Technologies used to Enable IoT

- **Wi-Fi:** Operating in the 2.4 GHz and 5 GHz bands, Wi-Fi is widely used for wireless internet access.
- **Bluetooth:** Operating in the 2.4 GHz band, Bluetooth is used for short-range wireless communication between devices, such as headsets, speakers, and peripherals.
- **Zigbee:** Operating in the 2.4 GHz, 915 MHz, and 868 MHz bands, Zigbee is a low-power wireless mesh network protocol often used for home automation and industrial applications.
- **Z-Wave:** Operating in the 908.42 MHz and 868.42 MHz bands, Z-Wave is another low-power wireless mesh network protocol commonly used for home automation.
- **RFID:** Operating in various ISM bands depending on the application, RFID is used for tracking and identifying objects.
- **Wireless sensors:** Operating in various ISM bands, wireless sensors are used for monitoring environmental conditions, such as temperature, humidity, and light.
- **Industrial wireless:** Operating in various ISM bands, industrial wireless is used for machine-to-machine communication in industrial settings.
- **Wireless microphones:** Operating in the 2.4 GHz and 6 GHz bands, wireless microphones are used for audio transmission in various applications, such as live performances and broadcasting.

M2M – MACHINE TO MACHINE

Machine-to-machine is used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans.

Artificial intelligence (AI) and machine learning (ML) facilitate the communication between systems, allowing them to make their own autonomous choices.

M2M technology was first adopted in manufacturing and industrial settings helped remotely manage and control data from equipment.

M2M has since found applications in other sectors, such as healthcare, business and insurance. M2M is also the foundation for the internet of things (IoT).

The main purpose of machine-to-machine technology is to tap into sensor data and transmit it to a network.

M2M systems often use public networks and access methods -- for example, cellular or Ethernet -- to make it more cost-effective.

M2M Vs IoT

Feature	M2M	IoT
Focus	Machine-to-machine communication	Connected devices and data
Communication	Traditional protocols	Internet protocols
Scope	Limited	Broader
Functionality	Data exchange	Monitoring, control, automation

Here's a comparison of **M2M (Machine-to-Machine)** and **IoT (Internet of Things)** technologies in a tabular form:

Feature	M2M (Machine-to-Machine)	IoT (Internet of Things)
Definition	Direct communication between machines without human intervention.	A network of interconnected smart devices communicating via the internet.
Connectivity	Uses wired or cellular networks (e.g., SIM cards, private networks).	Uses the internet, Wi-Fi, Bluetooth, LPWAN, or cloud-based connectivity.
Scope	Limited to specific machine-based communication.	Broader scope, connecting multiple devices and systems globally.
Data Handling	Processes data locally or in a closed network.	Uses cloud platforms for storage, processing, and analytics.
Flexibility	Less flexible, typically designed for fixed functions.	More flexible, allows dynamic interactions and updates.
Communication	Point-to-point communication between devices.	Many-to-many communication, enabling data sharing across multiple devices.
Scalability	Less scalable, usually confined to specific industries.	Highly scalable, supports large networks of devices.
Examples	Smart meters, industrial automation, ATMs.	Smart homes, connected healthcare, smart cities.
Dependency on Cloud	Minimal or no cloud integration.	Strong reliance on cloud services for data processing and management.
Data Processing	Processes data at the device level.	Data is processed and analyzed in the cloud or edge devices.
Security	More secure due to isolated networks.	Higher security concerns due to internet connectivity.

In summary, **M2M** is a subset of **IoT**, focusing on direct machine communication, while **IoT** leverages cloud and internet connectivity for broader, smarter interactions.

UNIT-III

DESIGN AND DEVELOPMENT

IoT Design Methodology – Steps

Step 1: Purpose & Requirements Specification • The first step in IoT system design methodology is to define the purpose and requirements of the system. In this step, the system purpose, behavior and requirements (such as data collection requirements, data analysis requirements, system management requirements, data privacy and security requirements, user interface requirements, ...) are captured.

Step 2: Process Specification • The second step in the IoT design methodology is to define the process specification. In this step, the use cases of the IoT system are formally described based on and derived from the purpose and requirement specifications.

Step 3: Domain Model Specification • The third step in the IoT design methodology is to define the Domain Model. The domain model describes the main concepts, entities and objects in the domain of IoT system to be designed. Domain model defines the attributes of the objects and relationships between objects. Domain model provides an abstract representation of the concepts, objects and entities in the IoT domain, independent of any specific technology or platform. With the domain model, the IoT system designers can get an understanding of the IoT domain for which the system is to be designed.

Step 4: Information Model Specification • The fourth step in the IoT design methodology is to define the Information Model. Information Model defines the structure of all the

IEEE 802.15.4: MAC Layer, Topology, and Security

IEEE 802.15.4 is a standard for **low-power, low-data-rate** wireless communication, widely used in **IoT applications** like smart homes and sensor networks.

1. MAC Layer (Medium Access Control)

- It controls how devices communicate over the wireless channel.
- Uses **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** to reduce interference.
- Supports **beacon-enabled** (synchronized) and **non-beacon-enabled** (unsynchronized) modes.
- Handles device addressing, frame formatting, and error detection.

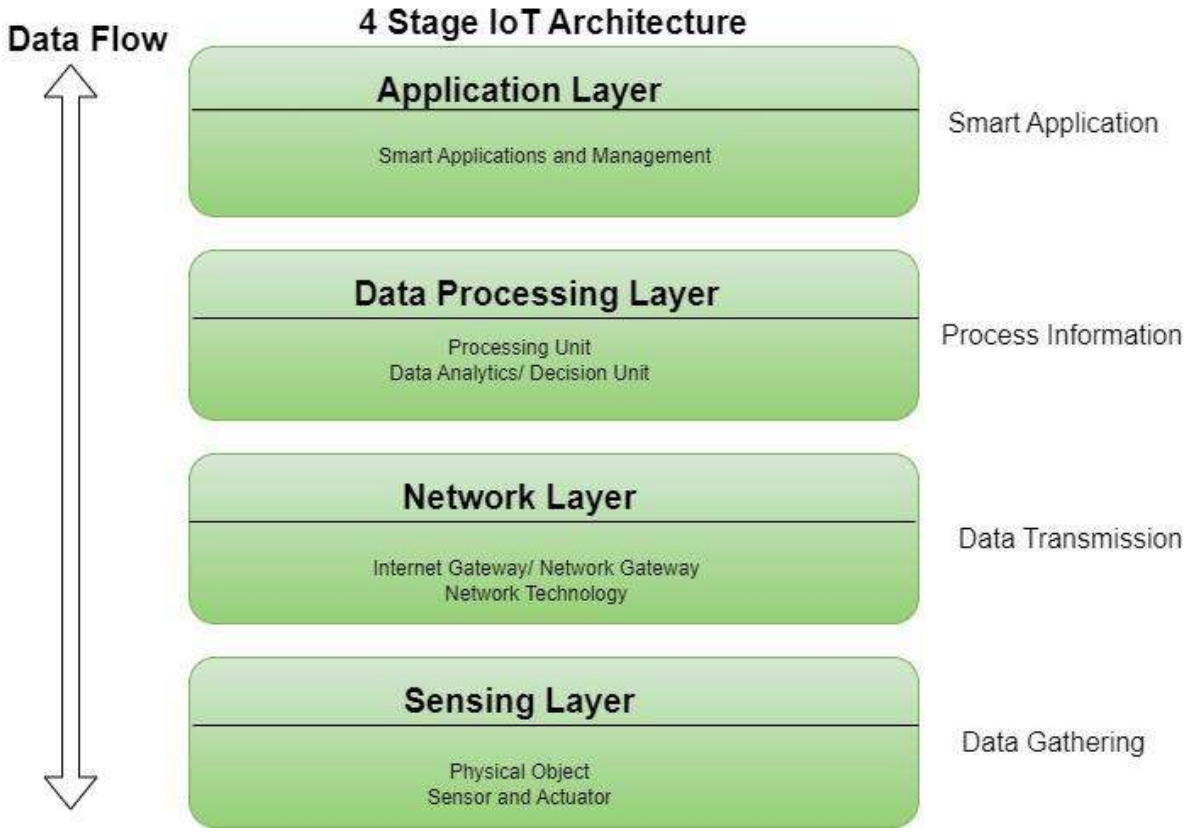
2. Topology

IEEE 802.15.4 supports three types of network structures:

- **Star Topology**: A central **coordinator** manages communication with multiple end devices.
- **Tree Topology**: Devices are arranged in a hierarchical structure with parent-child relationships.
- **Mesh Topology**: Devices can communicate directly with each other, improving reliability.

3. Security Features

- **AES-128 Encryption** ensures secure communication.
- Supports **authentication** to prevent unauthorized access.
- **Frame integrity check** protects against data tampering.



Simplified IoT Architecture (4 Layers)

1. Perception Layer (Sensing Layer) 📡

- The **physical layer** where IoT devices collect real-world data.
- Includes **sensors, actuators, cameras, RFID tags, GPS, etc.**
- Example: A temperature sensor measuring room temperature.

2. Network Layer (Communication Layer) 🌐

- Transfers data from the Perception Layer to processing units.
- Uses **Wi-Fi, Bluetooth, Zigbee, LoRa, 5G, etc.** for communication.
- Example: A smart thermostat sending temperature data to the cloud via Wi-Fi.

3. Data Processing Layer (Edge or Middleware Layer) 🖥️

- Processes data **locally (edge computing)** or on cloud servers.
- Reduces **latency** and makes **real-time decisions** before sending to applications.
- Example: An edge device filtering out unnecessary temperature data before sending it to the cloud.

4. Application Layer (User Interaction) 📲

- Displays processed data to users through **mobile apps, dashboards, or web interfaces**.

- Provides **notifications, analytics, and automation**.
- Example: A mobile app showing real-time temperature readings and sending alerts if the room is too hot.