# Overview

- Introduction to IoT
  - What is IoT?
  - IoT terms and Basic Definitions
  - Disambiguation of IoT vs IoE vs M2M vs Others
  - Characteristics of IoT
  - Applications of IoT
  - Things in IoT
  - IoT Reference Model
  - Building Blocks of IoT
  - 4 stages of IoT architecture

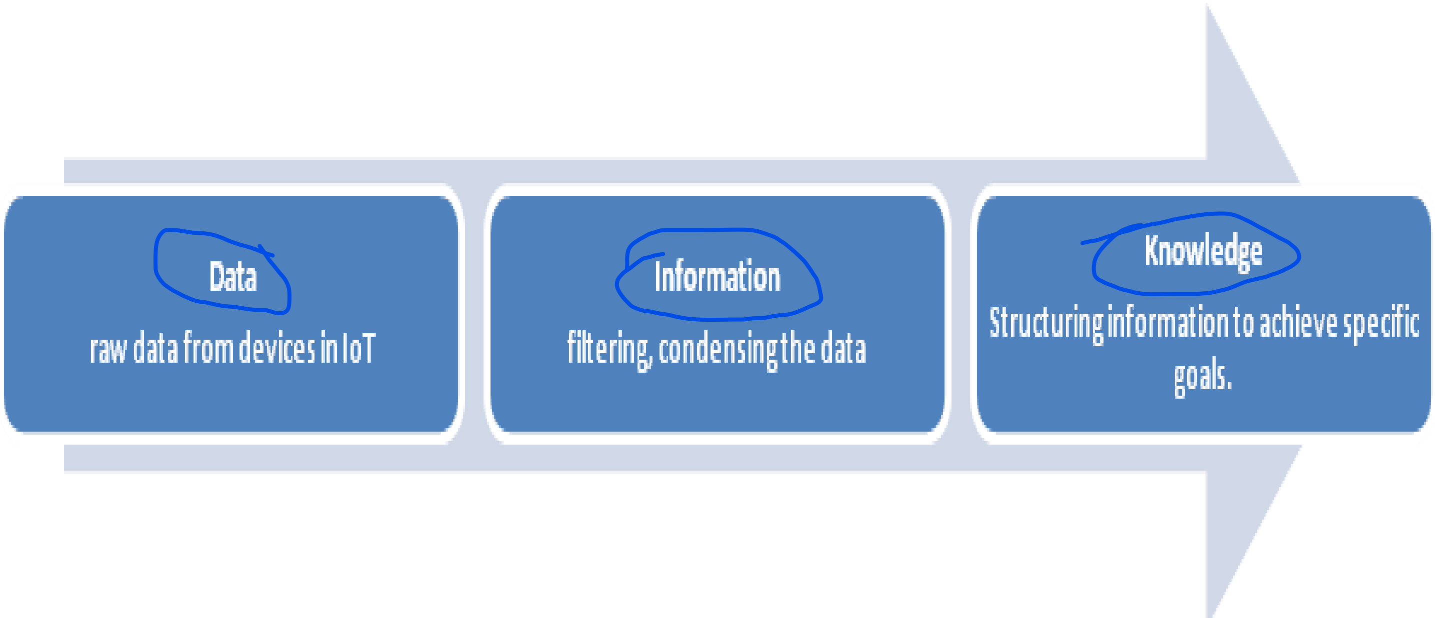
# Introduction to IoT

- **“Internet”** is to provide a connection between computers worldwide.
- **“Things”** is referring to devices that are capable of communicating data electronically over an Internet connection
- **So what is the Internet of Things?** For now you can think of IoT as a system that uses the *infrastructure of the Internet to establish a connection to and between our electronic devices.*

# Introduction to IoT

- **What Microsoft say about the Internet of Things:**
  - "The Internet of Things (IoT) is not a futuristic trend;
  - it’s the first step toward becoming a truly digital business and it starts with your things
  - your line-of-business assets and the data they produce, your cloud services, and your business intelligence tools.
  - That’s the Internet of Your Things, With an IoT strategy in place you can make your business thrive."

# What is IoT?




**Inferring information and knowledge from data**

# IoT terms and Basic Definitions

- **IoT**
- **IoT device**
- **IoT ecosystem**
- **Physical layer**
- **Network layer**
- **Application layer**
- **Remotes**
- **Dashboard**
- **Analytics**
- **Data storage**
- **Networks**

# IoT terms and Basic Definitions

- **IoT:** The internet of things, or **IoT**, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
- **IoT device:** A standalone entity connected to a web which can be identified and monitored from a remote area.
- **IoT ecosystem:** It's a collective system of components that empower organizations, governance with the governments, and peer customers to associate with their useful IoT gadgets with additional components such a remotes, dashboards, systems, entryways, investigation, information stockpiling, and security.

# IoT terms and Basic Definitions

- **Physical layer:** It's a layer which constitutes an IoT device/gadget which includes automating sensors and an administrative unit of systems.
- **Network layer:** It's a layer Responsible for the communication via transmitting the information gathered by the physical layer to route across various devices.
- **Application layer:** It's a layer which incorporates the set of protocols and the catalytic interfaces that devices use in order to recognize and speak often with each other.

# IoT terms and Basic Definitions

- **Remotes:** Empower substances which use IoT devices in order to associate with device components and control them with advent use of a dashboard, for example, a versatile application which can incorporate cell phones, tablets, PCs, shrewd watches, associated Televisions.
- **Dashboard:** It Displays data about the IoT biological community to peer clients which empowers clients control their integrated components in IoT environment, which is their by termed as large housed data on a remote.
- **Analytics:** It's a Software framework which examines the information produced by IoT devices. The information obtained from IoT devices can be utilized for an assortment of situations.

# IoT terms and Basic Definitions

- **Data storage:** Where information from IoT gadgets is put away.
- **Networks:** The web correspondence layer that empowers the substance to speak with their gadget, and now and then empowers gadgets to speak with each other.

# Disambiguation of IoT vs IoE vs M2M vs Others

- **M2M:** Machine to Machine (**M2M**) refers to a wireless or wired network setup that allows devices of the same type and ability to communicate freely.
- **IIoT:** The industrial internet of things, or IIoT, is the use of internet of things technologies to enhance manufacturing and industrial processes. Also known as the *industrial internet* or *Industrie 4.0*, IIoT incorporates machine learning and big data technologies to harness the sensor data, machine-to-machine (M2M) communication and automation technologies that have existed in industrial settings for years.

M2M in Industry Automation

# Disambiguation of IoT vs IoE vs M2M vs Others

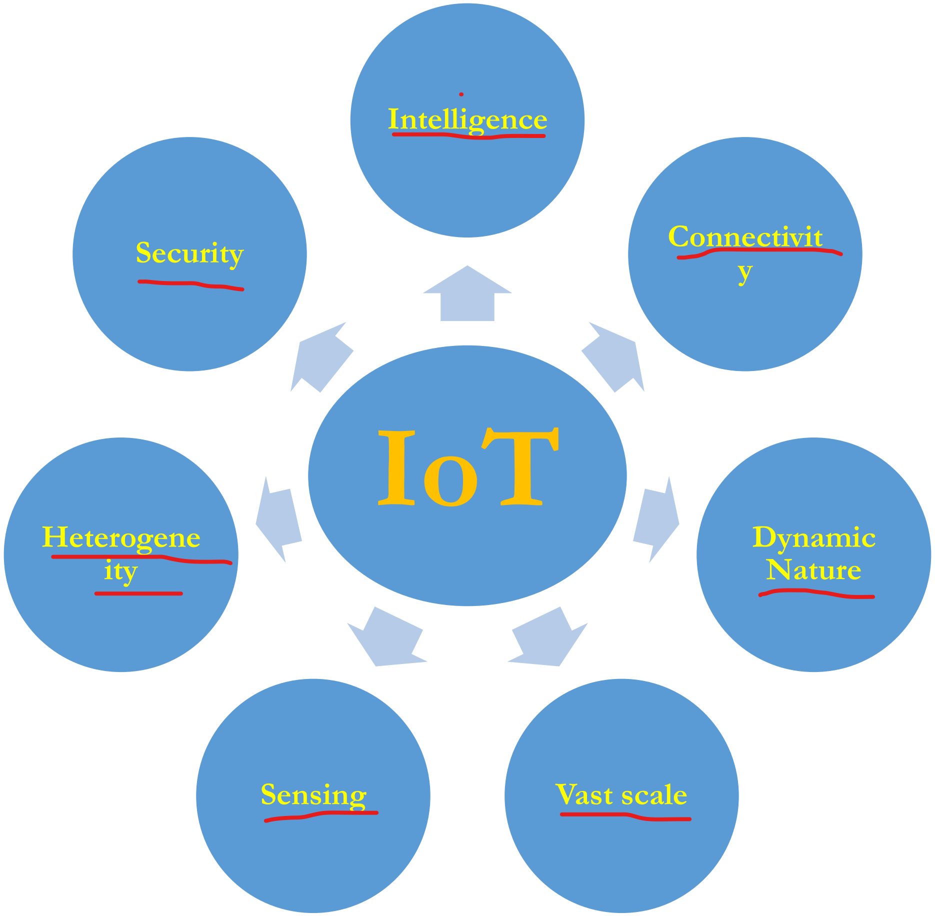
M2M + M2P + P2P

- **IoE:** IoE as "the intelligent connection of people, process, data and things." Because in the Internet of Things, all communications are between machines, IoT and M2M are sometimes considered synonymous. The more expansive IoE concept includes, besides M2M communications, machine-to-people (M2P) and technology-assisted people-to-people (P2P) interactions.

# Characteristics of IoT

ICDVHSS

Intelligents cant dance vigorously having swim suits



# Applications of IoT

Remember the generic names of sectors and examples

| | |
|---|---|
| Consumer | • Smart Home control, lighting, maintenance etc |
| Industrial | • Smart meters, Wear outs, Climate control, Product tracking |
| Automotive | • Parking, Traffic control, Anti theft location |
| Environmental | • Weather prediction, Resource managemet |
| Agriculture | • Crop management, soil analysis |
| Military | • troop monitoring, Threat analysis |
| Medical | • Wearable devices |

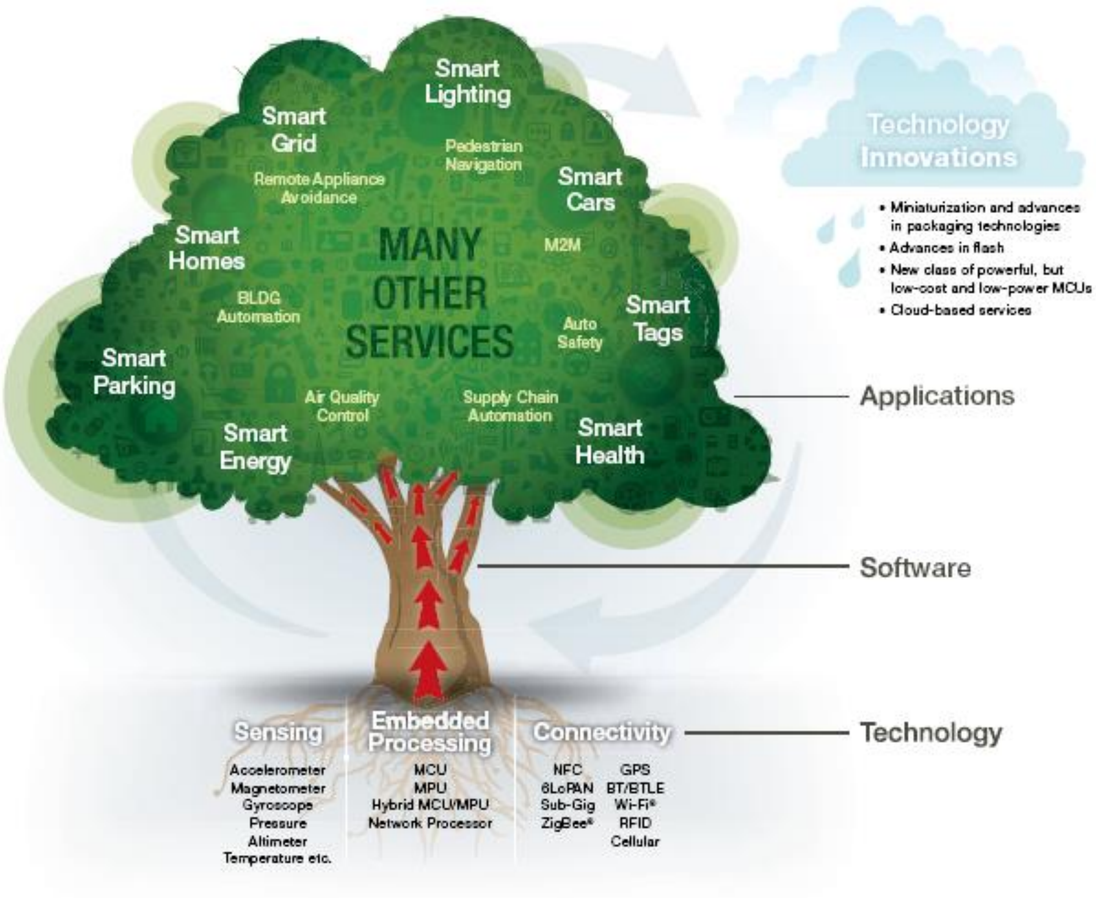
# IoT Applications categories

- **Category one**
  - interconnected devices with unique IDs interacting with other machines/objects, infrastructure, and the physical environment.
  - the IoT largely plays a remote track, command, control and route (TCC&R) role.
  - not about data mining of people’s behaviors but rather they extend the automation and machine-to-machine (M2M), machine-to-infrastructure (M2I) and machine-to-nature (M2N) communications that can help simplify people’s lives.
  - **Monitoring home remotely, Asset tracking , Remote patient monitoring**

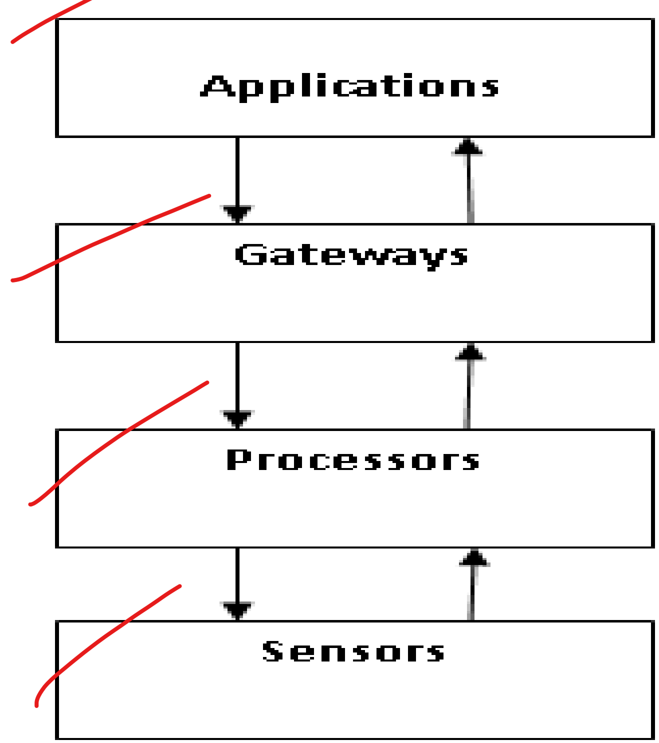
# IoT Applications categories

- **Category two**
  - leveraging the data that gets collected by the end nodes (smart devices with sensing and connectivity capability) and data mining for trends and behaviors that can generate useful marketing information to create additional commerce.
  - Credit card companies and membership shopping clubs

# The IoT: Different Services, Technologies, Meanings for Everyone



# Things in IOT




**Functional Blocks of IoT**

# Things in IOT

| Things in IoT | Functionality |
|---|---|
| **Sensors** | • Front end devices<br>• gathers information<br>• identifiable devices with a IP address<br>• dynamic in nature<br>• deal with their own or  can be made to work by the client .<br>• **Examples of sensors are**: gas sensor, water quality sensor, dampness sensor and so on. |
| **Processors** | • Processors are the brain of the IoT framework.<br>• Handle the information driven from Sensors to extract the knowledge from huge crude Processors for the most part work on continuous premise and can be effectively controlled by applications. Primarily installed on Microcontrollers. |

# Things in IOT

| Things in IoT | Functionality |
|---|---|
| **Gateways** | • Gateways are in charge of directing the prepared information and send it to legitimate areas for its (information) appropriate usage.<br>• Gateway causes to and fro information across devices and networks.<br>• Gateways can be implemented as LAN, WAN, PAN and so forth are cases of system portals. |
| **Applications** | • Applications frame another end of an IoT framework.<br>• Applications are fundamental for legitimate usage of the considerable number of information gathered.<br>• These cloud based applications which are in charge of rendering powerful intending to the information gathered.<br>• Applications are controlled by clients and are conveyance purpose of specific administrations.<br>• Examples are: home mechanization applications, security frameworks, mechanical control center point and so on. |

Paul Cant Eat Dogs, Donuts, Apples Cakes

PCEDDAC

# IOT REFERENCE MODEL

**Level 7: Collaboration and Processes**

- People and Business Processes

**Level 6: Application**

- Controll applications, Business intelligence and analytics

^

**Level 5: Data Abstraction**

- Aggregation and Access, Information Integration

^

**Level 4: Data Accumulation**

- Storage-Sampling,filtering,aggregation,converting the data

^

**Level 3: Edge (Fog) Computing**

- Peer to Peer communication, Data filtering, Cleanup, Packet content inspection

^

**Level 2: Connectivity**

- Edge Devices, Routers, Hubs etc, Protocols like Bluetooth, Wi-Fi

^

**Level 1: Physical Devices and Controllers**

- Sensors, Robots etc.

# Level 1: Physical Devices and Controllers

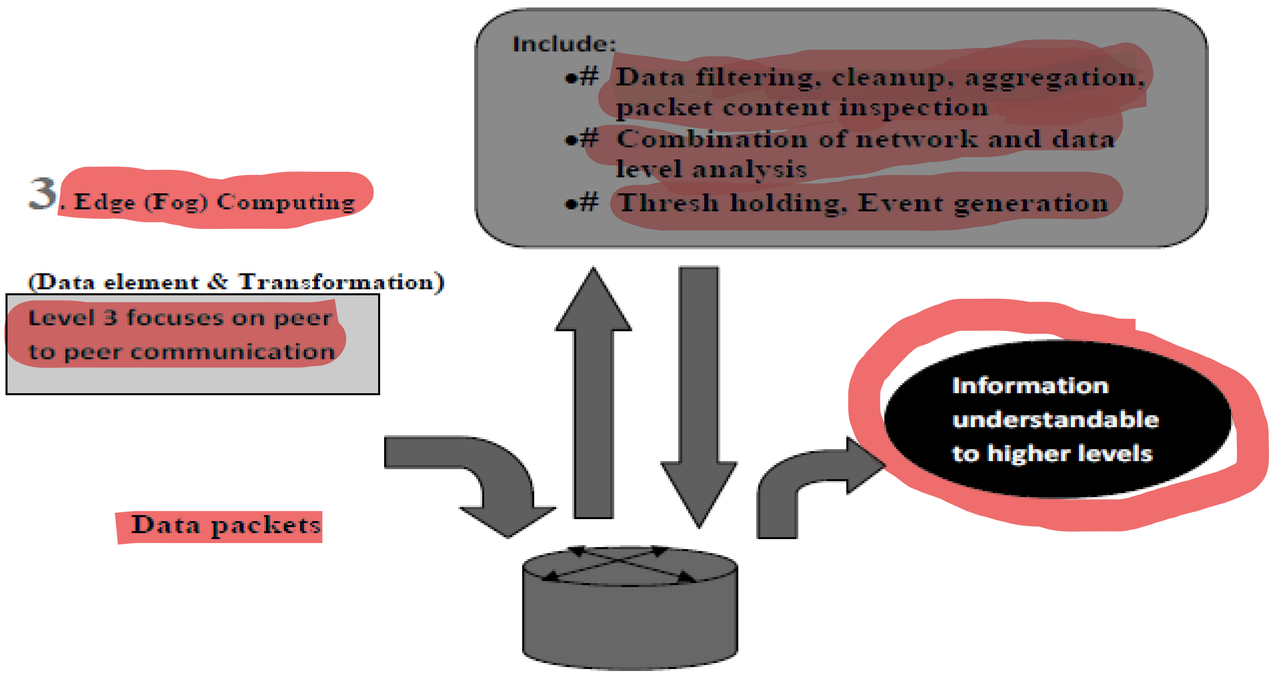
| Edge Devices in IoT | Functionality |
|---|---|
| • Sensors<br>• Cameras<br>• Robots | • Analog to digital conversion, as required<br>• Generating the data<br>• Being queried/controlled over the net |

**Level 1: Physical devices and controllers**

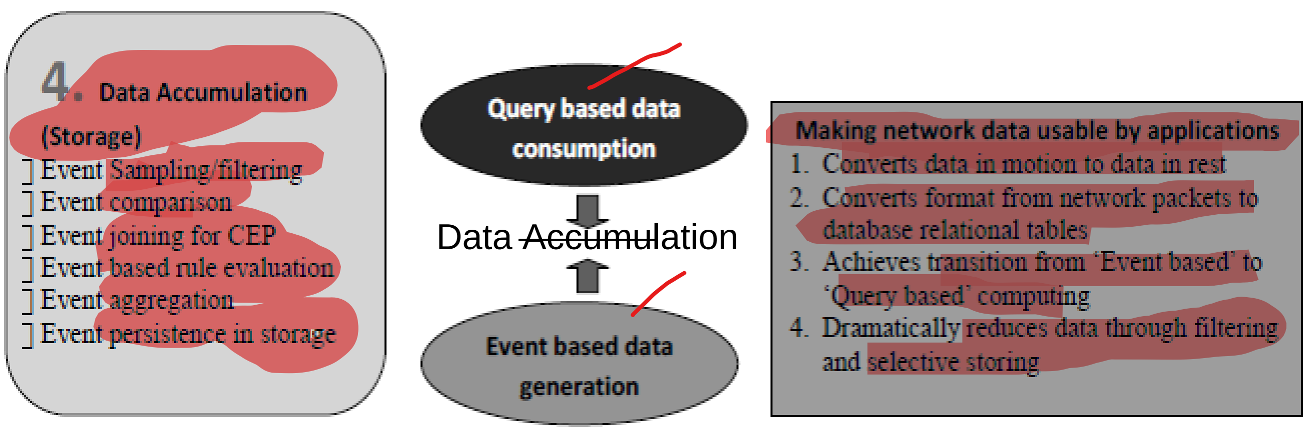
# Level 2: Connectivity

| Communication and processing Units | Connectivity includes |
|---|---|
| • Edge devices<br>• Routers<br>• Hubs<br>• switches | •Communicating with and between the level 1 devices<br>•Reliable delivery across the networks<br>•implementation of various protocols<br>•Switching & routing<br>•Translation between protocols<br>•Security at the network level<br>•Self learning - Networking analytics |

# Level 3: Edge (Fog) Computing



# Level 4: Data Accumulation



# Level 5: Data Abstraction

**5. Data Abstraction**

**(Aggregation & access)**

- Abstracting the data interface for applications

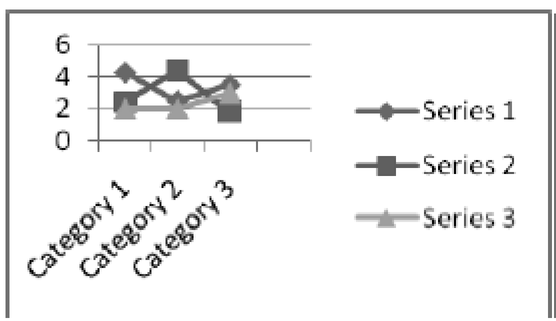
**Information integration**

1. Creates schemas and views of data in the manner that applications want
2. Combines data from multiple source, simplyfing the application
3. Filtering, selecting, projecting, and reformatting the data to serve the client applications
4. Reconciles differences in data shape, format, semantics, access protocol, and security
5. Filtering, selecting, projecting, and reformatting the data

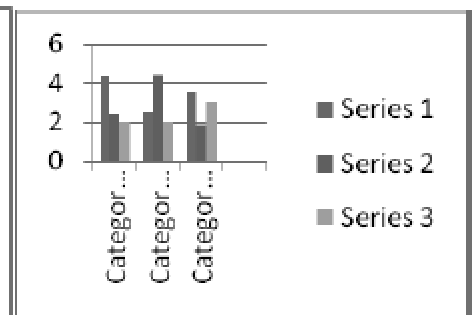
# Level 6: Application

Provide GUI for users to interact with the network and access services

**Control applications**




**Business intelligence and analytics**



# Level 7: Collaboration and Processes

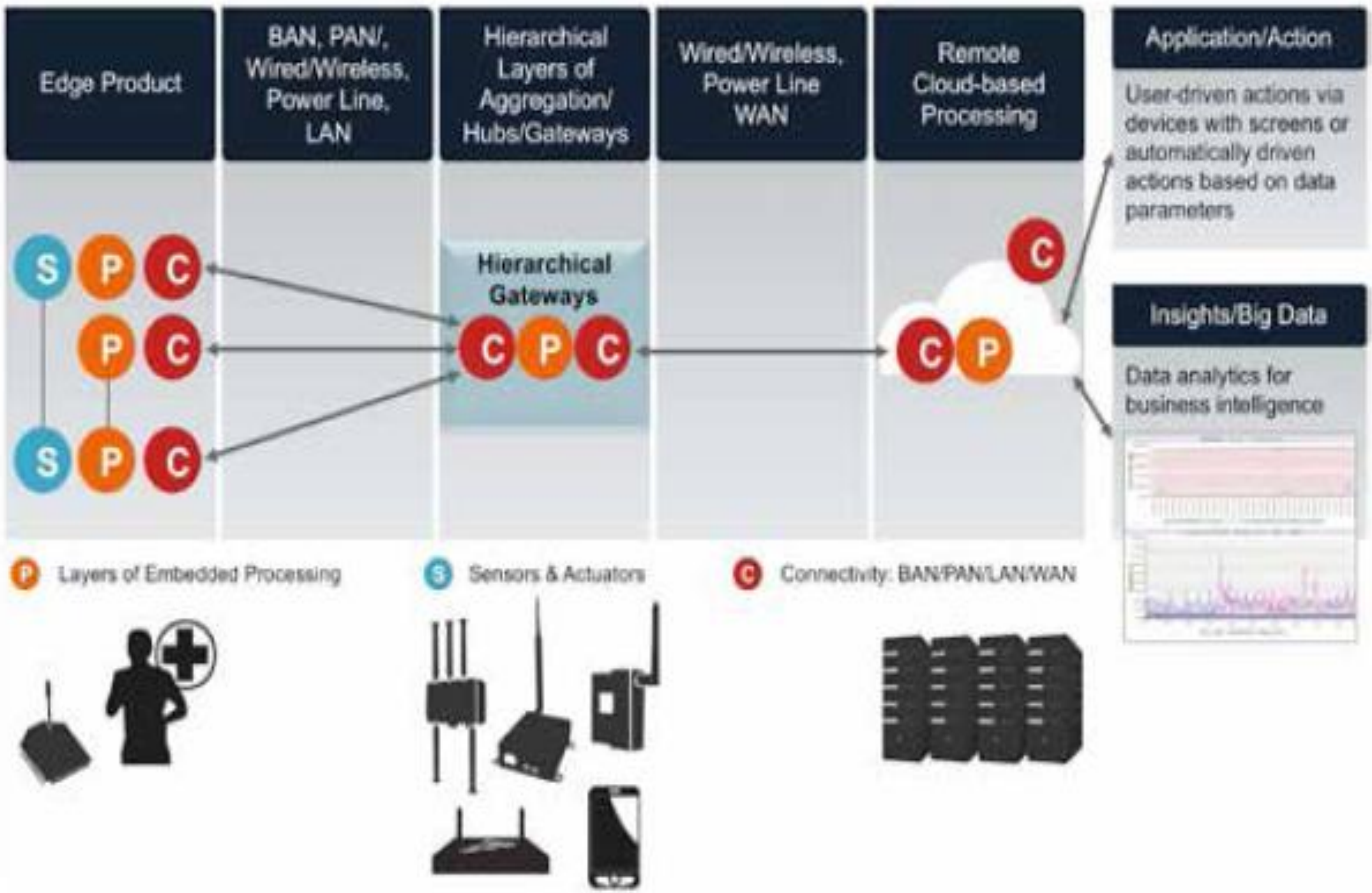
Businesses, people, governments, etc

7. Collaboration and Processes

| Involving People and business processes |
|---|

| Level 7: Collaboration and Processes |
|---|

# Building Blocks of IoT



# Building Blocks of IoT

Requirements common to all of the use cases of IoT include:

1) Sensing and data collection capability (sensing nodes)
2) Layers of local embedded processing capability (local embedded processing nodes)
3) Wired and/or wireless communication capability (connectivity nodes)
4) Software to automate tasks and enable new classes of services
5) Remote network/cloud-based embedded processing capability (remote embedded processing nodes)
6) Full security across the signal path

# 1. Sensing nodes

- The types of sensing nodes needed for the IoT vary widely, depending on the applications involved.
- Sensing nodes could include
  - a camera system for image monitoring
  - water or gas flow meters for smart energy
  - radar vision when active safety is needed
  - RFID readers sensing the presence of an object or person
  - doors and locks with open/close circuits that indicate a building intrusion
  - a simple thermometer measuring temperature.
- These nodes will all carry a unique ID and can be controlled separately via a remote command and control topology.

# 2) Layers of local embedded processing Nodes

- Embedded processing is at the heart of the IoT.
- Local processing capability is most often provided by MCUs, hybrid (MCUs/MPUs) or integrated MCU devices, which can provide the "real-time" embedded processing that is a key requirement of most IoT applications.
- Use cases vary significantly, and fully addressing the real-time embedded processing function requires a scalable strategy (using a scalable family of devices), as one size will not fit all.

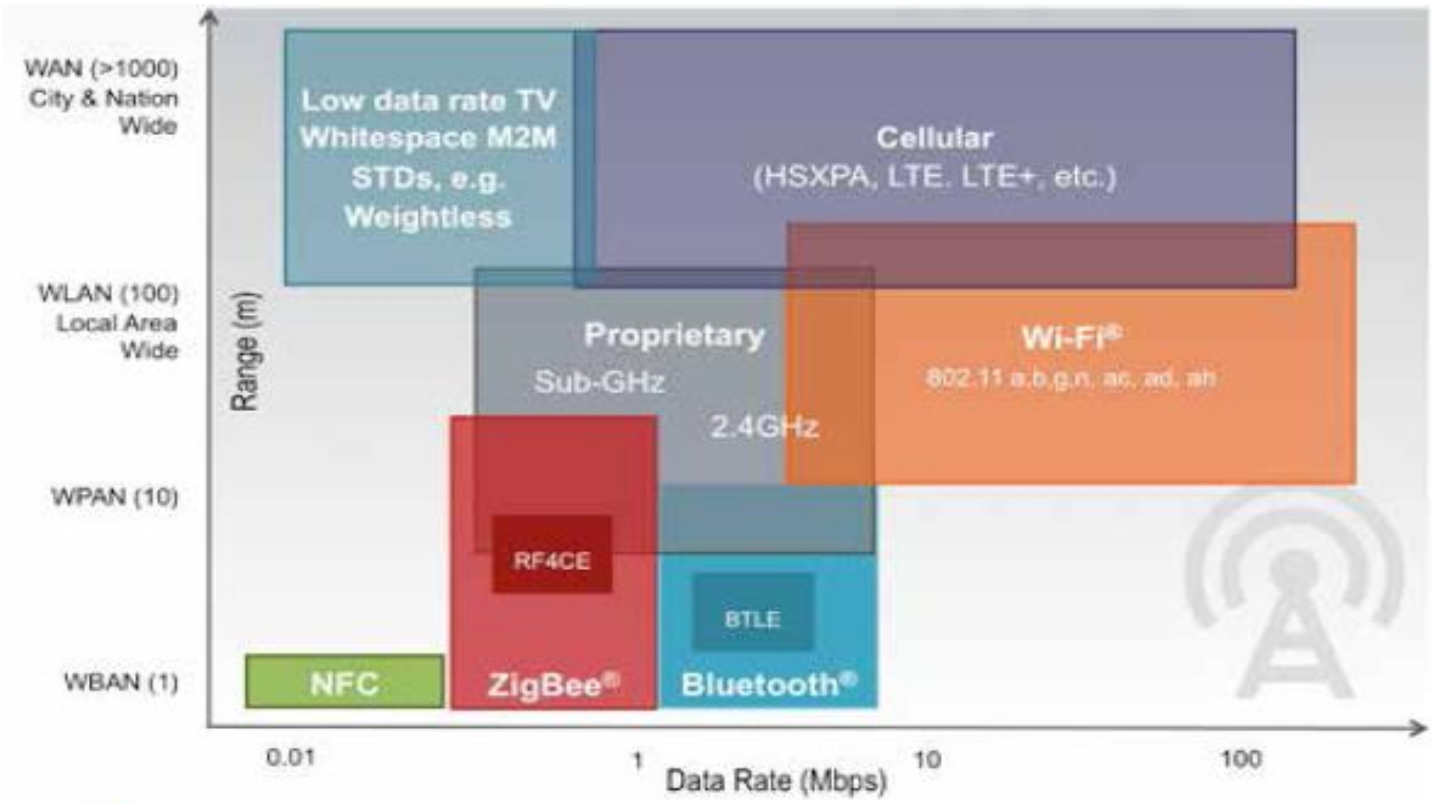
# 2) Layers of local embedded processing Nodes

- Requirements that make an MCU ideal for use in the IoT
  - Energy efficiency
  - Embedded architecture with a rich software ecosystem
  - Portfolio breadth that enables software scalability
  - Portfolio breadth that cost-effectively enables different levels of performance and a
  - robust mix of I/O interfaces
  - Cost-effectiveness
  - Quality and reliability
  - Security

# 3) Wired and/or wireless communication capability (connectivity nodes)

- The role of the communication node is to transfer information gathered by the sensing nodes and processed by local embedded processing nodes to the destinations identified by the local embedded processing nodes.
- And, once the data is remotely processed and new commands are generated, the communication node brings back the new commands to the local embedded processing nodes to execute a task.

# 3) Wired and/or wireless communication capability (connectivity nodes)- Todays wireless Landscape

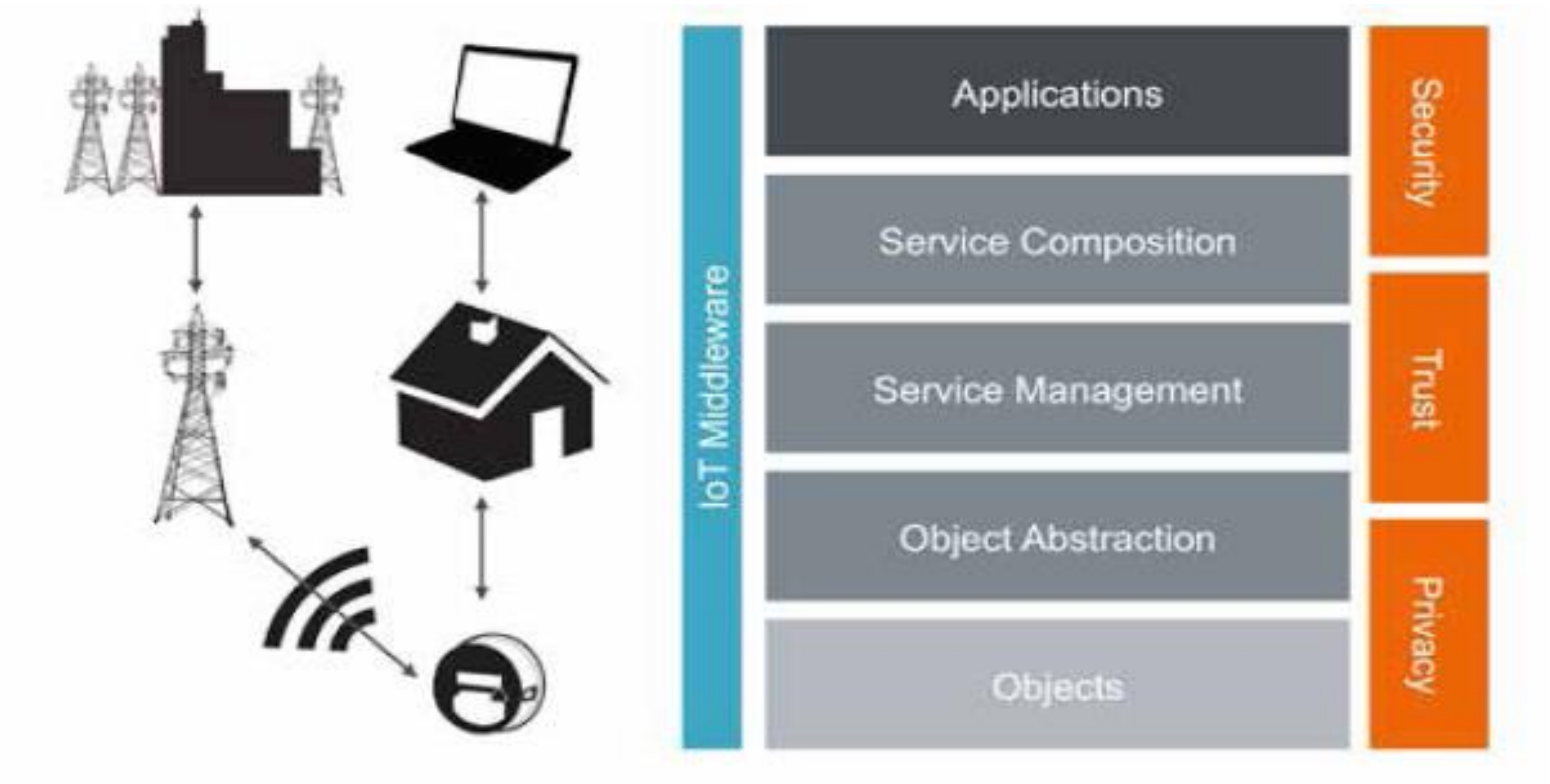


# 3) Wired and/or wireless communication capability (connectivity nodes)-Communication technologies

| | NFC | RFID | Blue-tooth® | Blue-tooth® LE | ANT | Proprietery (Sub-GHz & 2.4 GHz) | Wi-Fi® | ZigBee® | Z-wave | KNX | Wireless HART | 6LoWPAN | WiMAX | 2.5–3.5 G |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Network** | PAN | PAN | PAN | PAN | PAN | LAN | LAN | LAN | LAN | LAN | LAN | LAN | MAN | WAN |
| **Topology** | P2P | P2P | Star | Star | P2P, Star, Tree Mesh | Star, Mesh | Star | Mesh, Star, Tree | Mesh | Mesh, Star, Tree | Mesh, Star | Mesh, Star | Mesh | Mesh |
| **Power** | Very Low | Very Low | Low | Very Low | Very Low | Very Low to Low | Low-High | Very Low | Very Low | Very Low | Very Low | Very Low | High | High |
| **Speed** | 400 Kbs | 400 Kbs | 700 kbs | 1 Mbs | 1 Mbs | 250 kbs | 11-100 Mbs | 250 kbs | 40 Kbs | 1.2 Kbps | 250 kbs | 250 Kbs | 11-100 Mbs | 1.8-7.2 Mbs |
| **Range** | <10 cm | <3 m | <30 m | 5-10 m | 1-30 m | 10-70 m | 4-20 m | 10-300 m | 30 m | 800 m | 200 m | 800 m (Sub-GHz) | 50 km | Cellular network |
| **Application** | Pay, get access, share, initiate service, easy setup | Item tracking | Network for data exchange, headset | Health and fitness | Sports and fitness | Point to point connectivity | Internet, multimedia | Sensor networks, building and industrial automation | Residential lighting and automation | Building automation | Industrial sensing networks | Senor networks, building and industrial automation | Metro area broadband Internet connectivity | Cellular phones and telemetry |
| **Cost Adder** | Low | Low | Low | Low | Low | Medium | Medium | Medium | Low | Medium | Medium | Medium | High | High |

# 4) Software to Automate tasks

- Software Service Fabric for Metering Application



# 5) Remote network/cloud-based embedded processing

Centralised

- Some companies promote that all devices will be "dumb nodes," with all processing and decision-making done within "their cloud."
- Alternatively, some believe only minimal access to the cloud for basic Internet related services will be required, with most of the "thinking" done locally. De-centralised
- The architecture and building blocks of the IoT approaches, which will likely be necessary due to the wide variety of use cases and configurations anticipated.
- That flexibility will be needed to optimize system-level performance.

# 6) Full Security across the Entire Path

- Information needs to be available when needed
- Information needs to be confidential
- The integrity of data needs to be assured

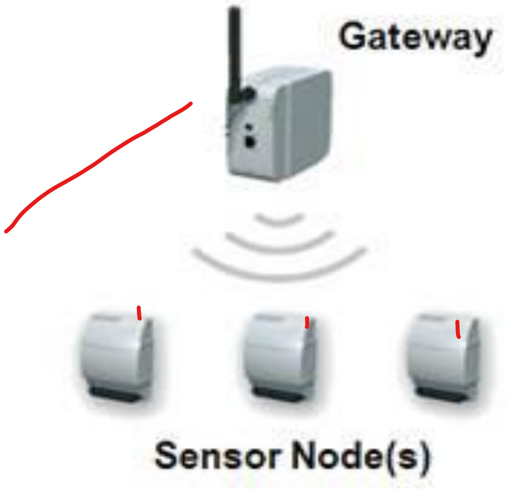
# Wireless sensor Networks

# Overview

- What is a Wireless sensor network
  - Applications of WSN
  - WSN system architecture
  - WSN Network topologies
  - Components of a WSN node

# What is a Wireless Sensor Network?

- (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions.



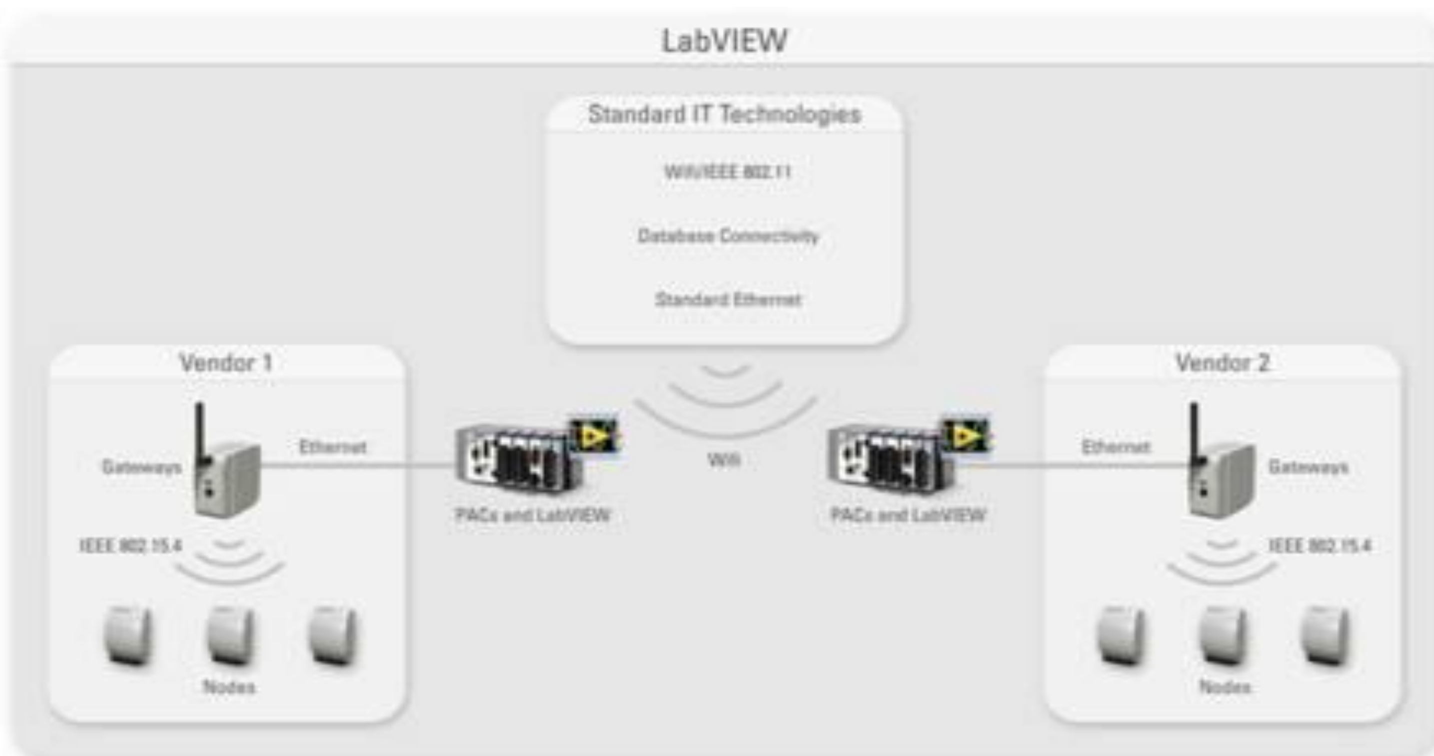
# What is a Wireless Sensor Network?

- A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes as shown in Figure.
- The wireless protocol selection depends on your application requirements.
- Some of the available standards include 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.

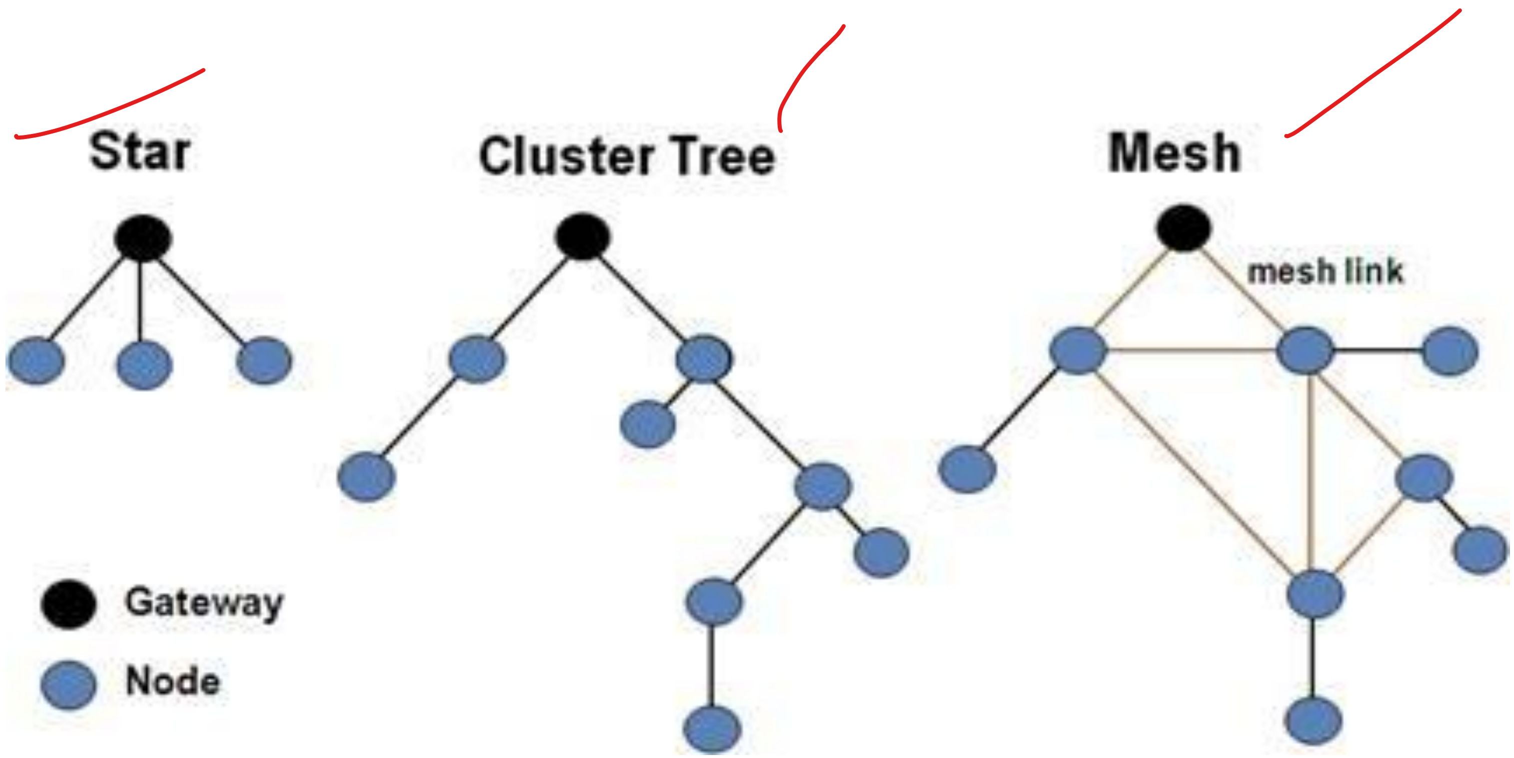
# Applications of Wireless Sensor Networks

- WSN applications for areas including **health care**, **utilities**, and **remote monitoring**.
- In **health care**, wireless devices make less invasive **patient monitoring** and health care possible.
- For **utilities** such as the **electricity grid**, **streetlights**, and **water municipals**, wireless sensors offer a lower-cost method for collecting system health data to reduce energy usage and better manage resources.
- **Remote monitoring** applications include:
  - Environmental monitoring of air, water, and soil
  - Structural monitoring for buildings and bridges
  - Industrial machine monitoring
  - Process monitoring
  - Asset tracking

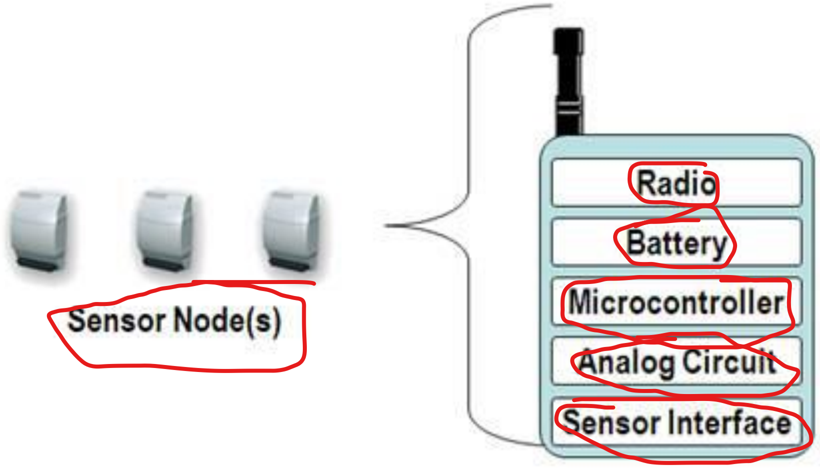
# WSN System Architecture



# WSN Network Topologies



# Components of a WSN node



# Components of a WSN node

- A WSN node contains several technical components. These include the **radio, battery, microcontroller, analog circuit, and sensor interface**.
- When using WSN **radio technology**
  - higher radio data rates and more frequent radio use consume more power.
  - Often three years of battery life is a requirement
  - so many of the WSN systems today are based on ZigBee due to its low-power consumption.
  - Because battery life and power management technology are constantly evolving and because of the available IEEE 802.11 bandwidth, Wi-Fi is an interesting technology.

# Components of a WSN node

- The second technology consideration for WSN systems is the **battery**.
  - The size and weight of batteries as well as international standards for shipping batteries and battery availability.
  - The low cost and wide availability of carbon zinc and alkaline batteries make them a common choice.

# Components of a WSN node

- To extend battery life, a WSN node periodically wakes up and transmits data by powering on the radio and then powering it back off to conserve energy.
- WSN radio technology must efficiently transmit a signal and allow the system to go back to sleep with minimal power use. This means the processor involved must also be able to wake, power up, and return to sleep mode efficiently.
- Microprocessor trends for WSNs include reducing power consumption while maintaining or increasing processor speed. Much like your radio choice, the power consumption and processing speed trade-off is a key concern when selecting a processor for WSNs. This makes the x86 architecture a difficult option for battery-powered devices.

# Questions

- Explain Things in IoT?
- Illustrate the IoT Reference model?
- Define IoT, entity in IoT, IoT ecosystem, IoT Device and M2M?
- Deficit the reasons why data generated from multiple devices may not land in the same data storage?
- Illustrate about enabling technologies in IoT?
- Enlist the security measures to be offered in the IoT Reference model?
- How IoT infers information from knowledge and data?
- Describe the basic capabilities of Device in IoT?

# Questions

- Explain the applications of IoT incorporating areas specific to urban areas, energy sustainable systems, retail, mechanical and e-health.
- Illustrate the functions of Data abstraction level of IoT Reference model?
- Explain the potential applications of Wireless Sensor Networks?
- Describe the basic capabilities of Device in IoT?
- Explain the Data Accumulation phase of IoT reference model?

# Questions

- Enlist the security measures to be offered in the IoT Reference model?
- Illustrate the characteristics of IoT?
- Illustrate the functionalities of connectivity layer in the IoT reference model?
- Explain the Data element Analysis and transformation phase of IoT reference model?

Thank you