an urban level improve drastically due its efficiency all thanks those involved who developed it via their involvement in setting up intelligent infrastructure using IOT solutions and innovation .

Real-World IoT Architecture Example: Healthcare

- The utilization of IoT devices and technology is having a major impact on healthcare, enabling remote patient monitoring, telemedicine services, as well as medical device management.
- Through the integration of these technologies into their practices providers are able to provide more efficient care that can result in improved outcomes for patients.
- For example IoT tech allow doctors to measure important vital signs from afar allowing them greater oversight than ever before while also providing physicians with early warning signals should an emergency arise.
- This architecture even enables access to specialists via tele-consultations regardless if they live near or far helping those who lack healthcare options get better treatments when needed.

Real-World IoT Architecture Example-Agriculture

- Using IoT sensors, farmers are able to collect data on soil moisture, temperature and nutrient levels – thus making precision farming possible as they will have accurate information available for application of water, fertilizer or pesticides precisely required for optimal crop growth.
- Monitoring systems like drones and satellite images provide valuable insight regarding yields which allows them make informed decisions concerning crop management.
- This same technology can be used to monitor livestock health too while increasing sustainability in agriculture practices with an additional advantage towards global food security through better efficiency gained from utilizing the power of IoT technology throughout all aspects related to farming activities.

THANK YOU