MONTH OF TECH : IOT

IOT SESSION-1: INTRODUCTION TO IOT

WHAT IS IOT ?

The Internet of Things (IoT) is a network of connected devices that can communicate with each other, share data, and perform tasks without human intervention. The importance of communication in IoT cannot be overstated, as it is the foundation on which the entire system is built. The devices that make up the IoT ecosystem need to be able to communicate with each other in order to function properly and achieve their intended purpose.

DEFINITION:

Internet of Things (IoT) is the networking of physical objects that contain electronics embedded within their architecture in order to communicate and sense interactions amongst each other or with respect to the external environment.

WHY WE NEED IOT?

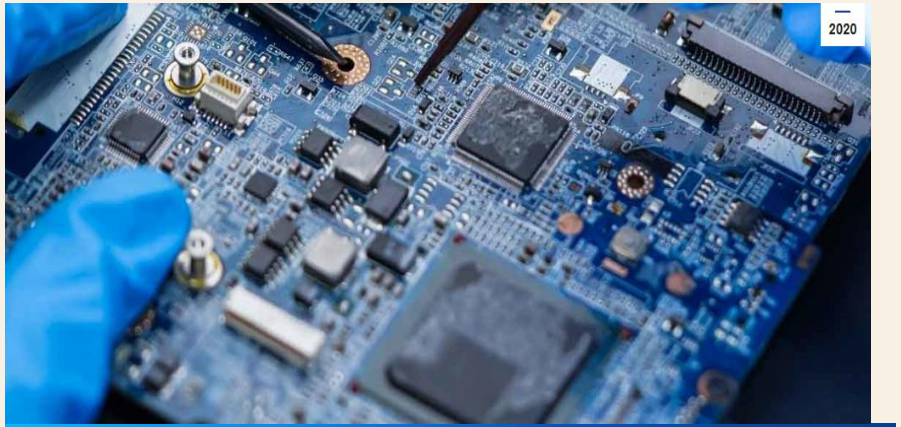
WHAT IS THE WORK OF AN IOT ENGINEER

1.Hardware Development:

1. Designing and integrating sensors, actuators, and microcontrollers.
2. Ensuring energy efficiency and durability.

2.Software Development and embedded systems :

1. Programming device firmware and developing IoT applications.
2. Debugging and optimizing system performance.



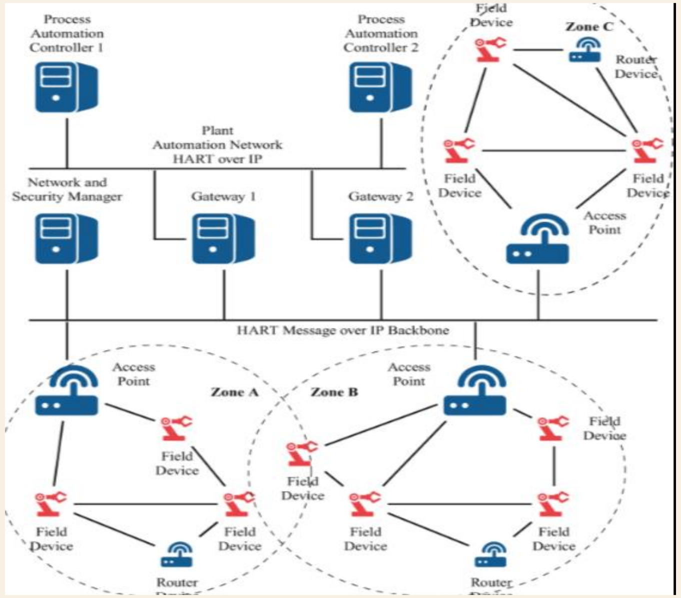
WHAT IS THE WORK OF AN IOT ENGINEER

3. **Networking:**

- Implementing and managing communication protocols (e.g., MQTT, CoAP, HTTP/HTTPS).
- Establishing secure and reliable device connectivity.

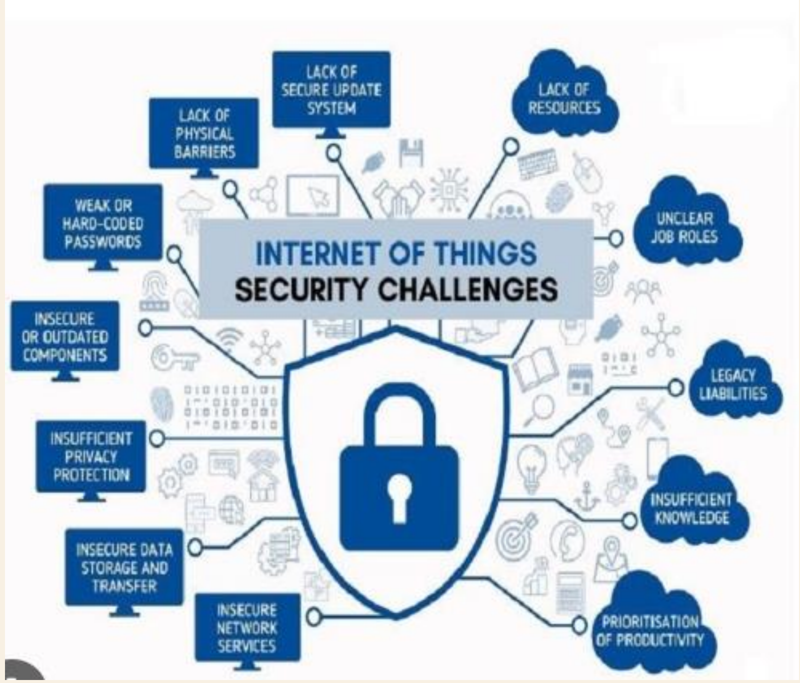
4.Data Management:

- Collecting, processing, and analyzing data for actionable insights.
- Using tools like cloud platforms and edge computing for efficient data handling.

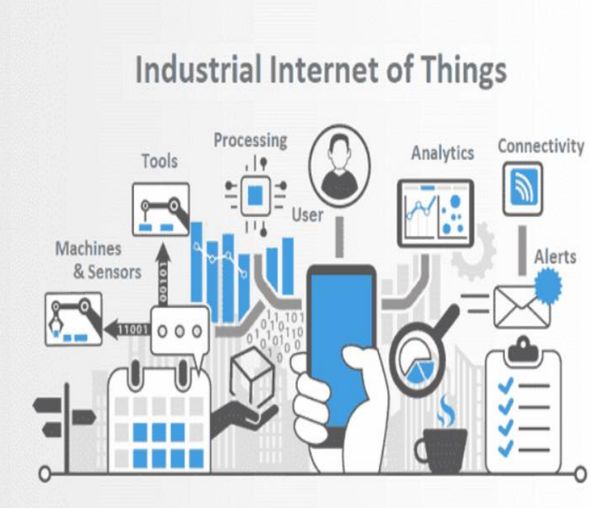


WHAT IS THE WORK OF AN IOT ENGINEER

•**Security:**
As networks of devices proliferate, cybersecurity is a top priority area for iot engineering. They have in-depth knowledge of security best practices, protocols, and technologies to protect IoT systems and the data they generate. Developers implement multi-factor authentication and access control mechanisms to restrict unauthorized access and privileges. Encryption standards like TLS are applied to transmitted data for confidentiality and prevention of snooping.


INTERNET OF THINGS
SECURITY CHALLENGES
LACK OF SECURE UPDATE SYSTEM
LACK OF PHYSICAL BARRIERS
LACK OF RESOURCES
WEAK OR HARD-CODED PASSWORDS
UNCLEAR JOB ROLES
INSECURE OR OUTDATED COMPONENTS
LEGACY LIABILITIES
INSUFFICIENT PRIVACY PROTECTION
INSUFFICIENT KNOWLEDGE
INSECURE DATA STORAGE AND TRANSFER
INSECURE NETWORK SERVICES
PRIORITISATION OF PRODUCTIVITY

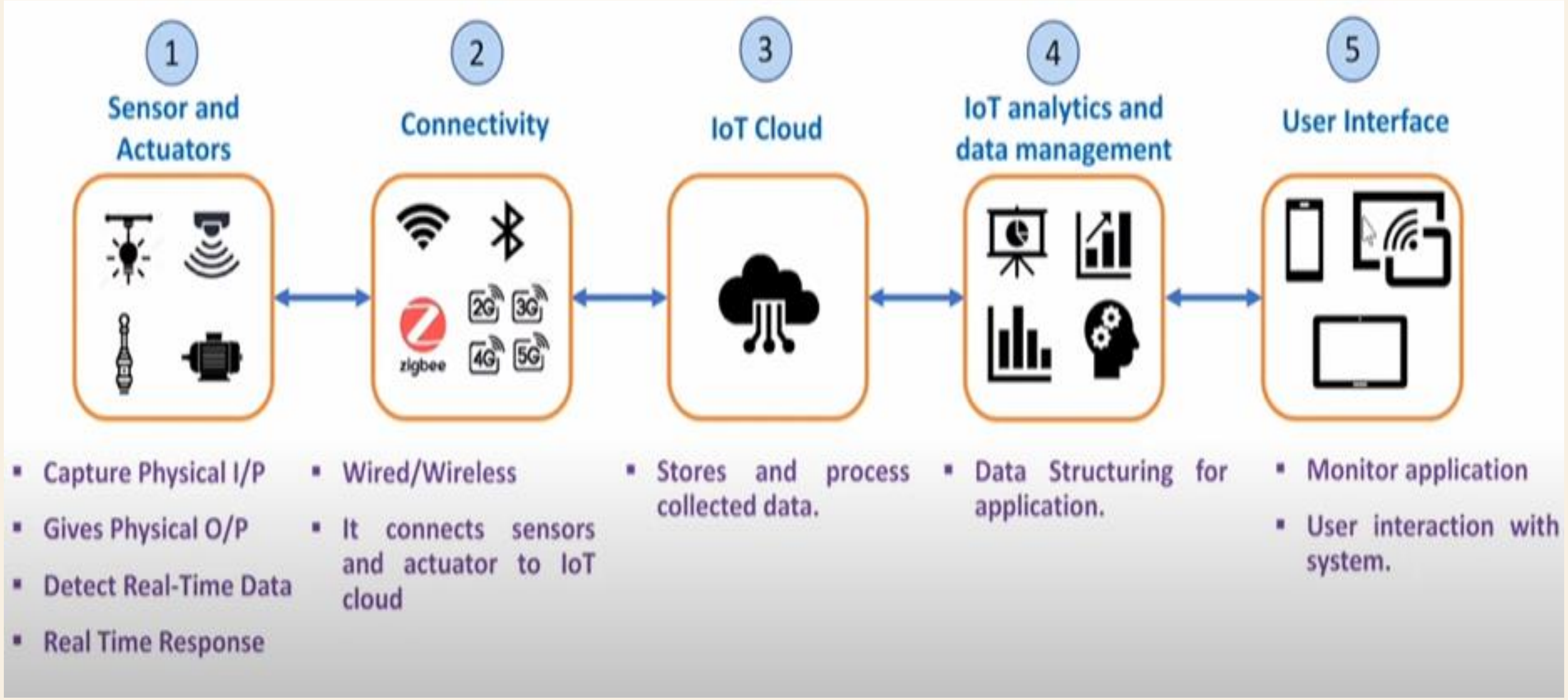
WHERE IS IOT USED?



- Wherever there is a connection between them for sharing information

1. **Smart Homes:**
   1. Connected devices like smart lights, thermostats, and security systems.
2. **Healthcare:**
   1. Wearable health monitors, remote patient care, and smart medical devices.
3. **Industrial IoT (IIoT):**
   1. Predictive maintenance, factory automation, and inventory management.
4. **Transportation:**
   1. Fleet management, connected vehicles, and traffic monitoring.
5. **Agriculture:**
   1. Precision farming, smart irrigation, and livestock monitoring.

COMPONENTS OF IOT



1 Sensor and Actuators

- Capture Physical I/P
- Gives Physical O/P
- Detect Real-Time Data
- Real Time Response

2 Connectivity

- Wired/Wireless
- It connects sensors and actuator to IoT cloud

3 IoT Cloud

- Stores and process collected data.

4 IoT analytics and data management

- Data Structuring for application.

5 User Interface

- Monitor application
- User interaction with system.

THINGS IN IOT :
SENSORS AND ACTUATORS

- **Sensors** :
  Sensors are devices that detect physical, chemical, or environmental changes and convert them into electrical signals for processing.They act as the "eyes and ears" of IoT systems, capturing data from the environment or a physical object.

- **Actuators** :

Actuators take action based on commands from the IoT system, completing the feedback loop. Actuators are devices that convert electrical signals into physical actions, such as movement, heating, or light generation

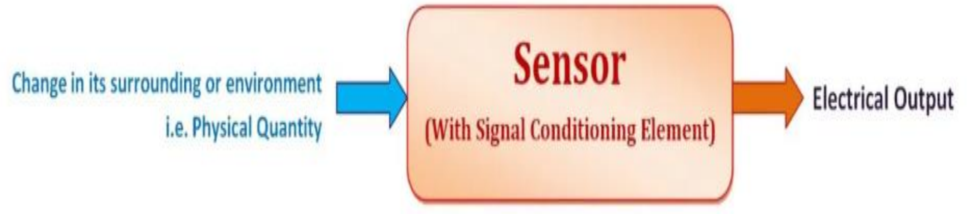

Change in its surrounding or environment
i.e. Physical Quantity
Sensor
(With Signal Conditioning Element)
Electrical Output

Figure- Block Diagram of a Sensor

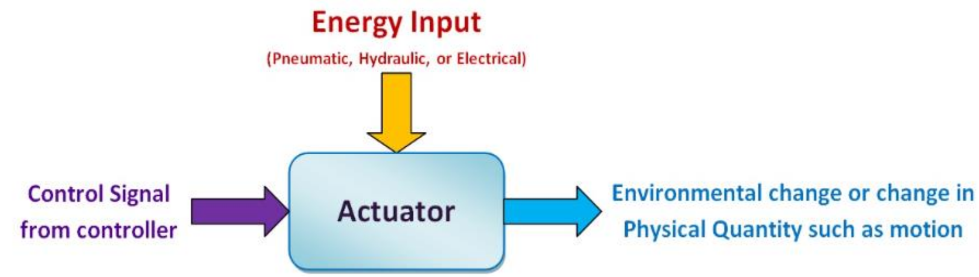

Energy Input
(Pneumatic, Hydraulic, or Electrical)
Control Signal
from controller
Actuator
Environmental change or change in
Physical Quantity such as motion

Figure- Block diagram of an actuator

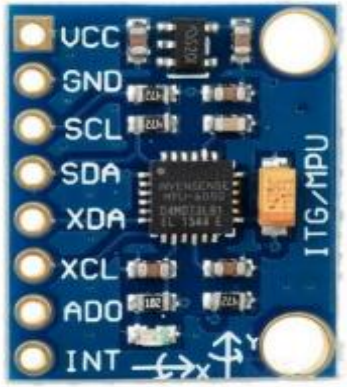
SENSORS:

Ultrasonic Proximity Sensor

Infrared Proximity Sensor

Microwave Radar Sensor

PIR Motion Sensor



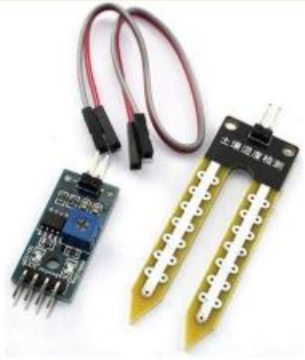
Gyroscope

Capacitive Touch Sensor

Barometric Pressure Sensor

SENSORS:

Water meter

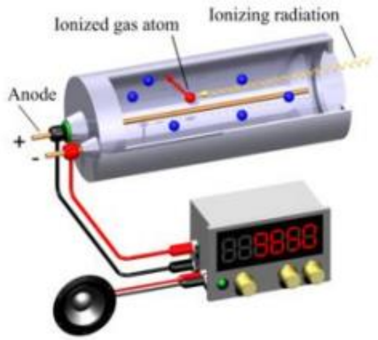


Soil moisture sensor

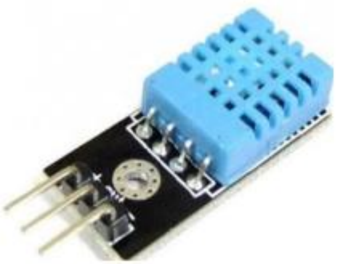
LDR light sensor

Flame sensor

Neutron detector



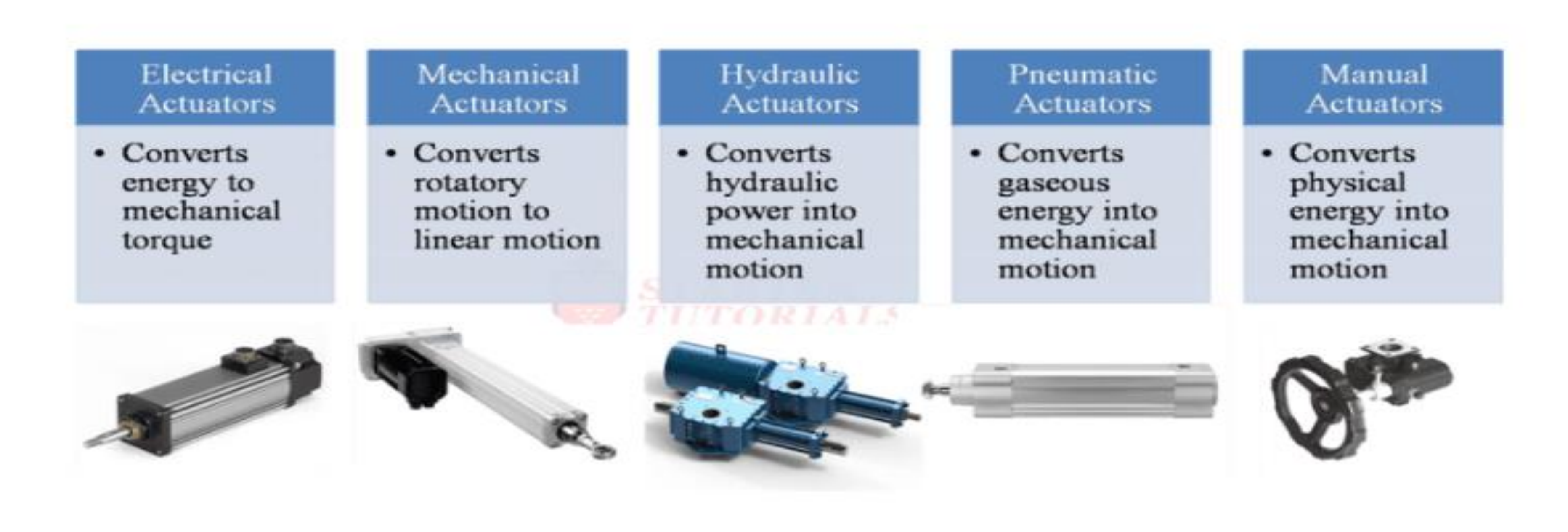
Geiger-Muller counter



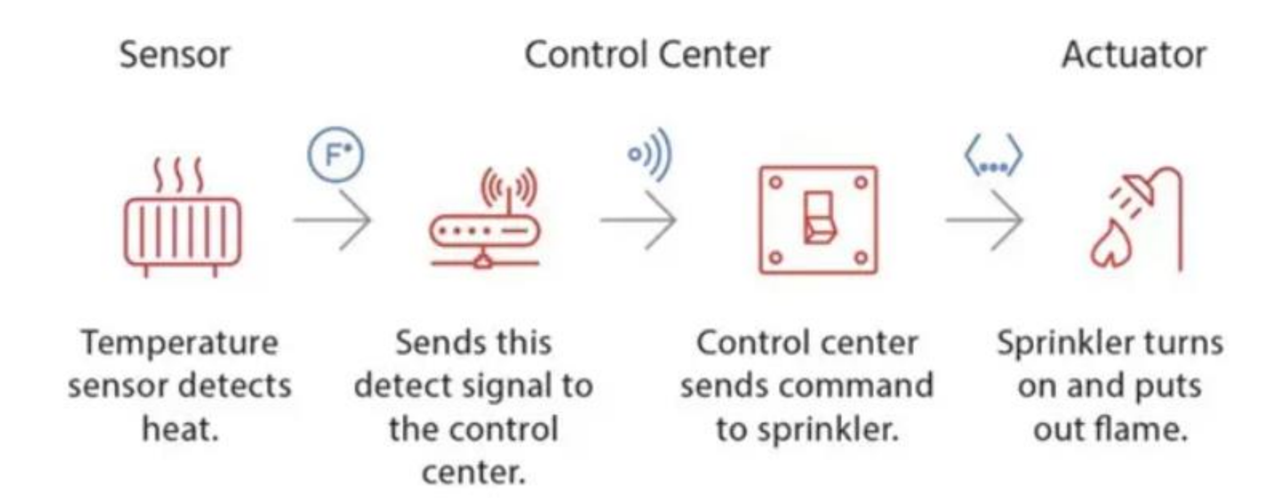
Temperature Sensor

Thermo-Hygrometer

ACTUATORS:



Electrical Actuators	Mechanical Actuators	Hydraulic Actuators	Pneumatic Actuators	Manual Actuators
• Converts energy to mechanical torque	• Converts rotatory motion to linear motion	• Converts hydraulic power into mechanical motion	• Converts gaseous energy into mechanical motion	• Converts physical energy into mechanical motion



Sensor → Control Center → Actuator

Temperature sensor detects heat.

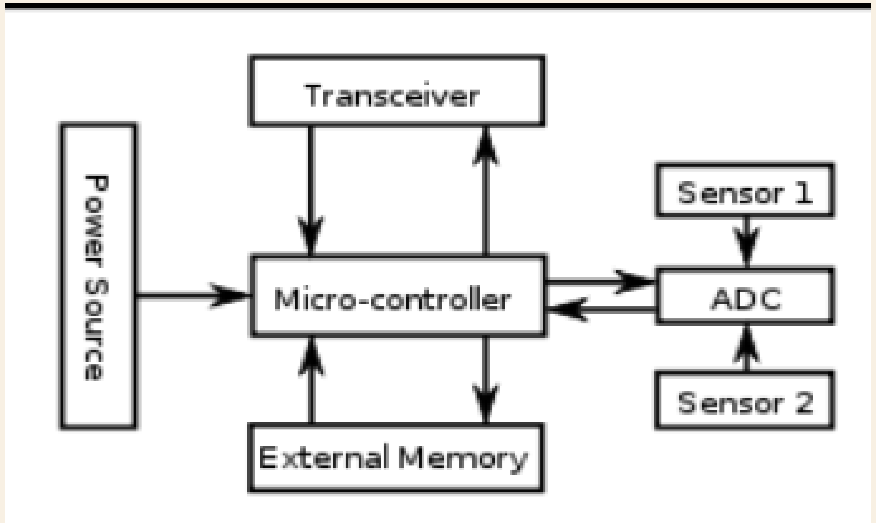
Sends this detect signal to the control center.

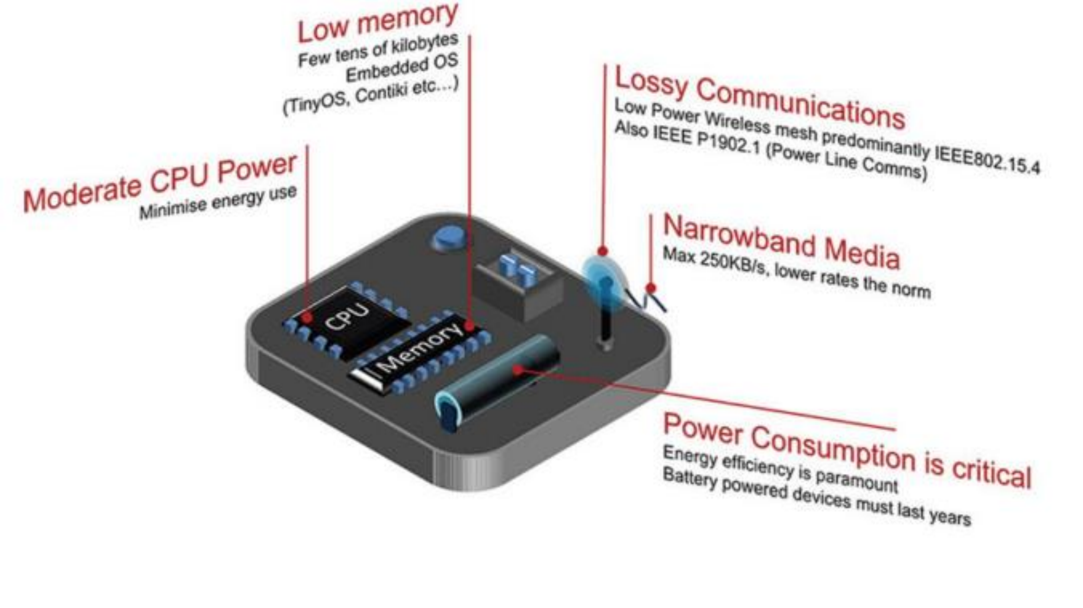
Control center sends command to sprinkler.

Sprinkler turns on and puts out flame.

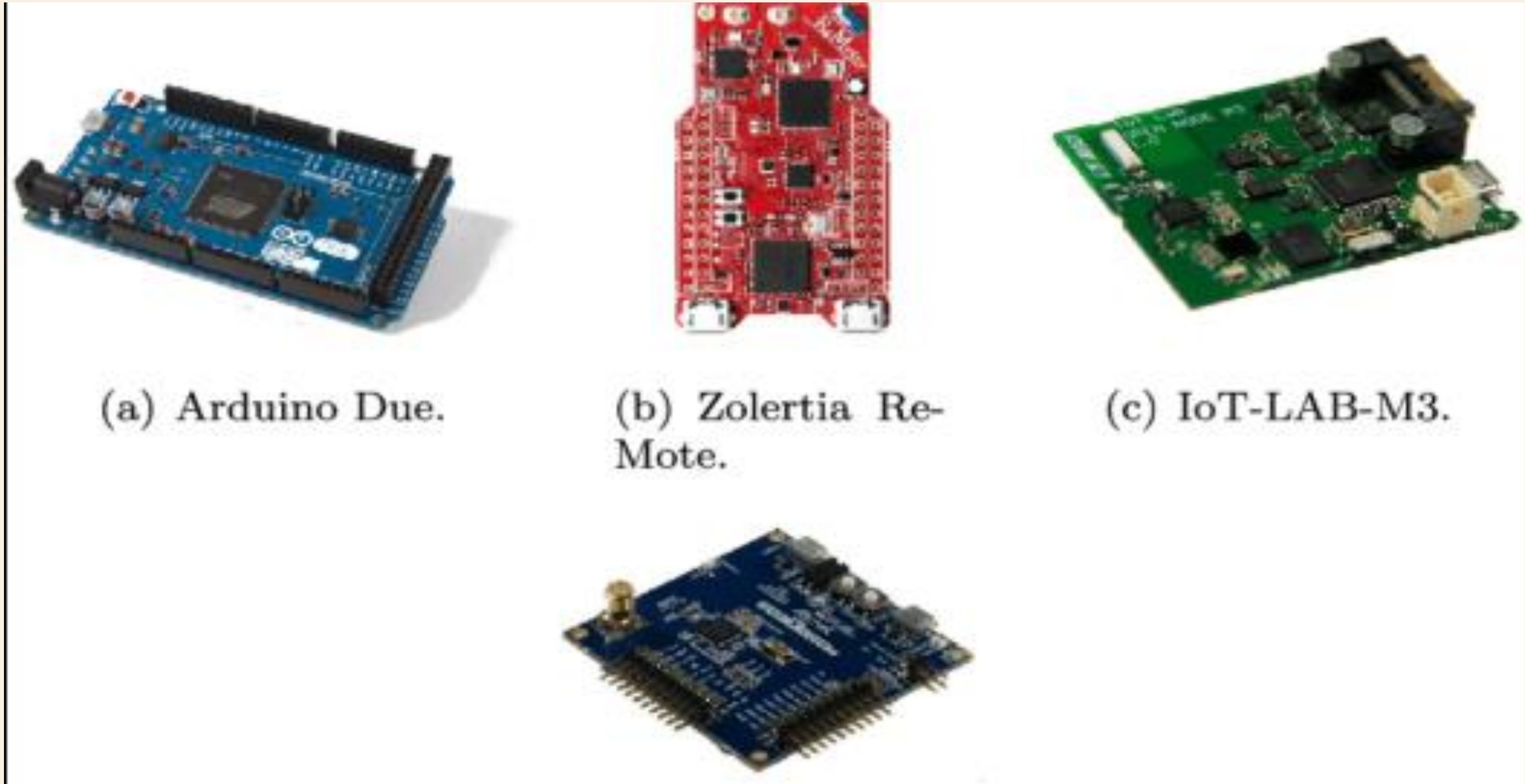
SMART DEVICES

- Smart object has the following five characteristics: – Sensor(s) and/or Actuator(s) – Processing unit
- For acquiring sensed data from sensors,
- processing and analysing sensing data
- coordinating control signals to any actuators, and
- controlling many functions (e.g. communication unit, power unit).
- Memory mostly on-chip flash memory
- user memory used for storing application related data
- program memory used for programming the device Communication unit
- Responsible for connecting a smart object with other smart objects and the outside world (via the network using wireless/wired communication) – Power source
- To powered all components of the smart object





Low memory
Few tens of kilobytes
Embedded OS
(TinyOS, Contiki etc...)
Moderate CPU Power
Minimise energy use
Lossy Communications
Low Power Wireless mesh predominantly IEEE802.15.4
Also IEEE P1902.1 (Power Line Comms)
Narrowband Media
Max 250KB/s, lower rates the norm
Power Consumption is critical
Energy efficiency is paramount
Battery powered devices must last years
CPU
Memory



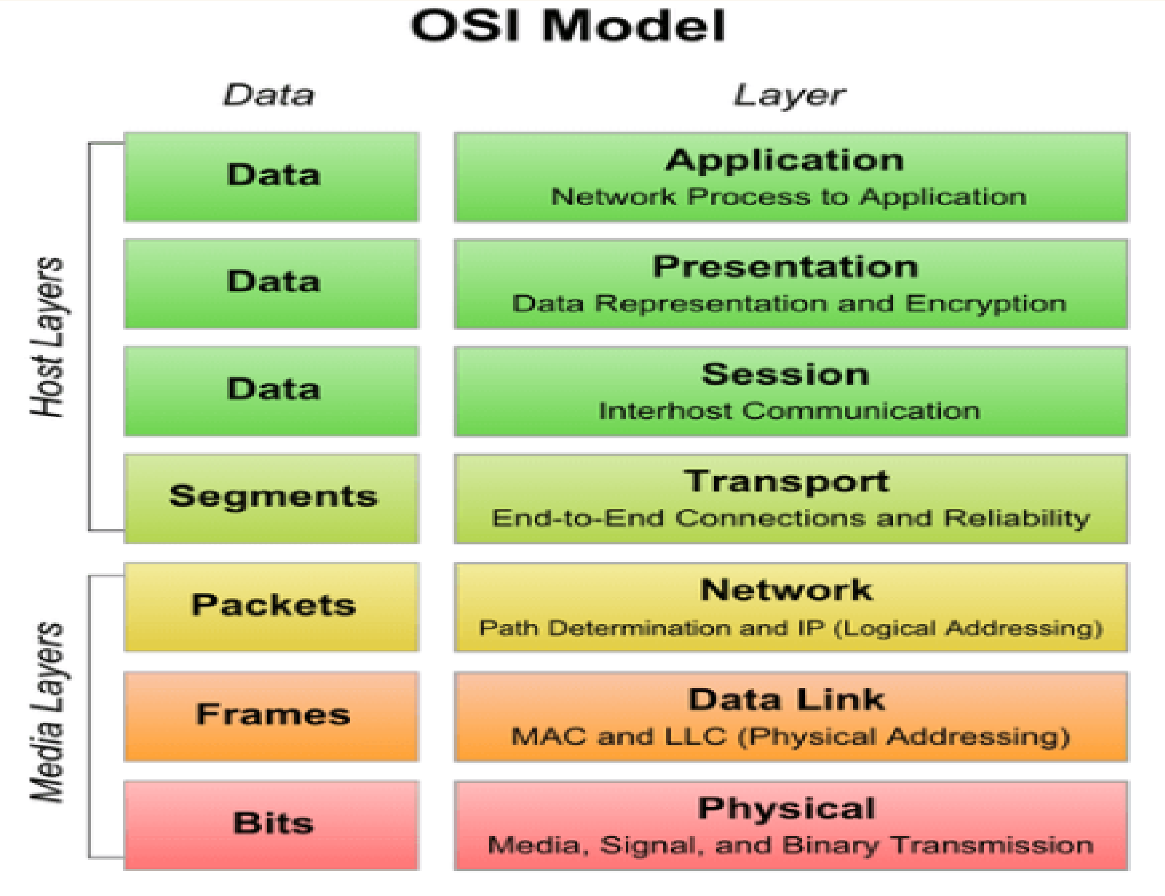
(a) Arduino Due.

(b) Zolertia Re-Mote.

(c) IoT-LAB-M3.

(d) Atmel SAM R21.

STANDARD OSI MODEL



OSI Model

	Data	Layer
Host Layers	Data	**Application** Network Process to Application
	Data	**Presentation** Data Representation and Encryption
	Data	**Session** Interhost Communication
	Segments	**Transport** End-to-End Connections and Reliability
Media Layers	Packets	**Network** Path Determination and IP (Logical Addressing)
	Frames	**Data Link** MAC and LLC (Physical Addressing)
	Bits	**Physical** Media, Signal, and Binary Transmission

NETWORKING AND CONNECTIVITY :

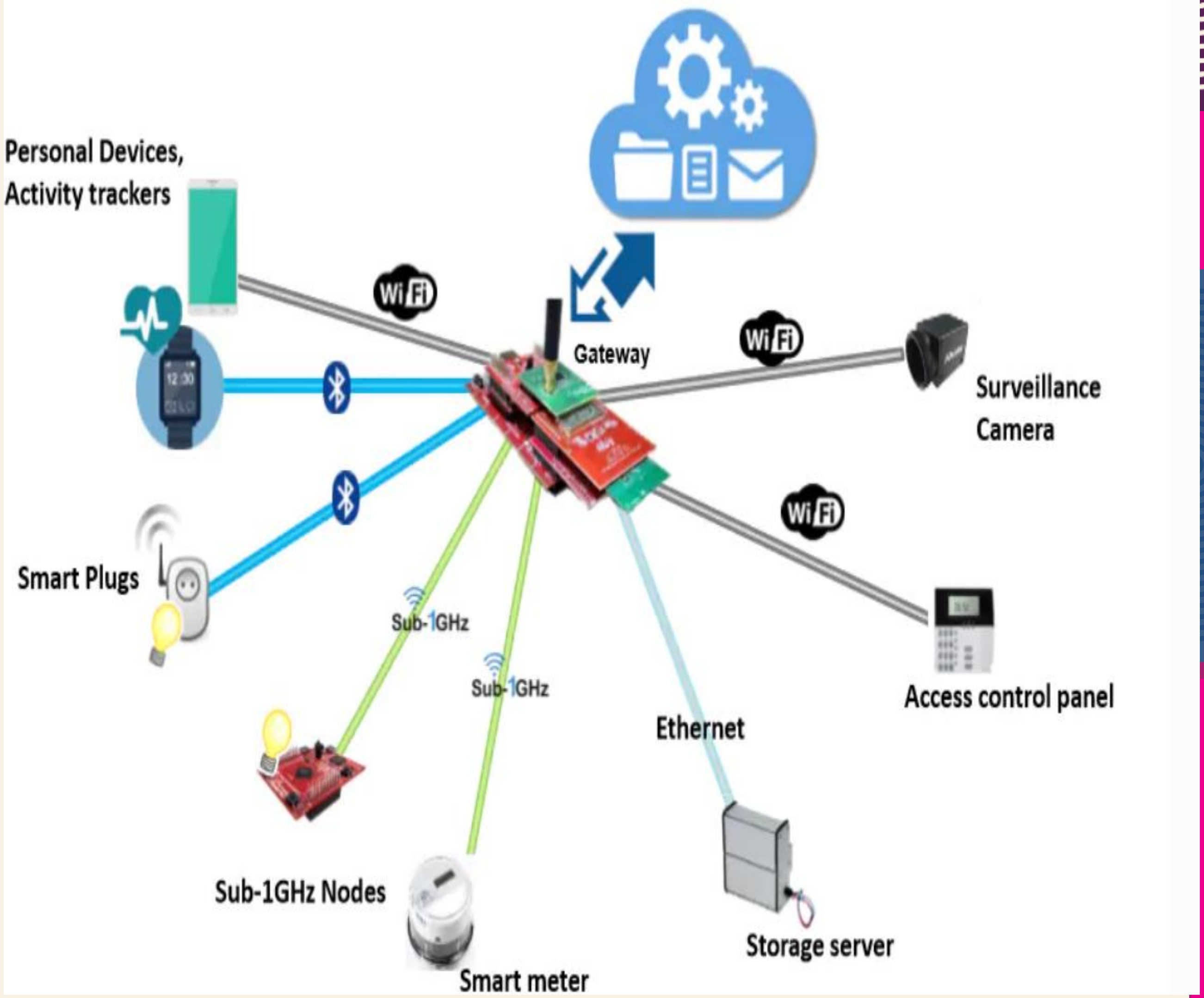
- Key words:

➢ Device
➢ Gateway
➢ Server
➢ Cloud

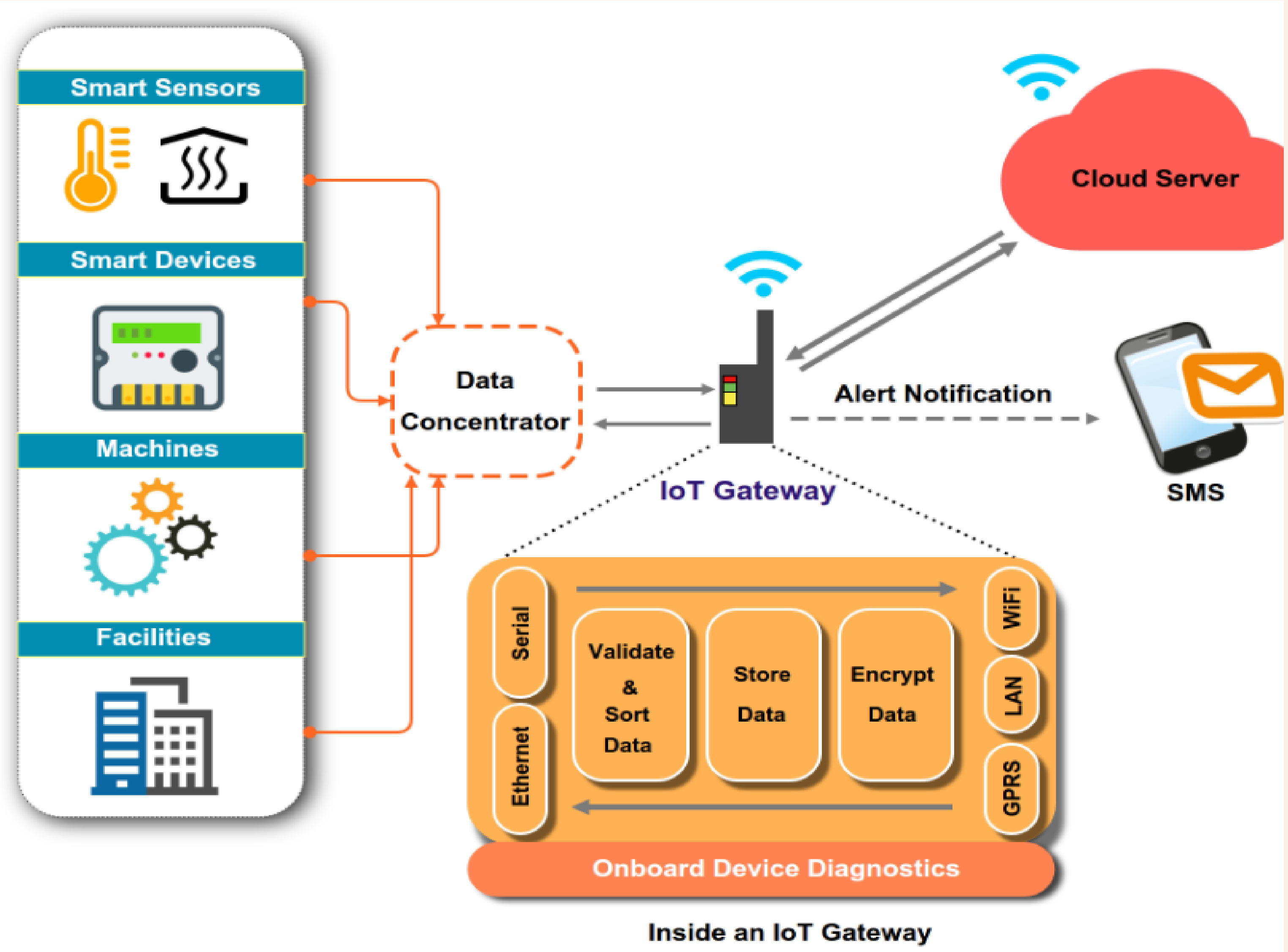
Device:
In IoT, a device refers to any physical object or hardware component that can connect to the internet and perform specific tasks, such as sensing, data collection, communication, or actuation. These devices are often embedded with sensors, actuators, microcontrollers, and communication modules to enable them to interact with their environment and other devices or systems.

IOT GATEWAY

Gateway provides a bridge between different communication technologies which means we can say that a Gateway acts as a medium to open up connections between the cloud and controller(sensors/devices) in Internet of Things (IoT). With the help of gateways, it is possible to establish device-to-device or device-to-cloud communication. A gateway can be a typical hardware device or software program. It enables a connection between the sensor network and the Internet along with enabling IoT communication.



- An iot gateway is more smarter than a router that we use .
- It not only receive the data but it process the data based on different protocols and sends the data to an application or cloud through different types of communications .



The key function of iot gateway :

- Data collection
- Protocol translation
- Data filtering and preprocessing
- Secure communication
- Two-way robust ciommunication

THEN WHAT ARE ROUTERS ?

A router acts as the traffic director of your network. It receives data packets, analyzes their digital addresses (similar to street addresses), and then forwards them to the intended device on the network. Data travels in packets, small chunks of information containing the source, destination, and the actual data itself. The router deciphers the destination address within each packet, ensuring it reaches the correct computer, printer, or other device connected to the network. They typically work on ip addresses and follow only a fixed data packet format.

EXAPLES OF IOT GATEWAY :

- **Intel® IoT Gateway**
- **Features**:
  - Supports multiple operating systems.
  - Scalable for large deployments.
  - Robust security features.
- **Cisco IR1101 Integrated Services Router**
- **Features**:
  - Modular design for flexibility.
  - Supports LTE, Wi-Fi, and Ethernet connectivity.
  - Advanced security and remote management capabilities.

WHY WE NEED GATEWAYS

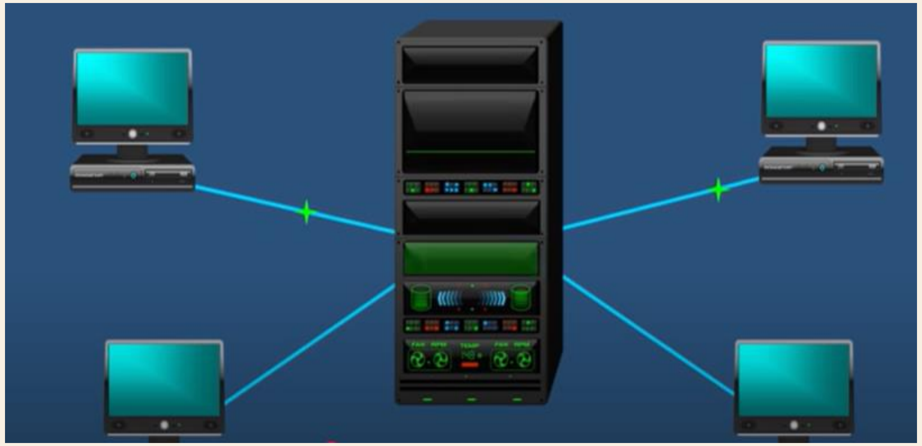
- Due to diverse communication protocols that we have
- Many IoT devices are designed to be cost-effective and energy-efficient, which limits their computing power and network connectivity options.
- High bandwidth usage without a gateway
- Security risks as ioT devices are vulnerable to hacking, and direct communication with the cloud exposes them to additional security risks.
- Lack of real time operation due to latency in the iot devices .
- Complexity in networking due to increase in the number of iot devices

SERVER:

A server is a computer or software application that provides services, resources, or data to other devices, known as clients, over a network.

- It listens the request from client
- Process the request like retrieving the data that is requested through running some scripts through its memory or resources
- Sending the requesting data
- Ex:
- Webserver
- Data base server
- Mail server

➢ It uses high performance process in more than one (intel xenon)



Cloud:

cloud is a big building consisting a lot of servers which provides storage ,processing , managment services of the data provides by iot devices

Famous iot cloud platforms are

- AWS IOT CORE
- MICROSOFT AZURE IOT HUB
- GOOGLE IOT CLOUD

TYPES OF COMMUNICATION

Device-to-Device Communication
Device-to-device communication allows two IoT devices to exchange data directly without relying on a central gateway or cloud service. This model is typically used in scenarios where low latency and direct interaction are required. Protocols like Bluetooth, Zigbee, or Wi-Fi Direct are commonly employed for this purpose. The devices must be within proximity or connected through a shared wireless standard.

•**Examples**:

- A smart lock communicating directly with a smart doorbell to unlock the door when authorized.
- Wearable fitness devices syncing data with a nearby smartphone via Blueto

Device-to-Gateway Communication
In this model, IoT devices send data to a local gateway, which aggregates, processes, and may transmit the data to the cloud. Gateways can provide computational power to preprocess data, reducing the load on cloud infrastructure. This model is ideal for scenarios with multiple devices requiring data aggregation or where internet access may be intermittent.

•**Examples**:

- Smart home devices (lights, thermostats) communicating with a central hub like Amazon Echo.
- Industrial sensors sending real-time production data to a local gateway for immediate analysis.

Device-to-Cloud Communication

IoT devices transmit data directly to the cloud over the internet using protocols such as HTTP, MQTT, or CoAP. The cloud processes, analyzes, and stores the data, often providing a user interface for monitoring and control. This model is suited for scenarios requiring large-scale data analytics or remote monitoring.

- **Examples**:
  - A weather station uploading temperature and humidity data to a cloud server for public access.
  - Smart cameras streaming footage to a cloud-based storage and monitoring service

Device-to-Network Communication

IoT devices communicate with network infrastructure, such as cellular towers or 5G base stations, to transmit data. This model is used when devices are spread across wide areas and need to maintain connectivity with minimal direct device interaction. It relies on communication standards like LTE, NB-IoT, or 5G.

- **Examples**:
  - Smart meters transmitting energy usage data to utility providers via cellular networks.
  - IoT devices in agriculture sending soil moisture data to a cloud platform using NB-IoT.

. **Cloud-to-Cloud Communication**

Cloud-to-cloud communication enables different IoT platforms to share data and functionality, promoting interoperability. This is essential when devices from different ecosystems or services need to collaborate seamlessly. APIs and web services are commonly used for cloud-to-cloud integration.

•**Examples**:

- A fitness tracker's cloud sharing activity data with a diet tracking app's cloud for health insights.
- A smart home platform communicating with a weather service cloud to adjust indoor settings based on forecasts.

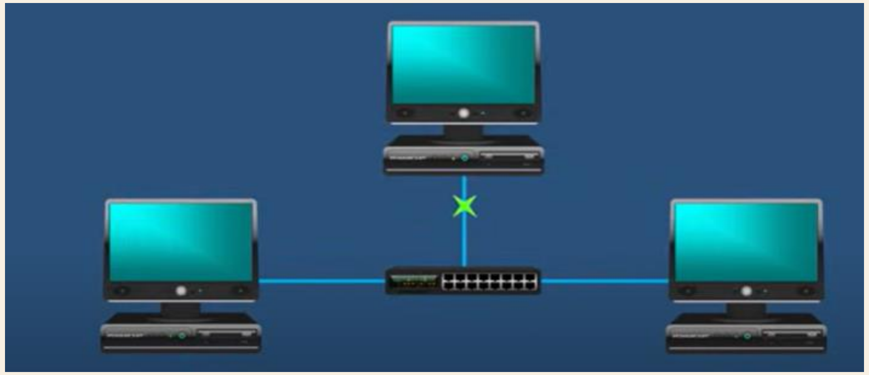
- **Broadcast or Multicast Communication**

Broadcast communication sends data to all devices in a network, while multicast targets a specific group of devices. This model is used for scenarios requiring simultaneous updates or notifications to multiple devices. It is efficient for disseminating the same data to multiple endpoints.

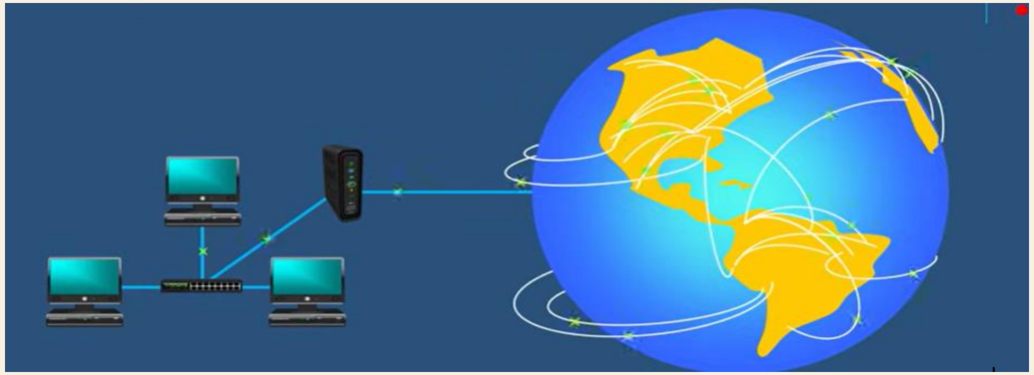
•**Examples**:

- A smart irrigation controller broadcasting soil moisture alerts to all farmers in a region.
- An emergency alert system multicasting weather warnings to IoT devices in a specific geographic area.

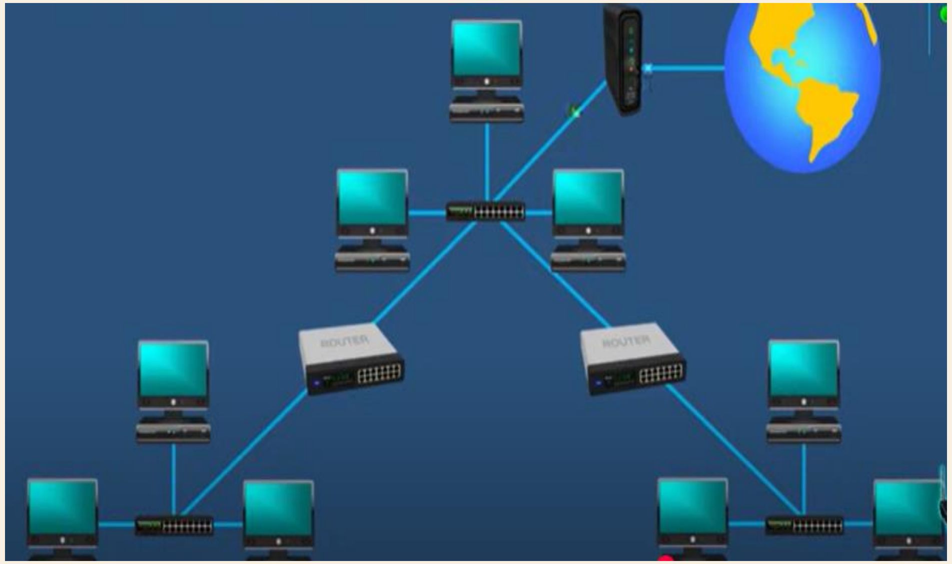
NETWORKING BASICS :



A Local Area Network (LAN) connects devices within a small geographic area, such as a home, office, or campus. It uses Ethernet or Wi-Fi to provide high-speed communication and allows devices to share resources like printers and servers. LANs are privately managed and operate independently of external networks, making them ideal for localized IoT setups like smart homes.



A Wide Area Network (WAN) connects multiple LANs and other networks over large geographic areas, such as cities, countries, or continents. The internet is the most common example, using infrastructure like fiber optics, satellites, or cellular networks to enable global communication



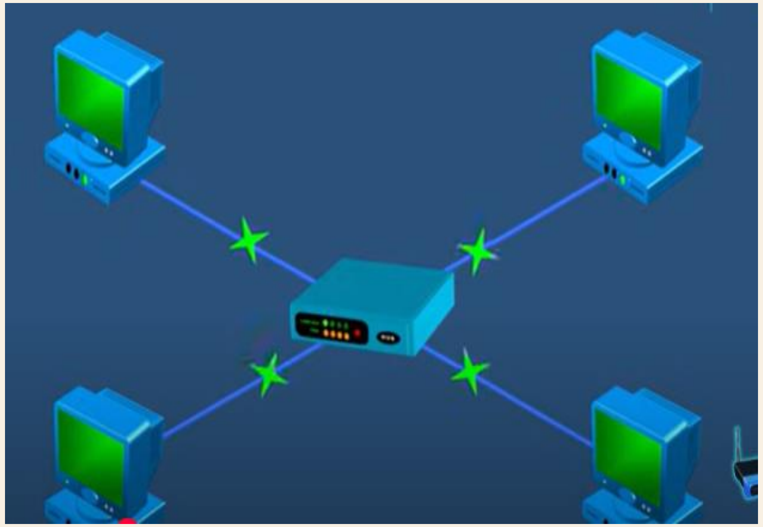
SUBNET

NETWORKING DEVICES :

- Router
- Switch
- Hub
- Modem
- Repeater
- Network interfacing card(NIC)
- Gateway

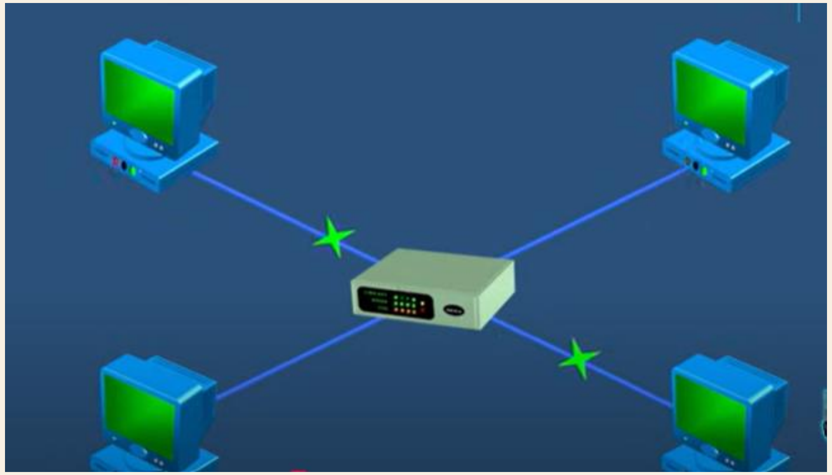
HUB:

Hubs operate by receiving data signals from connected devices and rebroadcasting them to all other devices. When a device sends data, the hub receives the signal and immediately broadcasts it to all other connected devices. This broadcast approach is known as "store-and-forward" transmission, where the hub doesn't perform any data filtering or processing.

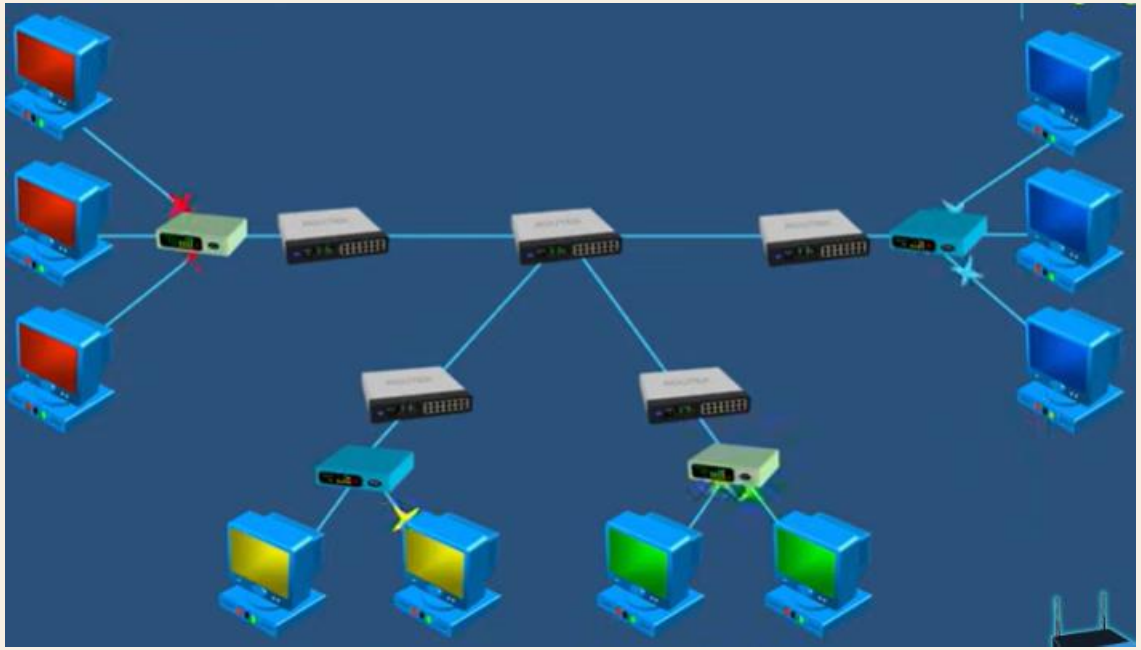


- **SWITCH:**

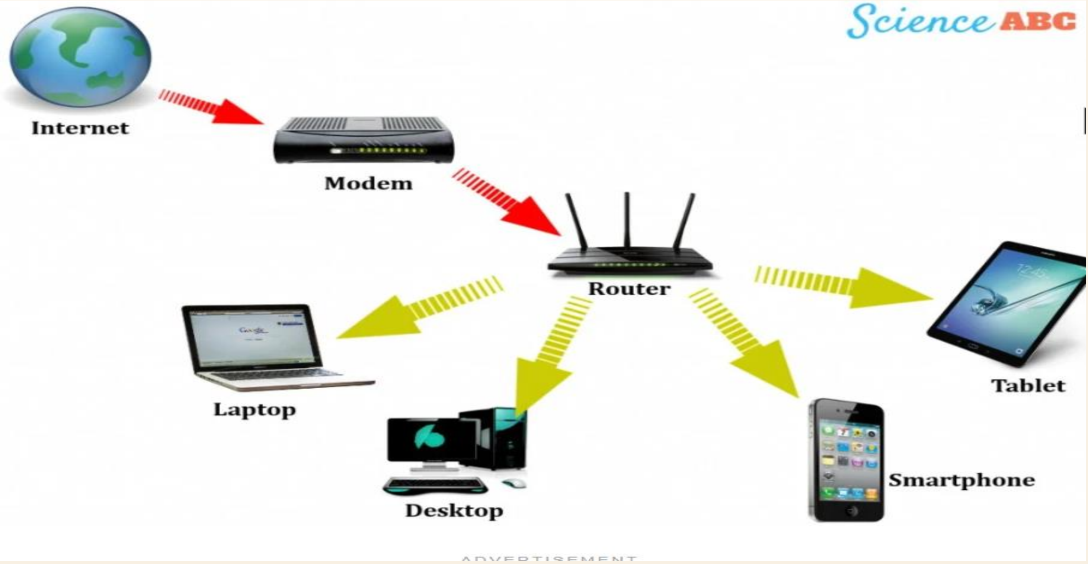
A network switch connects network devices (printers, computers, and wireless devices/access points, and enables users to exchange data packets. Switches may be both hardware and software-based virtual devices that govern physical system

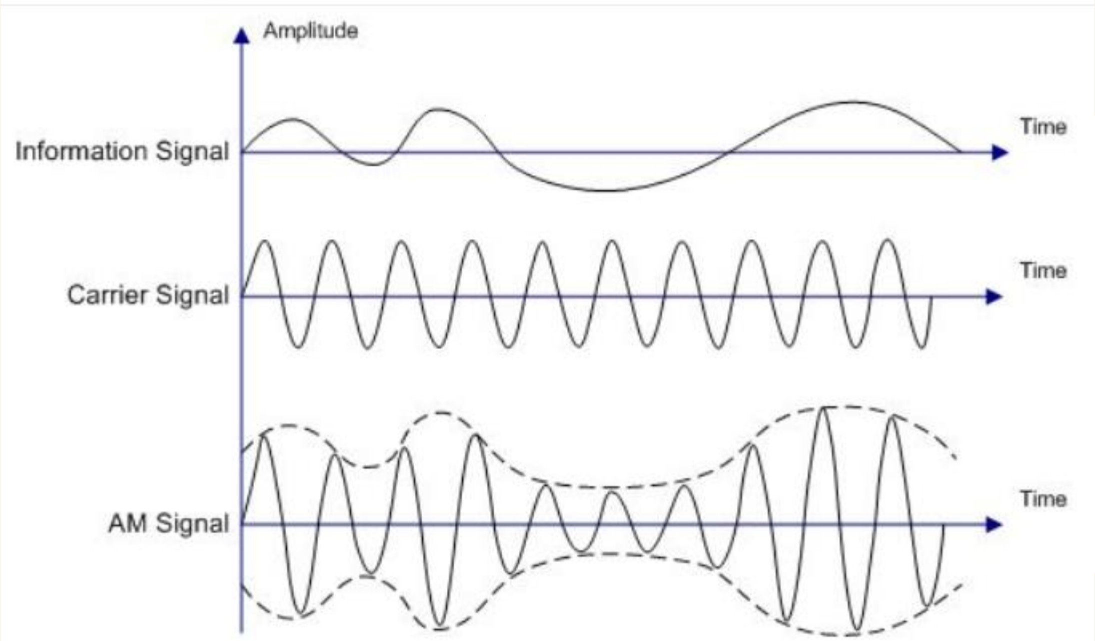


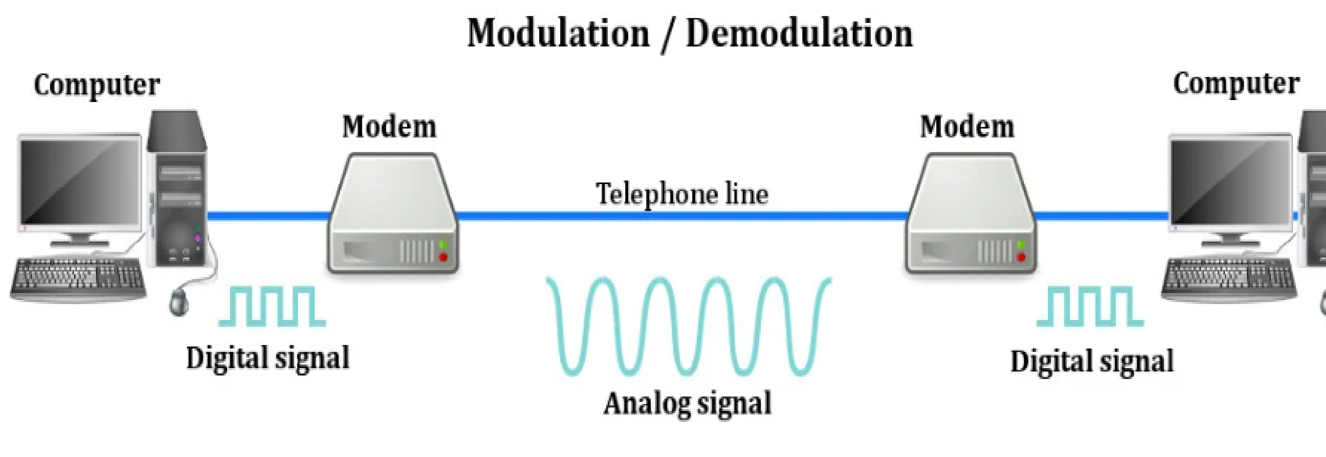
- **ROUTER:**
- It is a device that connects two or more packet-switched networks or subnetworks
- ➢ Routers connect networks like local area networks (LANs) and wide area networks (WANs).
- ➢ Routers analyze network metrics to find the best path for data to travel.
- ➢ It forward the data packets by ip addressing



MODEM(modulator and demodulator):
A modem's purpose is to make data easier to transmit and read. It acts as a digital translator, converting information from a cable or phone line into a form that a computer can understand
As analog data comes in from the internet, the modem demodulates the incoming analog signals into a digital signal so that a computer can understand it







REPEATER:

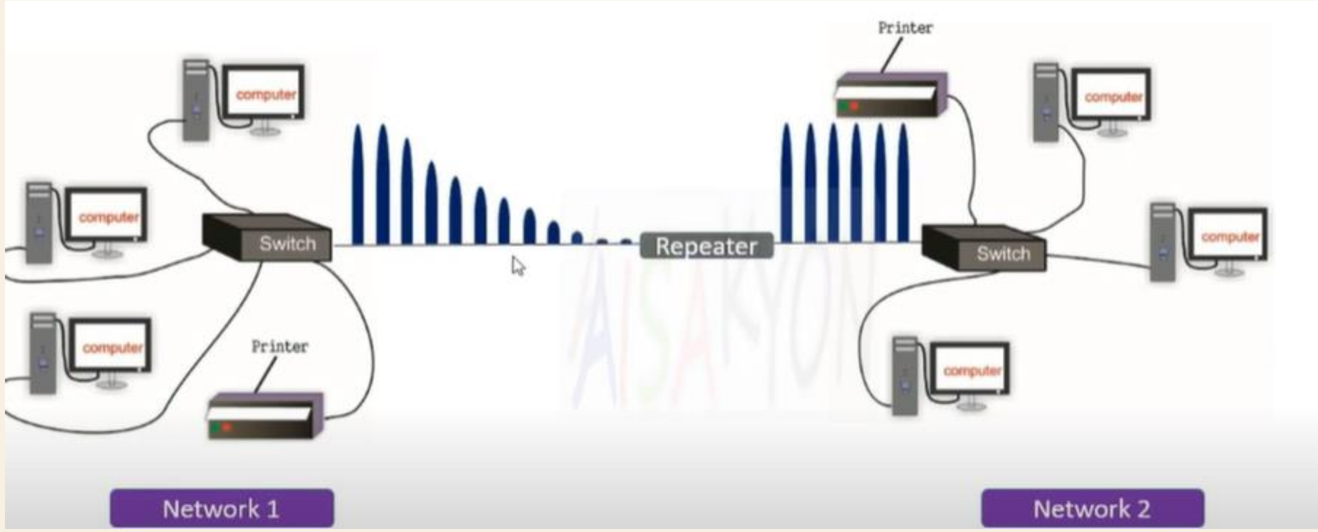
A **repeater** is a network device used to amplify or regenerate signals in a network to extend the transmission distance. In networking, as data signals travel through cables or wireless mediums, they weaken or degrade over long distances due to attenuation

Types of repeaters :

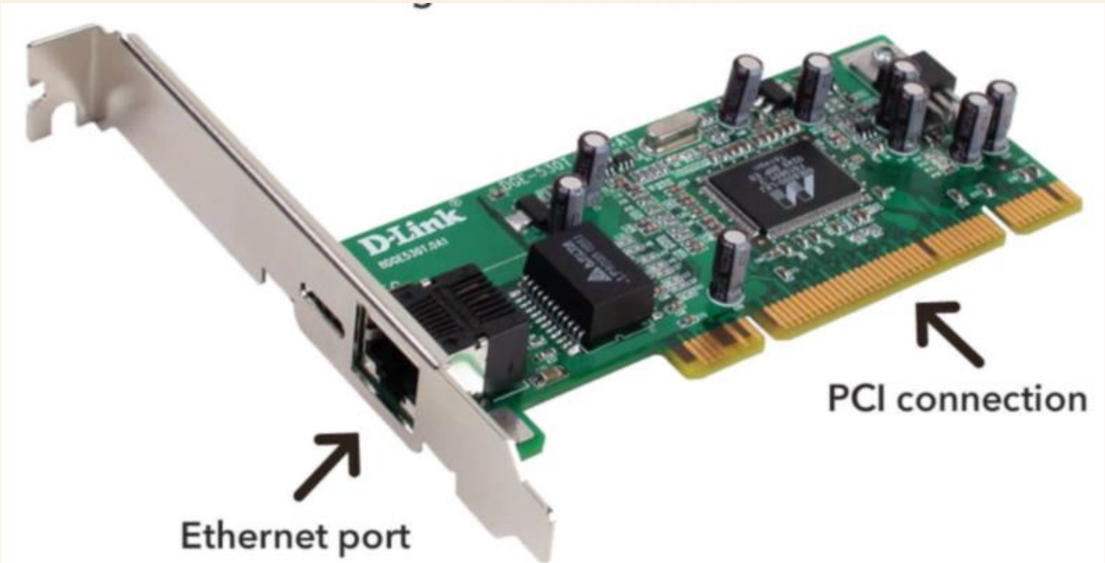
- Analog repeaters
- Digital repeaters
- Wireless repeaters
- Optical repeaters

EX:

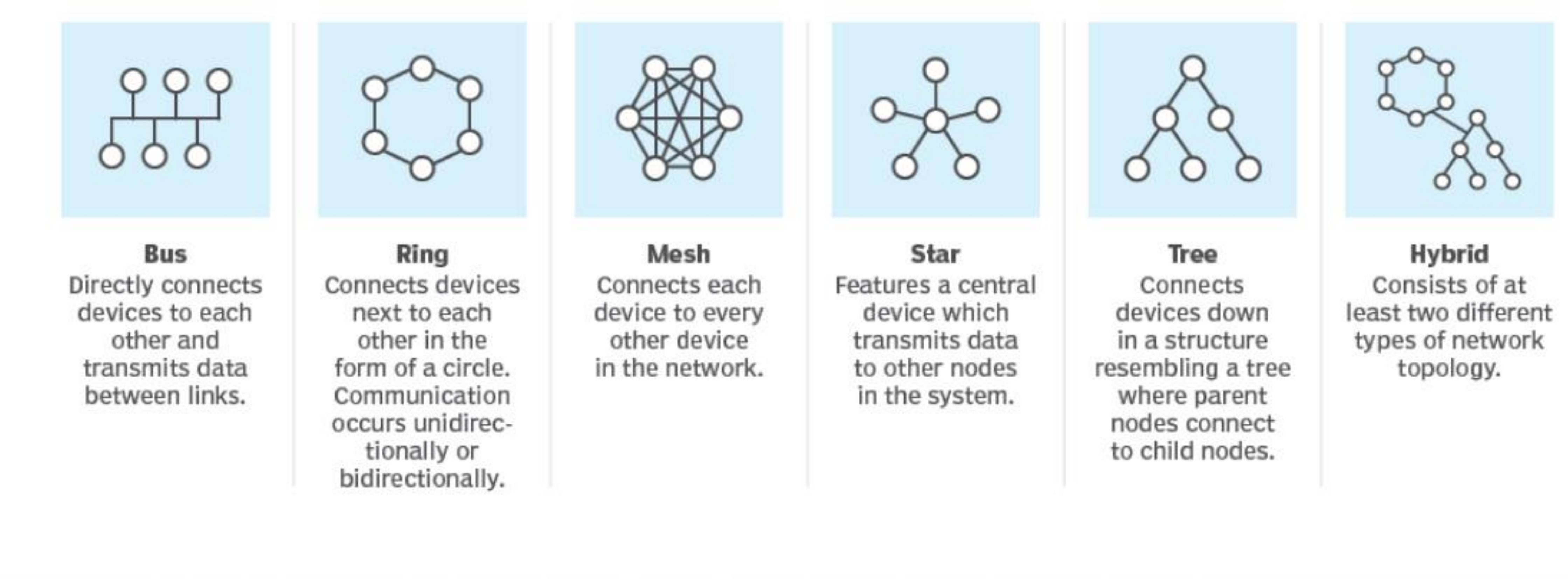
Wifi extenders , optical amplifiers



NETWORKING INTERFACING CARD:



NETWORK TOPOLOGIES :



Bus
Directly connects devices to each other and transmits data between links.

Ring
Connects devices next to each other in the form of a circle. Communication occurs unidirectionally or bidirectionally.

Mesh
Connects each device to every other device in the network.

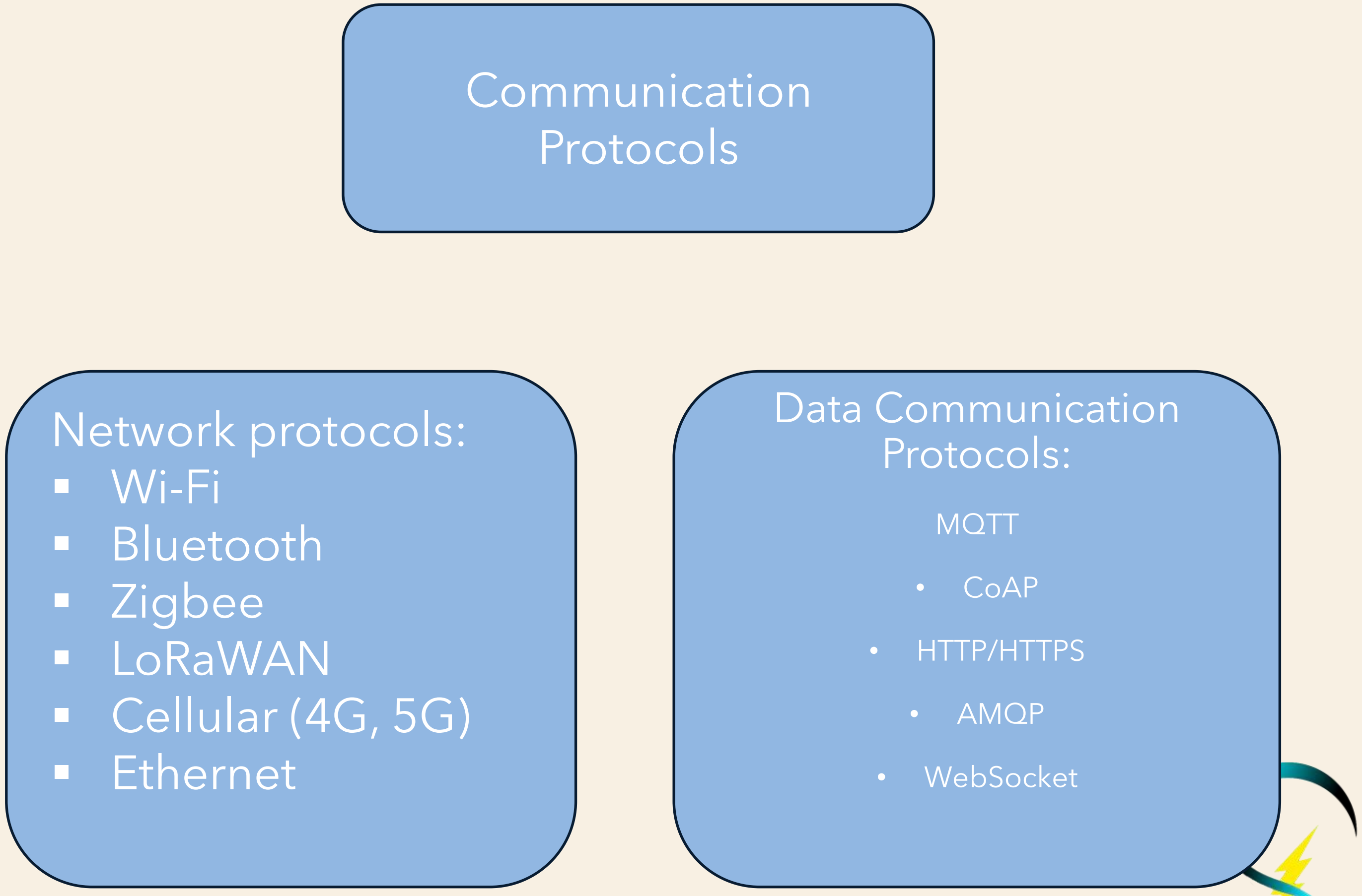
Star
Features a central device which transmits data to other nodes in the system.

Tree
Connects devices down in a structure resembling a tree where parent nodes connect to child nodes.

Hybrid
Consists of at least two different types of network topology.

COMMUNICATION PROTOCOLS

- Communication protocols in IoT define the rules and standards that enable data exchange between IoT devices, gateways, and cloud platforms. These protocols ensure that devices with different architectures, operating systems, and manufacturers can communicate effectively and reliably.



Communication Protocols

Network protocols:

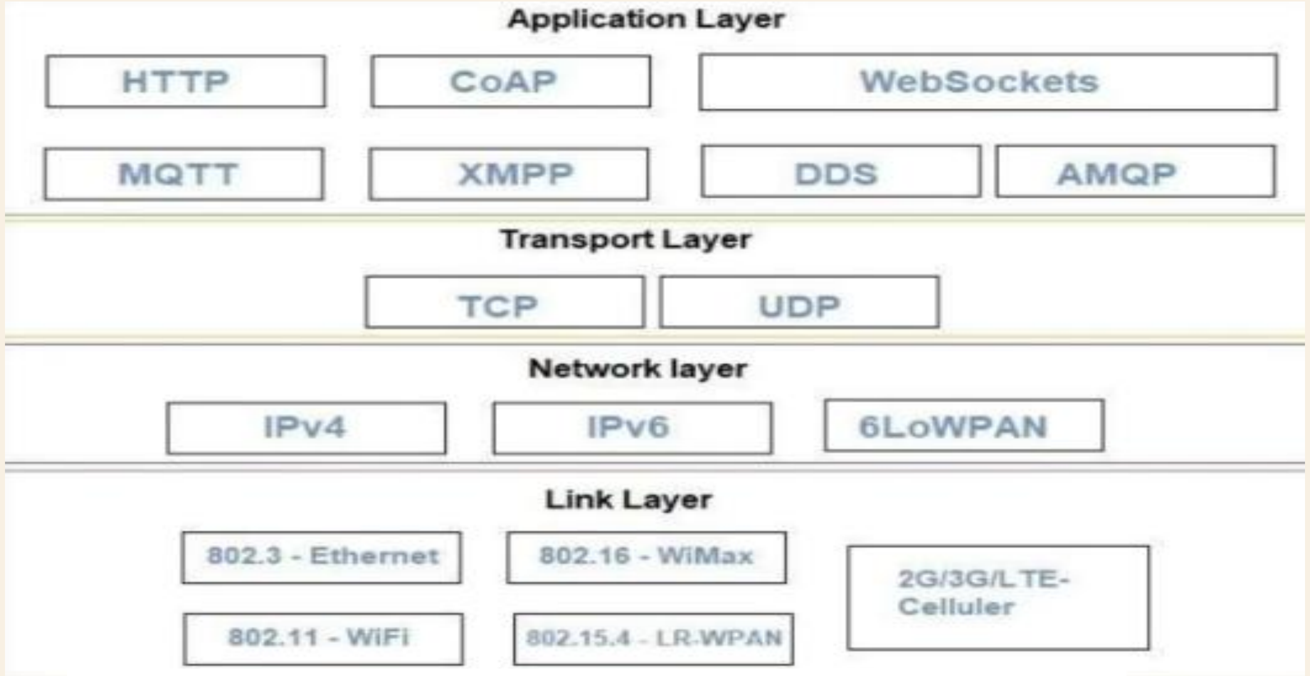
- Wi-Fi
- Bluetooth
- Zigbee
- LoRaWAN
- Cellular (4G, 5G)
- Ethernet

Data Communication Protocols:

MQTT

- CoAP
- HTTP/HTTPS
- AMQP
- WebSocket

- Based how the smart devices and sensor operate in the industry the protocols are divided into four layers
- Protocols are chosen based on the range that we are operating .
- The size or amount of the data that we are sending and receiving .
- Sometimes based on the power consumption also



Application Layer

HTTP | CoAP | WebSockets

MQTT | XMPP | DDS | AMQP

Transport Layer

TCP | UDP

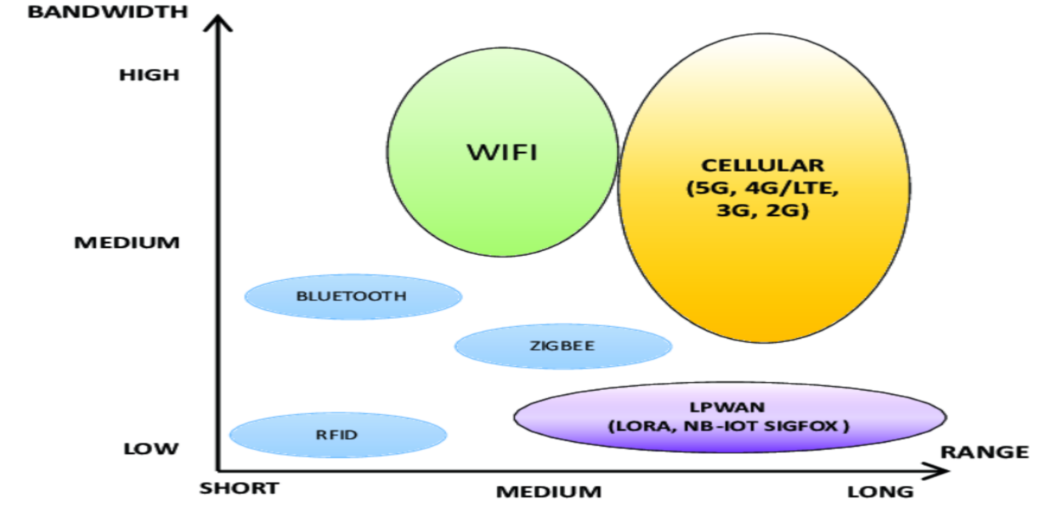
Network layer

IPv4 | IPv6 | 6LoWPAN

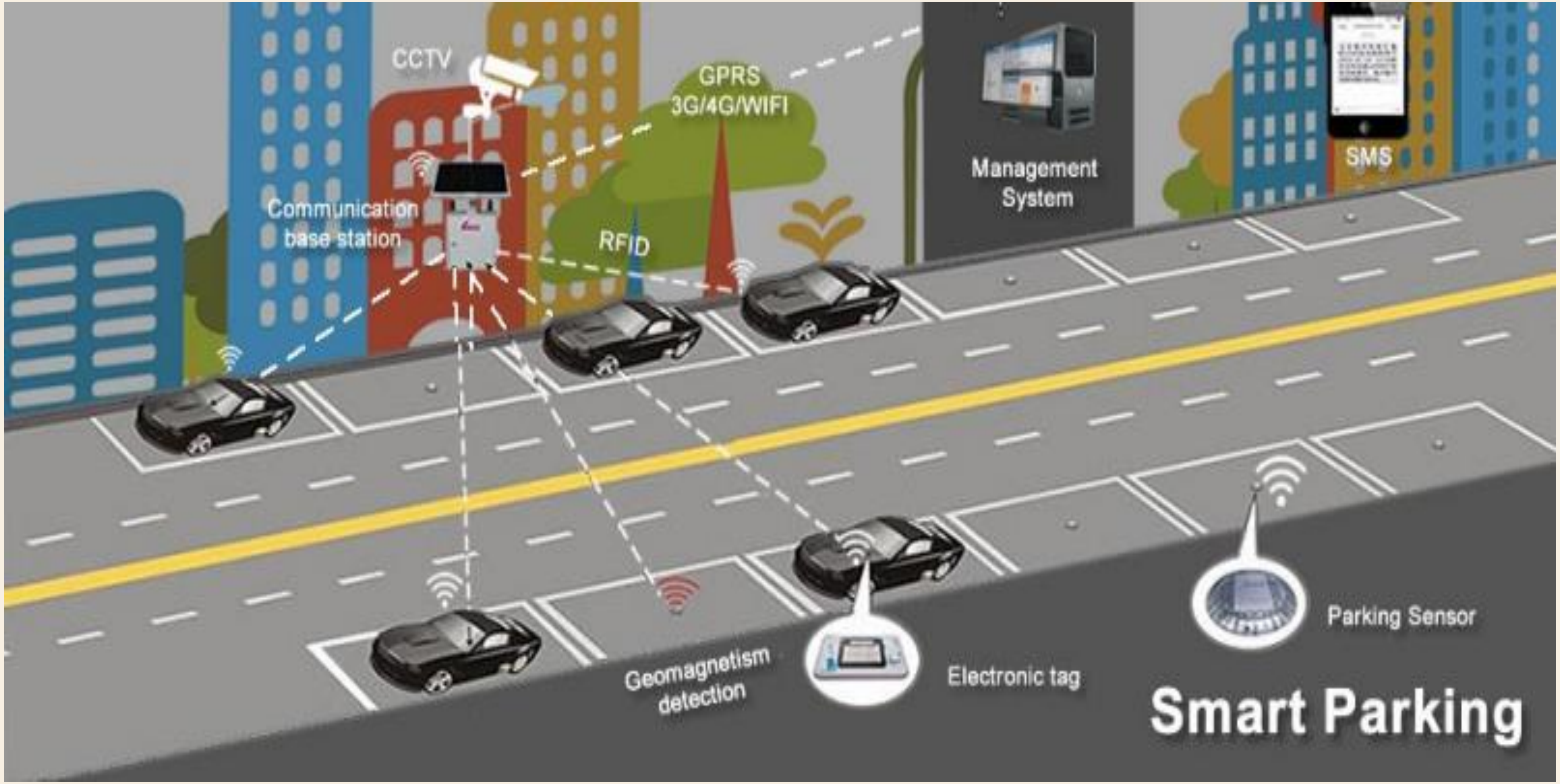
Link Layer

802.3 - Ethernet | 802.16 - WiMax | 2G/3G/LTE- Celluler

802.11 - WiFi | 802.15.4 - LR-WPAN

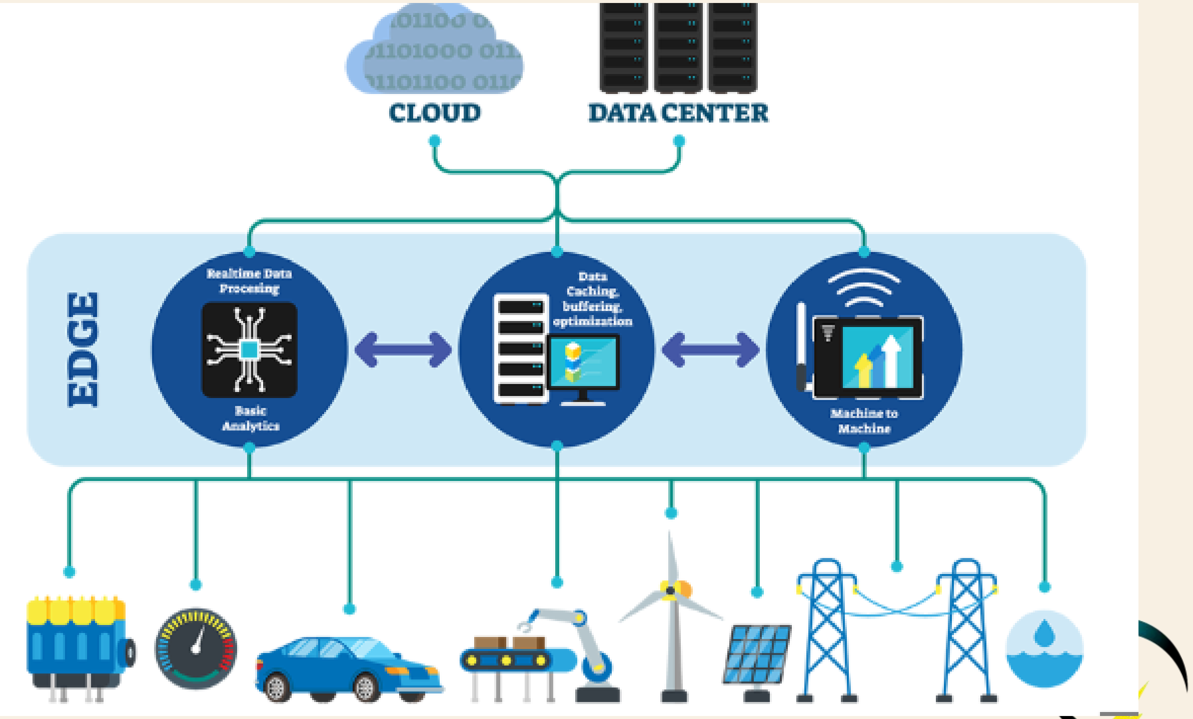


SIMPLE EXAMPLE :



EDGE COMPUTING :

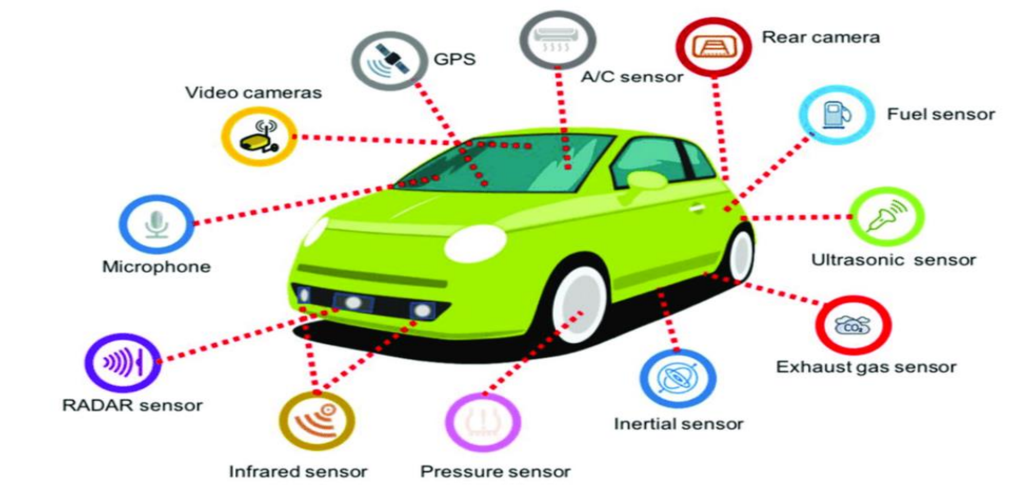
- Edge computing refers to the practice of processing data near its source (e.g., on IoT devices, gateways, or local servers) rather than sending it to a centralized cloud for processing. This approach minimizes latency, reduces bandwidth consumption, and improves real-time responsiveness.



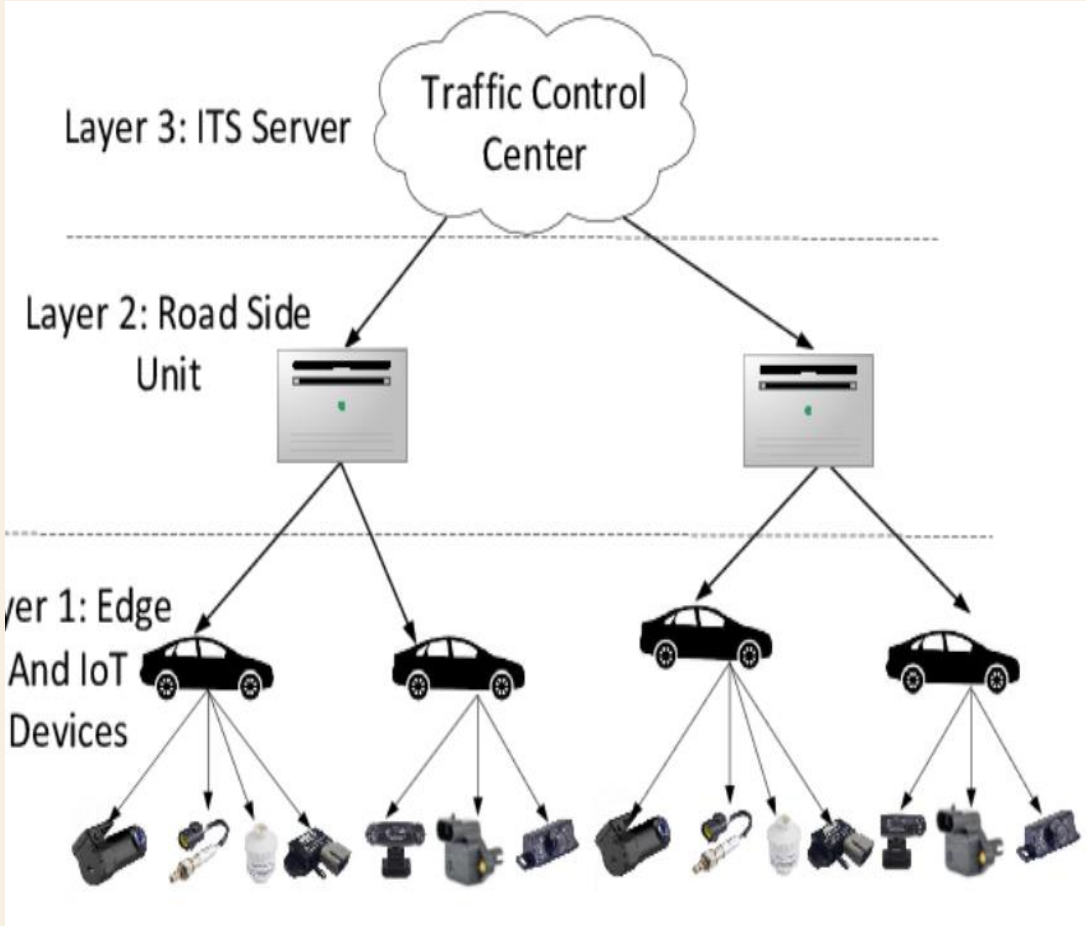
1. **Proximity to Data Source**:
    1. Processes data locally, at or near the IoT device.
2. **Real-Time Processing**:
    1. Enables immediate action based on data analysis.
3. **Reduced Latency**:
    1. Avoids delays caused by sending data to and from the cloud.
4. **Bandwidth Optimization**:
    1. Reduces the amount of data transmitted over networks.
5. **Enhanced Privacy and Security**:
    1. Limits data exposure by processing sensitive information locally.

WHERE IT IS USED

- **Autonomous Vehicles**:
- Self-driving cars process vast amounts of sensor data (from LiDAR, cameras, and radar) locally to make split-second driving decision
- **Predictive Maintenance:**
- Edge devices in factories analyze equipment data (e.g., vibration or temperature) in real time to predict failures and reduce downtime.
- **Traffic Management Systems**:
- Sensors at intersections process data locally to optimize traffic lights and reduce congestion.
- **Self-Checkout Systems**:
- Cameras and sensors process data locally to identify purchased items and speed up transactions.

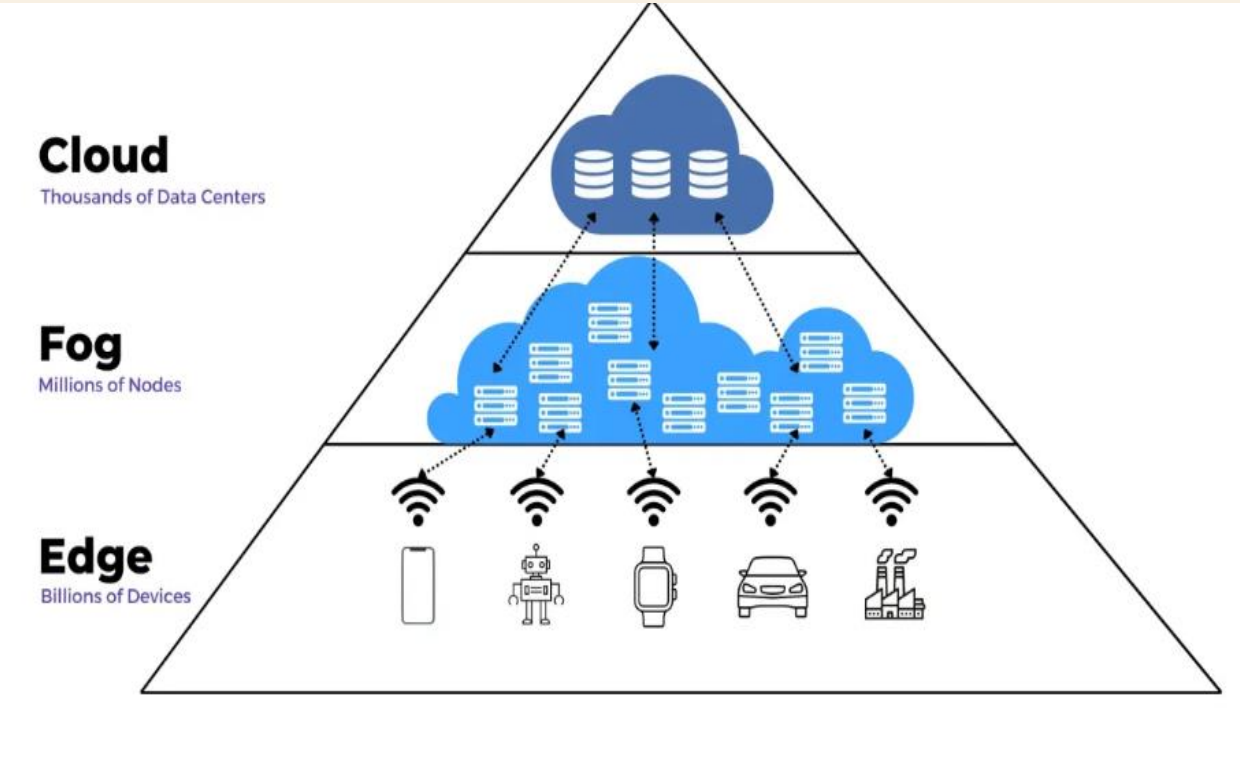

GPS
A/C sensor
Rear camera
Video cameras
Fuel sensor
Microphone
Ultrasonic sensor
Exhaust gas sensor
RADAR sensor
Inertial sensor
Infrared sensor
Pressure sensor

FastLane
Scannen & Einpacken
Abschluss & Zahlung


Traffic Control Center
Layer 3: ITS Server
Layer 2: Road Side Unit
yer 1: Edge And IoT Devices

FOG COMPUTING :

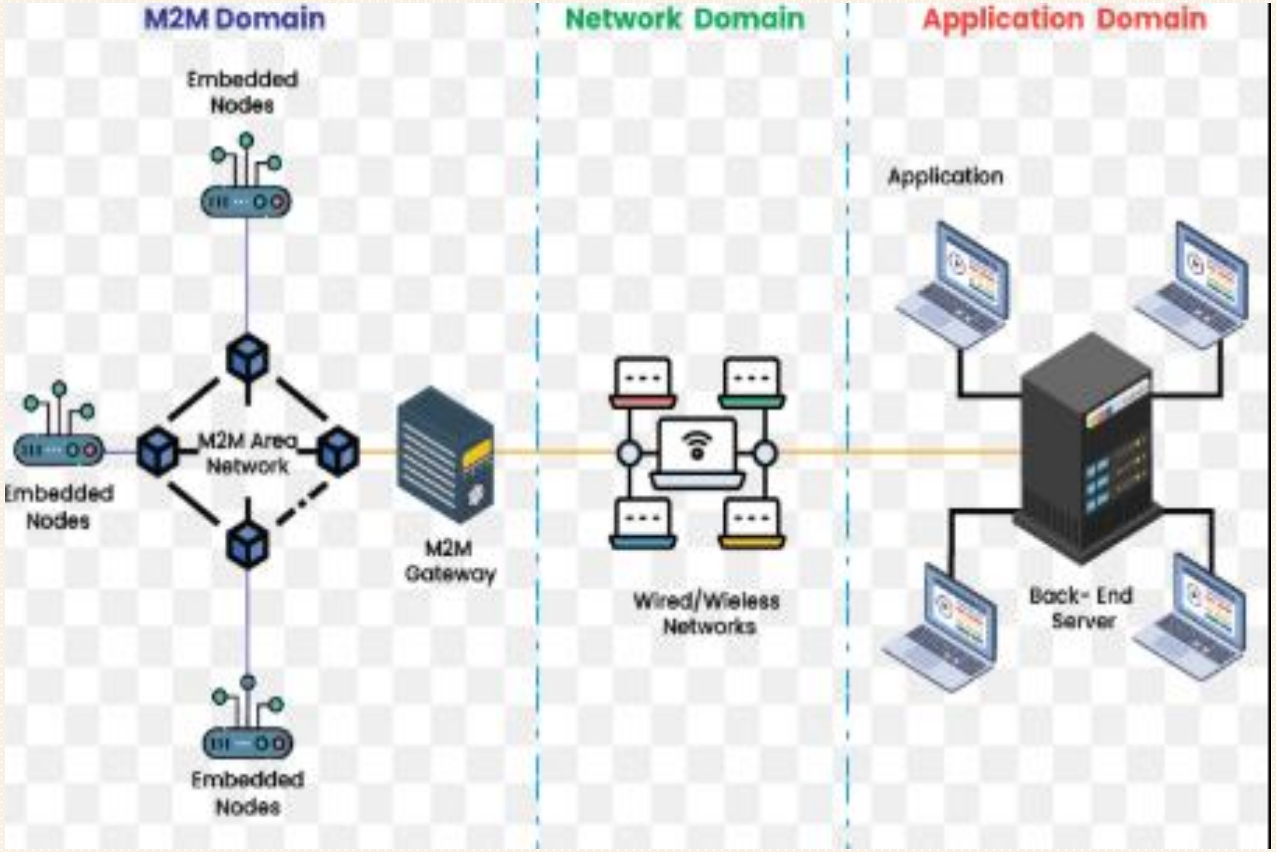
Fog computing is an extension of edge computing. It is a layer in between the edge and the cloud. When edge computers send huge amounts of data to the cloud, fog nodes receive the data and analyze what's important. Then the fog nodes transfer the important data to the cloud to be stored and delete the unimportant data or keep them with themselves for further analysis. In this way, fog computing saves a lot of space in the cloud and transfers important data quickly



ADVANTAGES OVER EDGE COMPUTING :

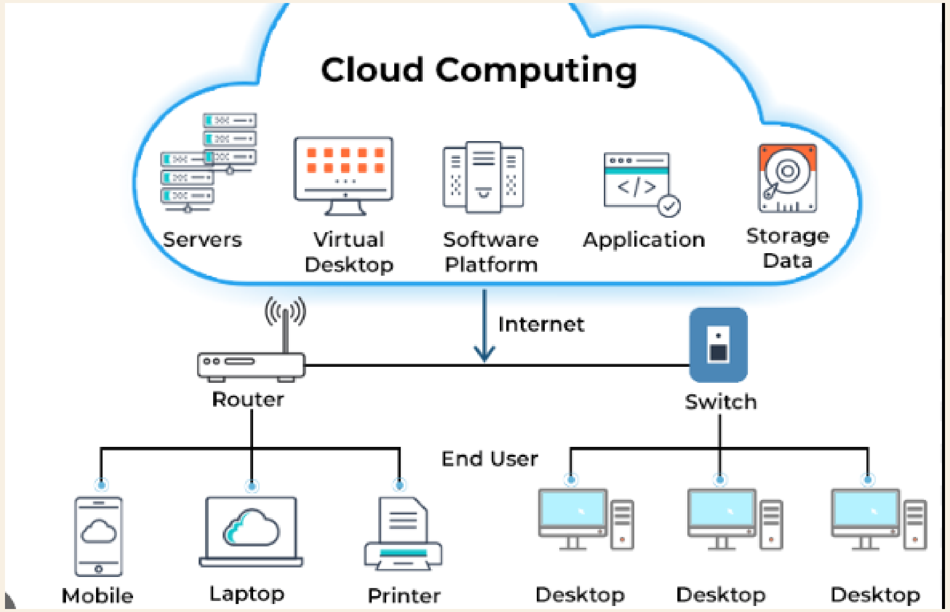
- Data aggregation and filtering:
- Fog computing can collect data from multiple edge devices and filter out irrelevant information before sending it to the cloud, significantly reducing bandwidth consumption.
- Fog computing can easily scale by adding or removing fog nodes based on network needs, offering greater flexibility compared to edge computing.
- Fog computing can handle more data locally, minimizing the need to constantly send data to the cloud, potentially lowering cloud service costs
- Reduces the networking complexity of edge devices by adding sub network

M2M ARCHITECTURE :



CLOUD COMPUTING

Cloud computing refers to the centralized processing, storage, and management of data on remote servers hosted on the internet. In IoT, cloud platforms act as hubs for data storage, analysis, and application hosting.



There are three types :

- Infrastructure as service(IAAS)
- Platform as service (PAAS)
- Software as service (SAAS)

1. **Centralized Storage**:
   1. Stores large volumes of data for long-term analysis.
2. **Powerful Analytics**:
   1. Leverages advanced tools like AI and ML for deeper insights.
3. **Global Accessibility**:
   1. Allows remote access to data and applications from anywhere.
4. **Scalability**:
   1. Dynamically scales resources to accommodate varying data loads.
5. **Integration**:
   1. Connects diverse devices and systems across geographies.

WHERE WE USE IT

- **Online Data Backup Services**
- Applications like Google Drive, Dropbox, and iCloud allow users to back up and store their files securely in the cloud.
- **Streaming Services**
- Platforms like Netflix, YouTube, and Spotify deliver movies, videos, and music to users. Content is stored in cloud servers and distributed globally via content delivery networks (CDNs).No real-time processing on local devices—only data retrieval from the cloud.
- **E-commerce Platforms**
- websites like Amazon or Shopify run their operations, including inventory management, order processing, and customer transactions, using cloud computing.

Cloud layer

Big data processing

Business logic

Data warehousing

Fog layer

Local network

Data analysis & reduction

Control resone

Virtualization/ standardization

Edge layer

Large volume real-time data processing

At source/on-prem data visualization

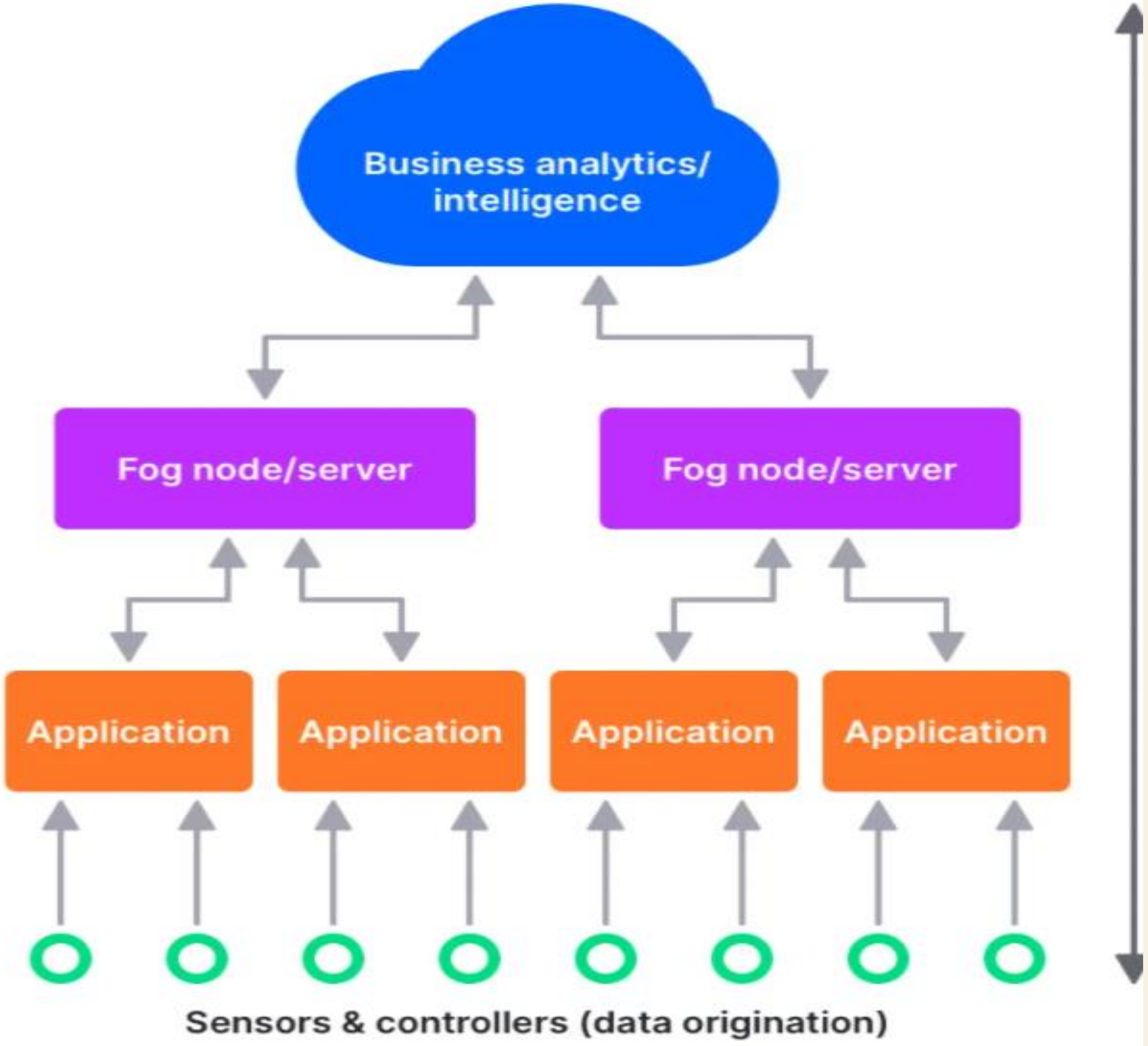
Industrial PCs

Embedded systems

Micro data storage

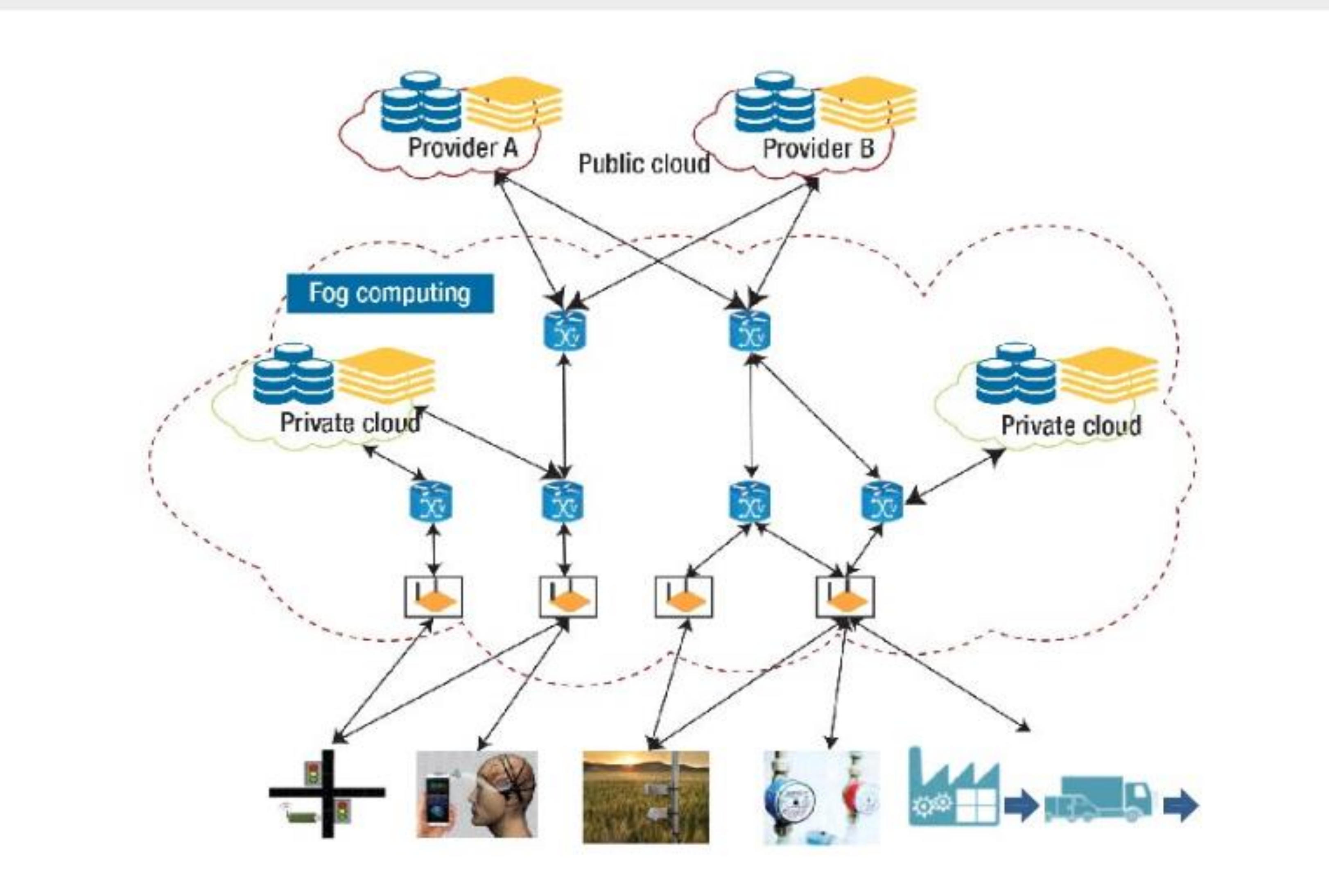
Wearables

Self-driving cars



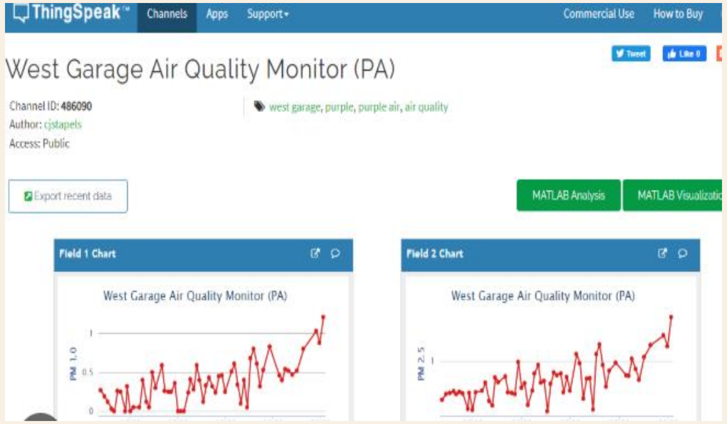
WHERE BOTH EDGE AND CLOUD COMPUTING IS USED ?

- **Remote Patient Monitoring**
- **Edge Computing Role:**
    - Wearable devices (e.g., heart rate monitors) process real-time health data to alert patients or medical staff of emergencies.
- **Cloud Computing Role:**
    - Patient data is stored in the cloud for doctors to analyze historical trends and make informed decisions.
- **Traffic Management and prediction**
- **Edge Computing Role:**
    - Traffic cameras and sensors process data locally to adjust signals in real time, optimizing traffic flow.
- **Cloud Computing Role:**
    - The cloud collects data from multiple intersections to identify long-term patterns, plan infrastructure upgrades, and improve urban planning.


Provider A
Public cloud
Provider B
Fog computing
Private cloud
Private cloud

DATA HANDLING

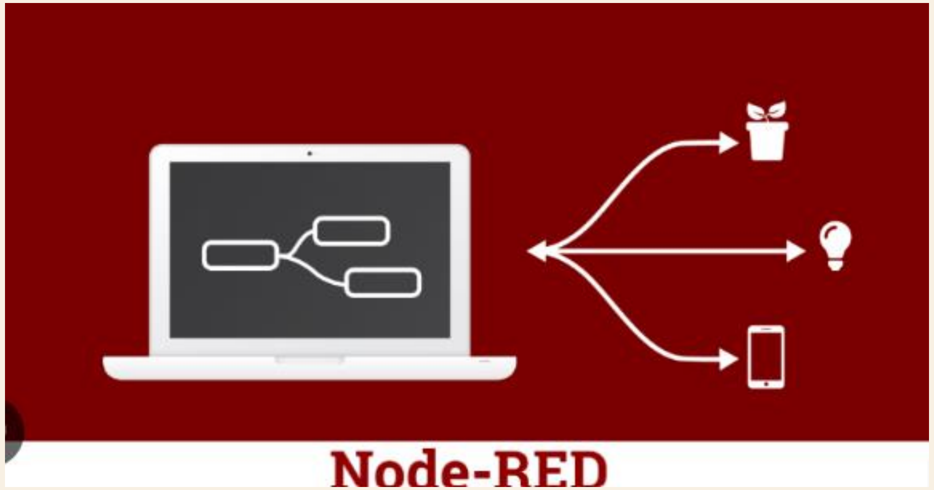
- **Data Collection:**
- Sensors and IoT devices gather data in real time (e.g., temperature, humidity, motion, etc.).
- Data is transmitted to storage systems or directly processed.
- **Data Storage:**
- Data is stored in cloud platforms, edge devices, or local databases.
- Examples: AWS IoT Core, Microsoft Azure, and Google Cloud IoT.
- **Data Processing:**
- Organizing and preparing data for analysis.
- Involves cleaning, filtering, and transforming data formats.
- **Data Analysis:**
- Advanced analytics methods like statistical analysis, machine learning, and artificial intelligence (AI) are used to extrac
- Predictive analytics and anomaly detection are common techniques.
- **Visualization:**
- Data is presented in a user-friendly manner through dashboards, graphs, and charts to facilitate understanding.
- **Actionable Insights:**
- Data-driven insights are used to automate processes, optimize operations, or improve decision-making.



West Garage Air Quality Monitor (PA)

Channel ID: 486090
Author: cjstapels
Access: Public

west garage, purple, purple air, air quality

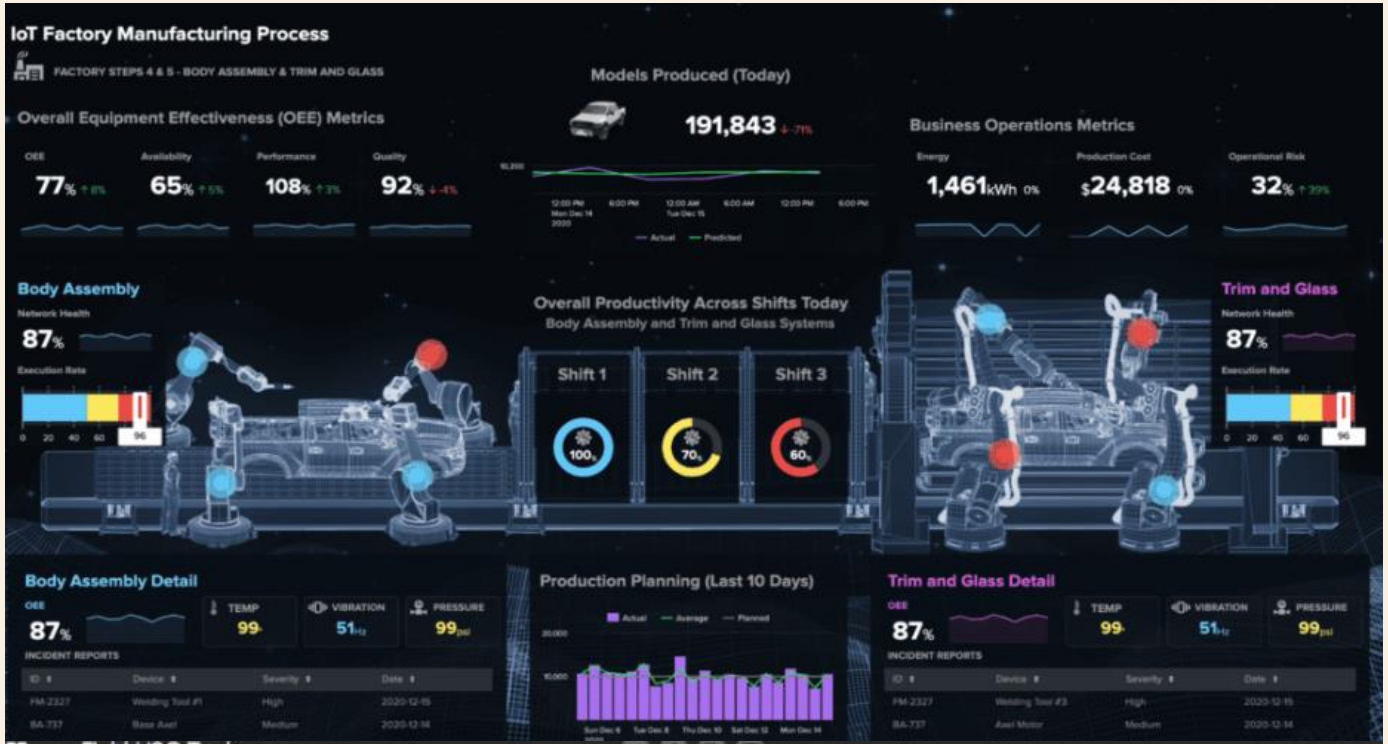


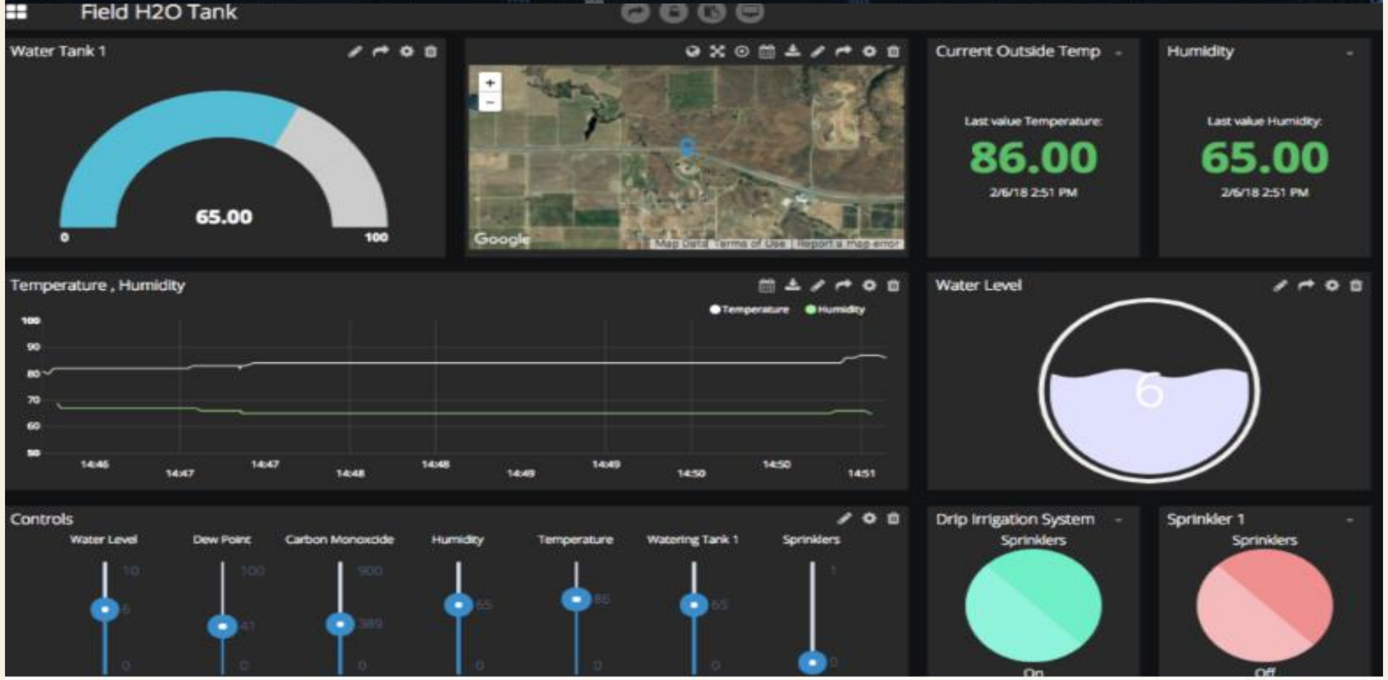
UI/UX

- Information made available to the end-users
- Users can actively check and act in for their IOT system

It can be through :

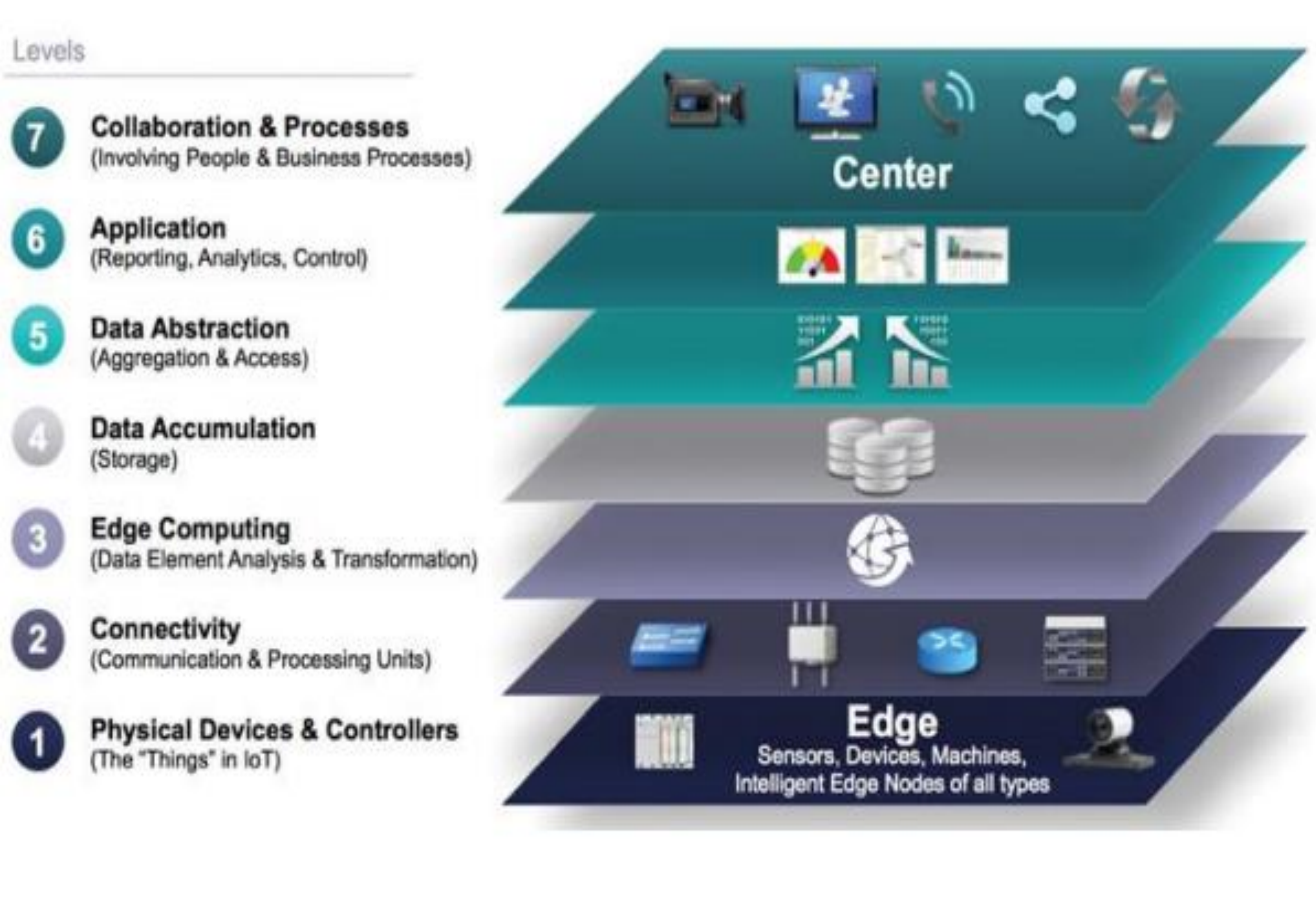
- Websites
- Apps
- Notifications
- Alarms





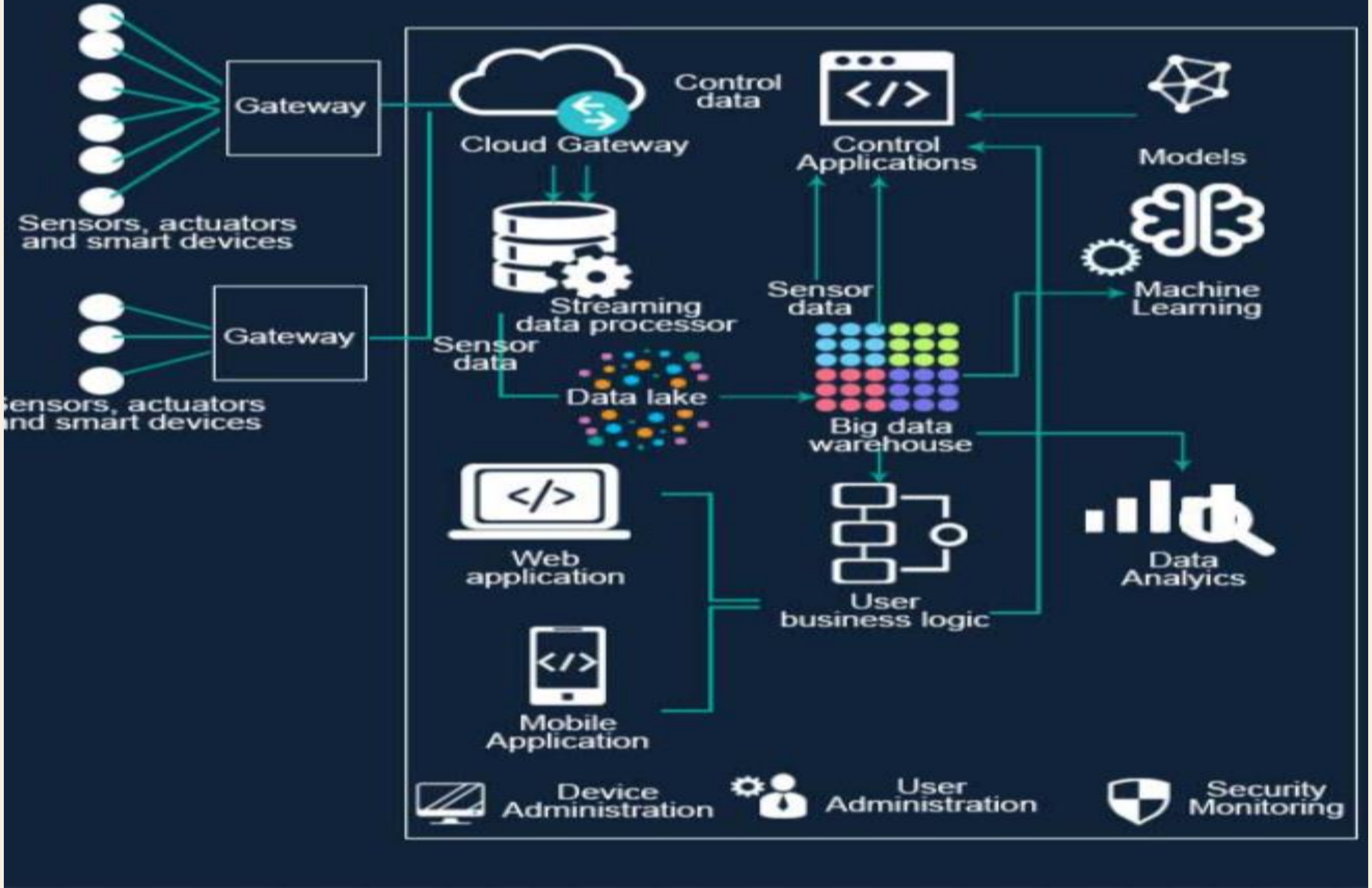
IOT ARCHITECTURE

- There Is no particular architecture that is followed universally because it changes based on the problem we are facing and the solution we are going design.
- However here we can discuss about one of the standard 7 layer architecture **IOTWF**


Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types

- **Physical Devices and Controllers Layer**
  primary function is generating data
- **Connectivity Layer**
  focus is on connectivity
- **Fog Layer**
  Data reduction by filtering and cleaning up – Reformatting and compressing data – Initial processing of data (e.g. alert generation, data validation, etc)
- **Data Accumulation**
  Captures data and stores it for applications ,Convert event-based data to query-based processing
- **Data Abstraction**
  Reconciles multiple data formats , Ensures consistent semantics for various data sources , Confirmation about dataset completeness
- **Application**
  Interpret data using software applications ,Applications may monitor, control, and provide report based on analysing the data
- **Collaboration and processes**
  Consumes and shares the application information , Collaborating and communicating IoT information

IoT Architecture



A CASE STUDY TO UNDERSTAND IMPORTANCE OF SECURITY IN IOT DEVICES:

The MIRAI DDOS ATTACK :

- The Mirai botnet attack in 2016 used compromised IoT devices to launch a massive Distributed Denial of Service (DDoS) attack. Mirai scanned the internet for IoT devices with default credentials or outdated firmware and infected them to   form a botnet.
- The attack targeted Dyn, a major DNS provider, disrupting internet services for major websites like Twitter, Netflix, and Reddit.
- The botnet generated over **1 terabit per second (Tbps)** of traffic, one of the largest DDoS attacks at the time.
- Devices like IP cameras, DVRs, and routers were exploited due to their weak security.
- The attack caused widespread outages, affecting businesses and users globally.
- Mirai was discovered due to its aggressive scanning behavior for vulnerable devices.

SECURITY IN IOT

1. Device-Level Security

- Encryption**:** Protects data at rest and in transit using protocols like TLS/SSL.
- Authentication**:** Ensures only authorized users and devices can access the IoT network.

  Example: Multi-factor authentication (MFA).
- Secure Boot: Prevents unauthorized firmware or software from running on devices.

2. Network-Level Security

- Firewalls: Prevent unauthorized traffic from entering IoT networks.
- Virtual Private Networks (VPNs): Encrypt communication between devices and networks.
- Intrusion Detection Systems (IDS): Identify and alert about unusual activities.

3. Cloud-Level Security

- Cloud Access Security Brokers (CASBs): Monitor and secure data flow between IoT devices and cloud platforms.
- Data Tokenization: Replaces sensitive data with tokens to protect it during storage or transmission.

4. Edge Computing Security

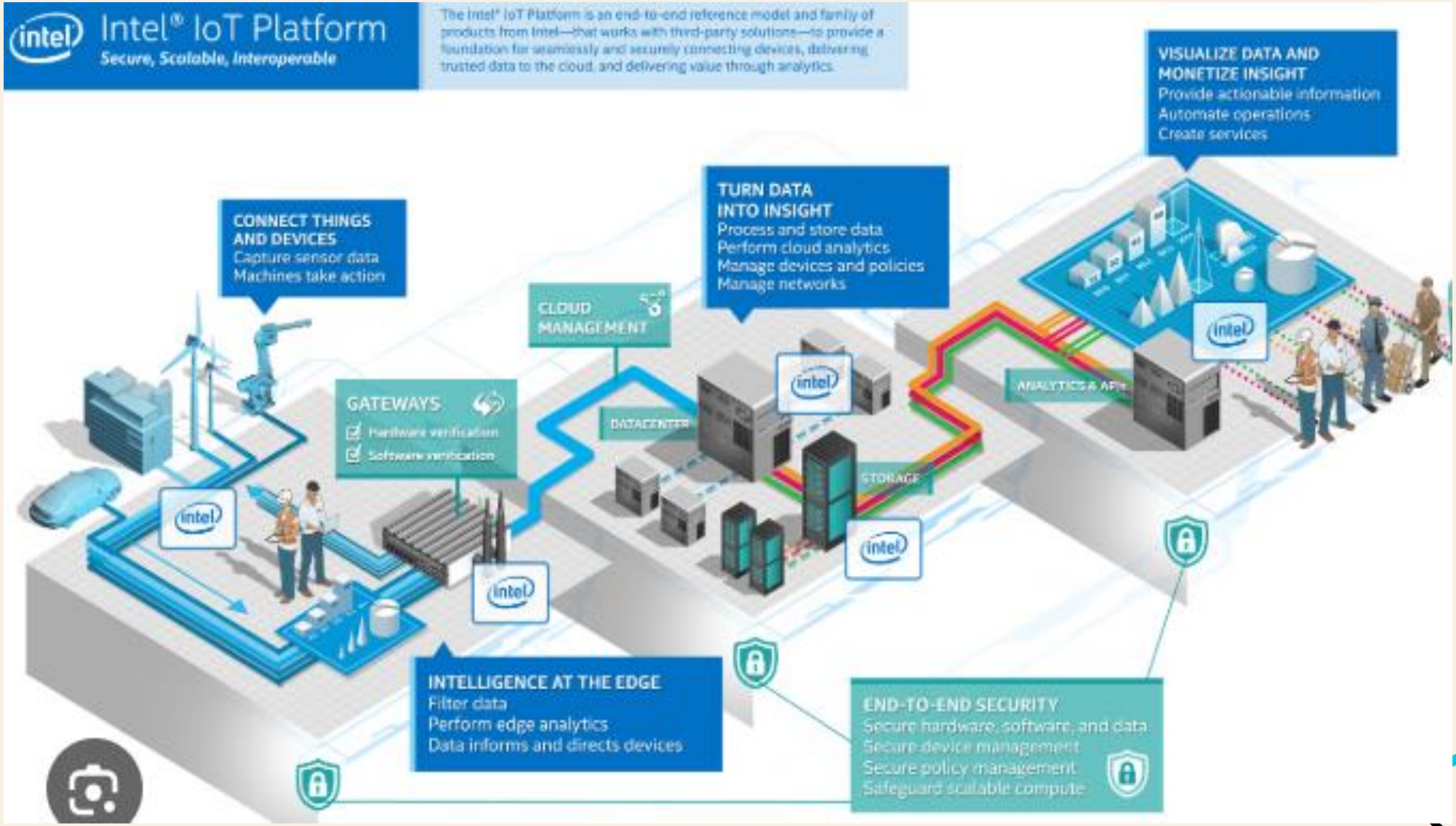
- Local Processing**:** Reduces the need to transmit sensitive data over networks by processing it locally.
- Edge Firewalls and Gateways: Protect edge devices from external threats.

5. Threat Detection and Monitoring

- AI and Machine Learning**:** Identifies patterns of malicious activity in real-time.
- Anomaly Detection Tools**:** Highlight deviations in device behavior.

6. Security Standards and Frameworks

- IoT Security Foundation (IoTSF): Offers guidelines for securing IoT systems.
- NIST Cybersecurity Framework**:** Provides comprehensive security practices for IoT.



Intel® IoT Platform

Secure, Scalable, Interoperable

The Intel® IoT Platform is an end-to-end reference model and family of products from Intel—that works with third-party solutions—to provide a foundation for seamlessly and securely connecting devices, delivering trusted data to the cloud, and delivering value through analytics.

CONNECT THINGS AND DEVICES
Capture sensor data
Machines take action

INTELLIGENCE AT THE EDGE
Filter data
Perform edge analytics
Data informs and directs devices

TURN DATA INTO INSIGHT
Process and store data
Perform cloud analytics
Manage devices and policies
Manage networks

VISUALIZE DATA AND MONETIZE INSIGHT
Provide actionable information
Automate operations
Create services

END-TO-END SECURITY
Secure hardware, software, and data
Secure device management
Secure policy management
Safeguard scalable compute