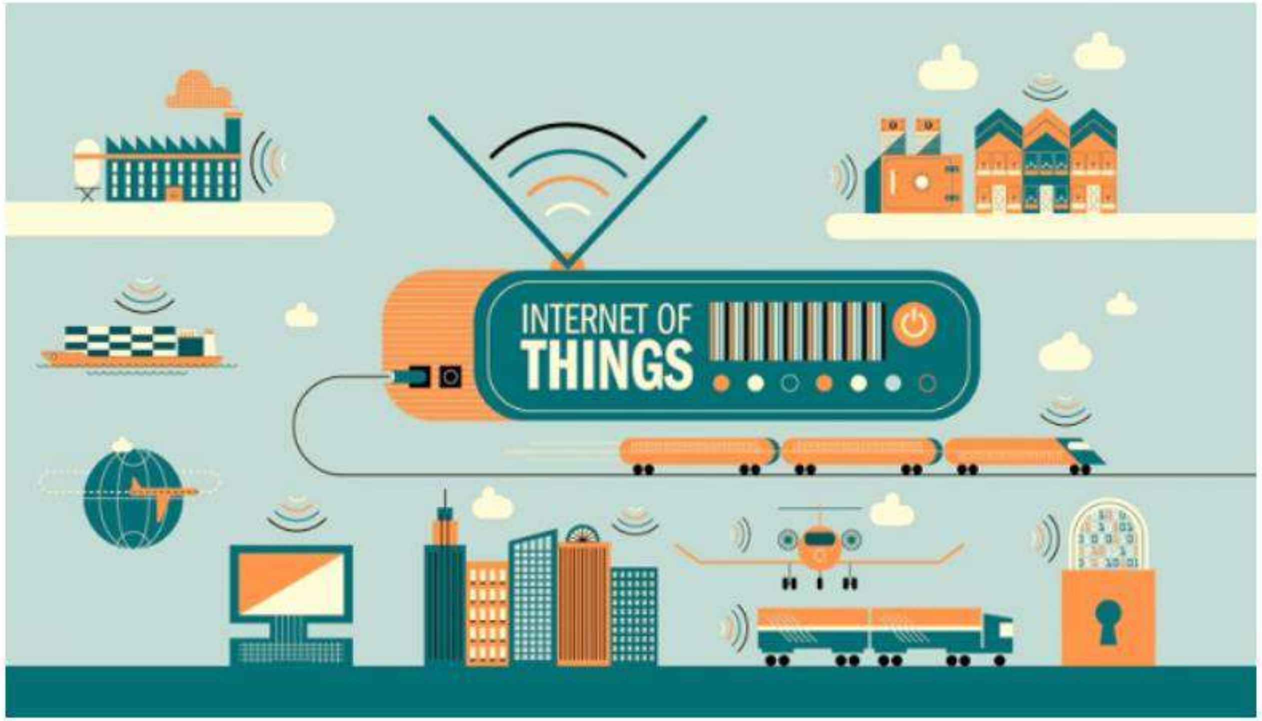


Prof Raghavendran T S
Asst Prof, School of C&IT, Reva University, Bengaluru
Raghavendran.ts@reva.edu.in

www.reva.edu.in

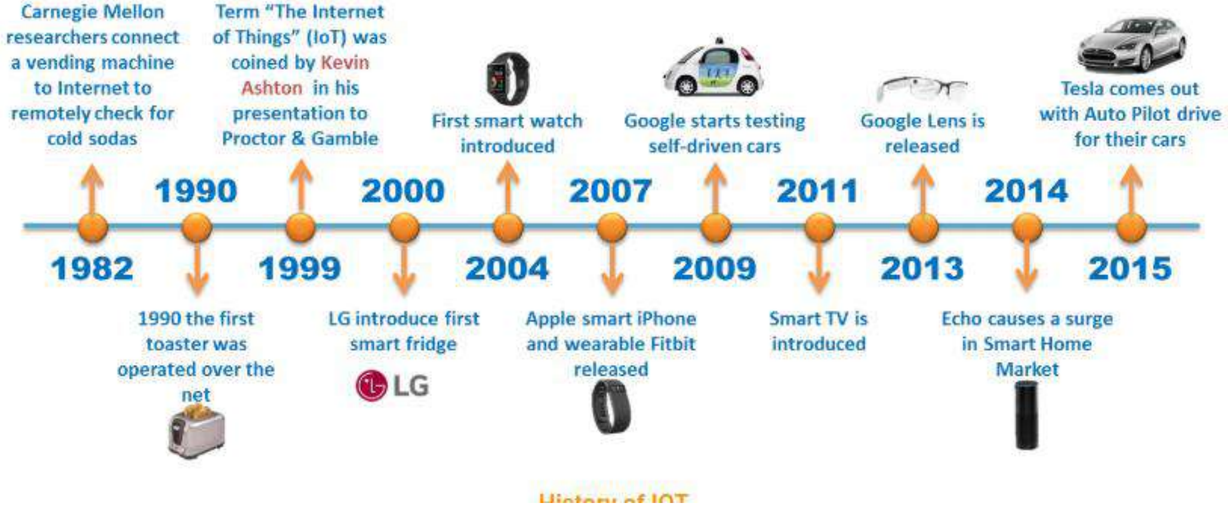
B22EK0601

Agenda

- Genesis of IOT
- IOT & Digitization
- IOT Impact
- Convergence of IT & OT
- IOT Challenges

Genesis of IOT

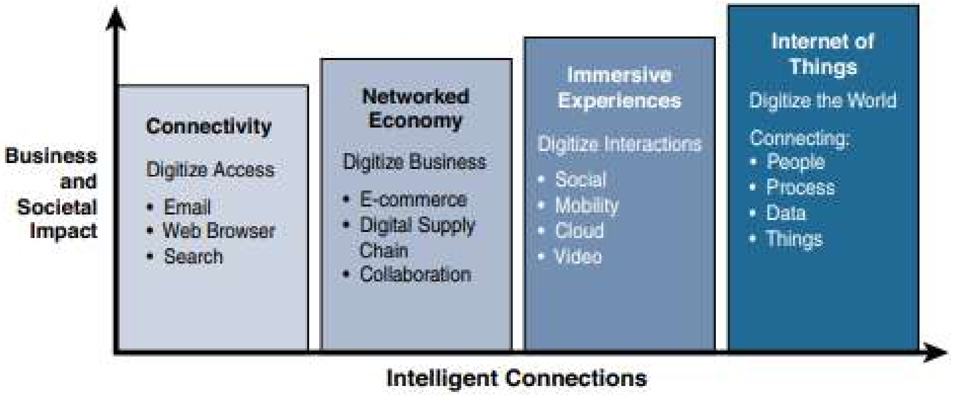
- IOT Age started in 2008-09. Where number of devices connected to the internet surpassed the world's human population.
- Kevin Ashtron was person behind coining the of the term "Internet of Things".
- In 20th Century Computers were termed brainy without any senses and were completely dependable on human's data.
- In 21st century Computers are sensing the data themselves and are brainy by default.



Evolutionary phases of Internet

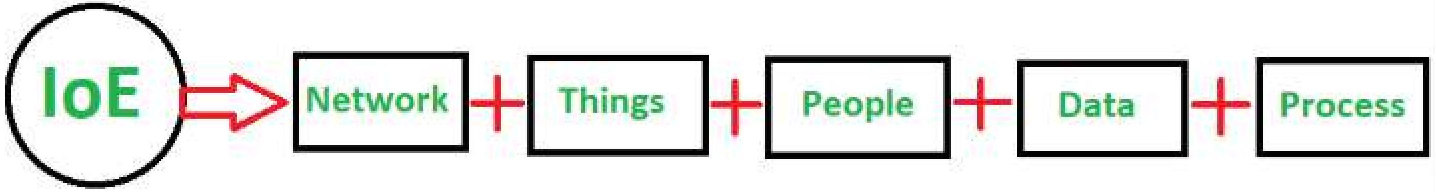
- Connectivity Phase- Digitize Access
- Networked Economy- Digitize Business
- Immersive Experiences- Digitize Interactions
- Digitize the World

Genesis of IoT



IOT & Digitization

- IOT is IOT (Internet of Things) & Digitization is IOE (Internet of Everything).
- IOT is Prime Enabler for Digitization as smart objects & increased connectivity drives Digitization.
- IOE is just extension of IOT.



Impact of IOT

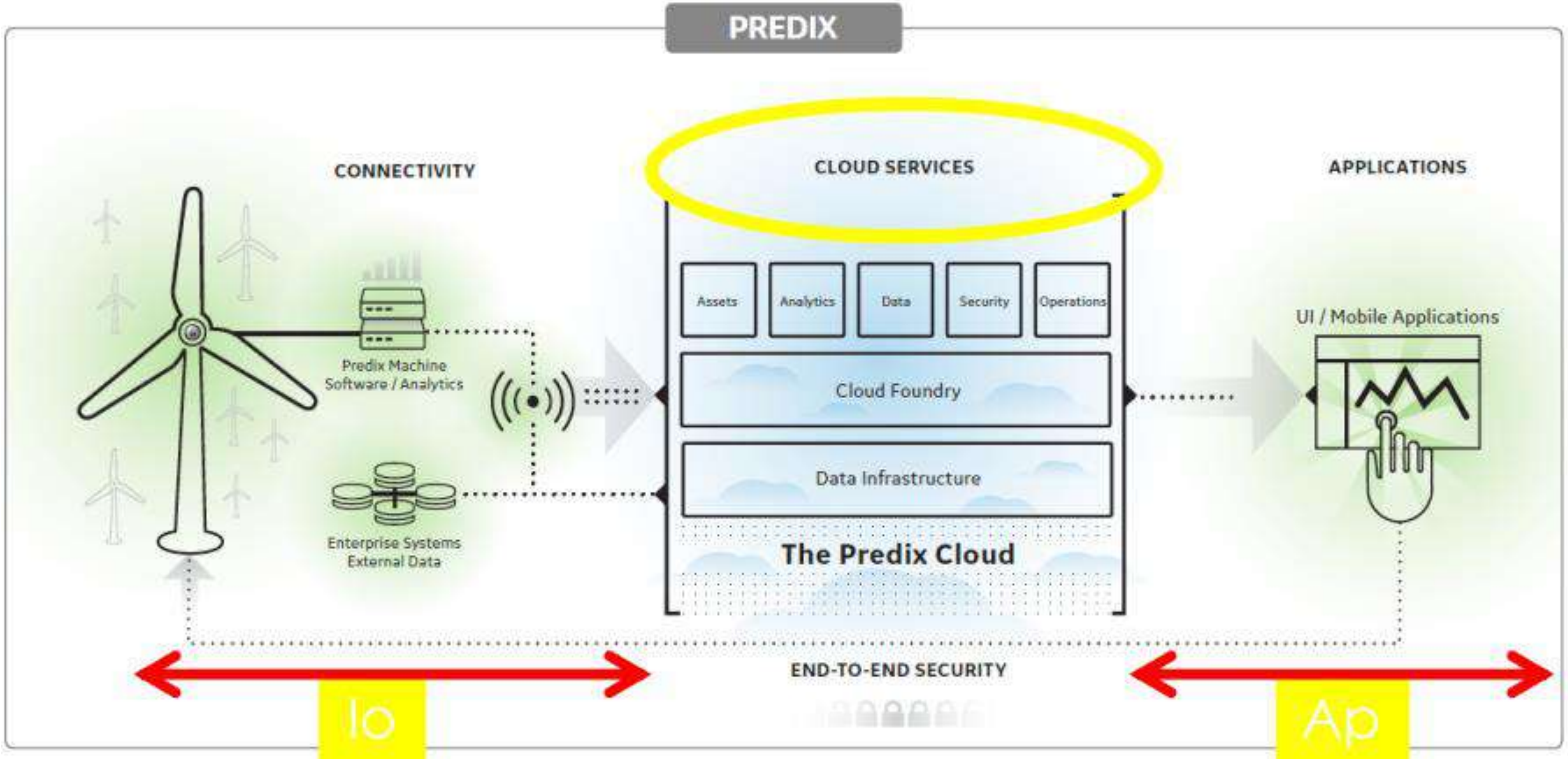
Driverless Cars---

- Basis Sensors- To Monitor Oil Pressure, Tyre Pressure, Temperature & Humidity of Surroundings.
- Ultrasonic Sensors To detect obstacles in front and rear end.
- Cameras providing images of car surroundings.

These sensors collecting the data and helping the car to make decisions on how to navigate.

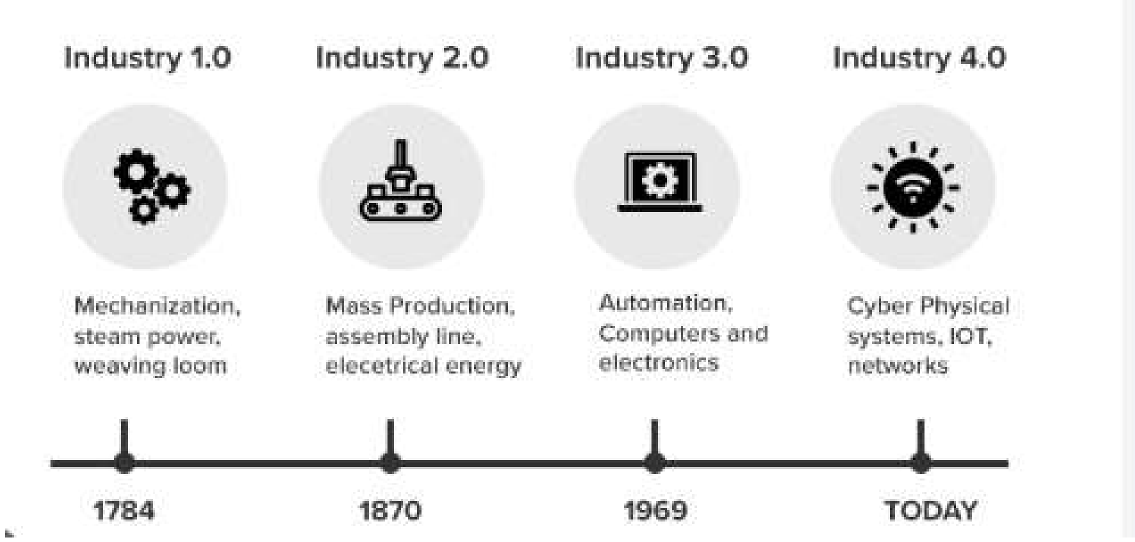
Vehicle-to-Vehicle Communication:- Enables car to have a 360 degree view of other vehicles on roads & Allows cars to have a exchange of information based on position, speed and distance.

IOT Predictive Maintenance



- IOT Enables Predictive Maintenance by analyzing data from sensors on equipment to predict failures even before they occur. This reduces unexpected downtime, enhances equipment, longitivity and reduces maintenance costs.

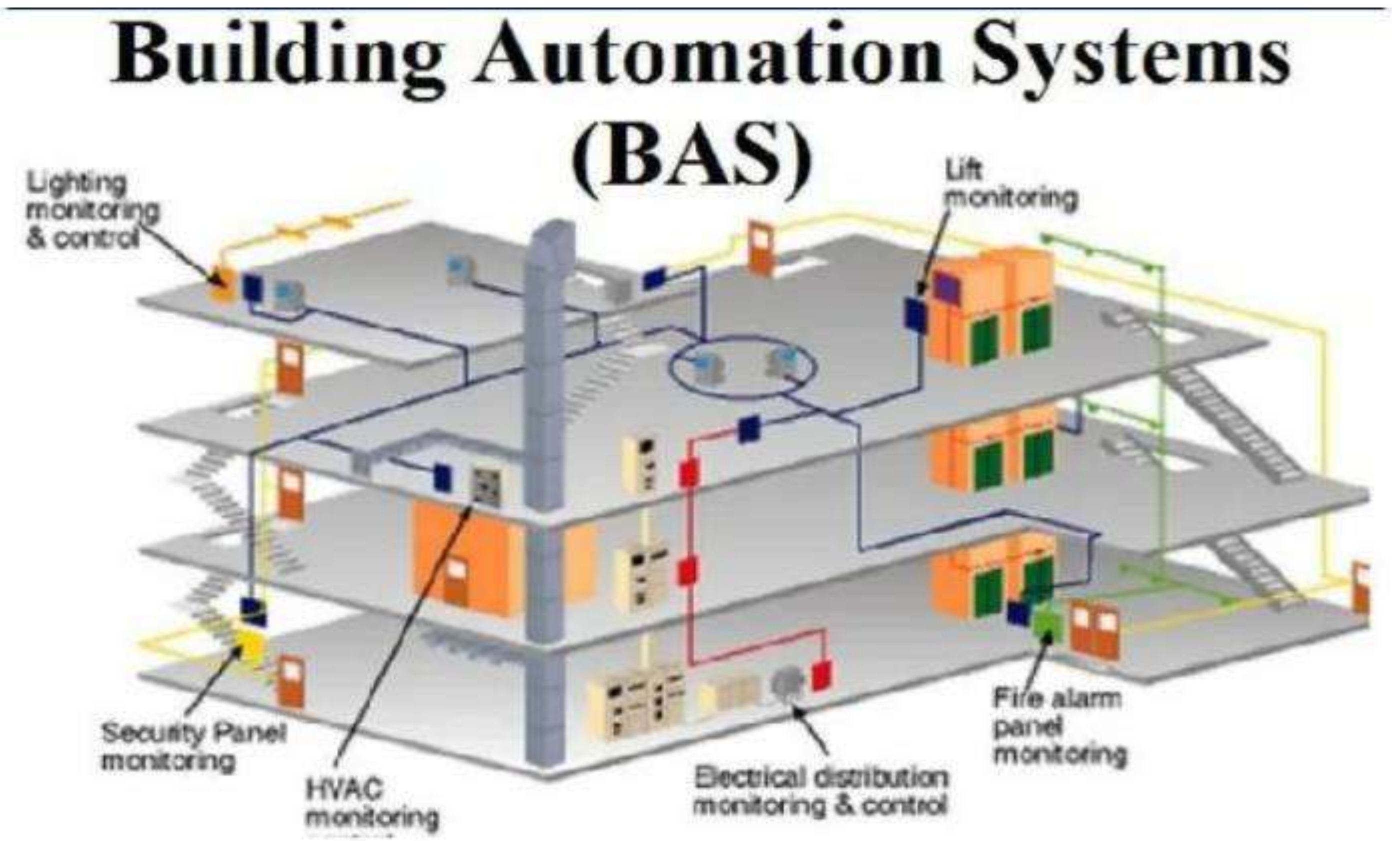
IOT Industrial Revolutions



Smart Connected Buildings

Smart Connected Buildings utilizes Technology and data to monitor and control various building systems, including lighting, HVAC and security. This interconnectedness enables real-time adjustments that enhance comfort and efficiency.

BACS Framework for Smart Buildings

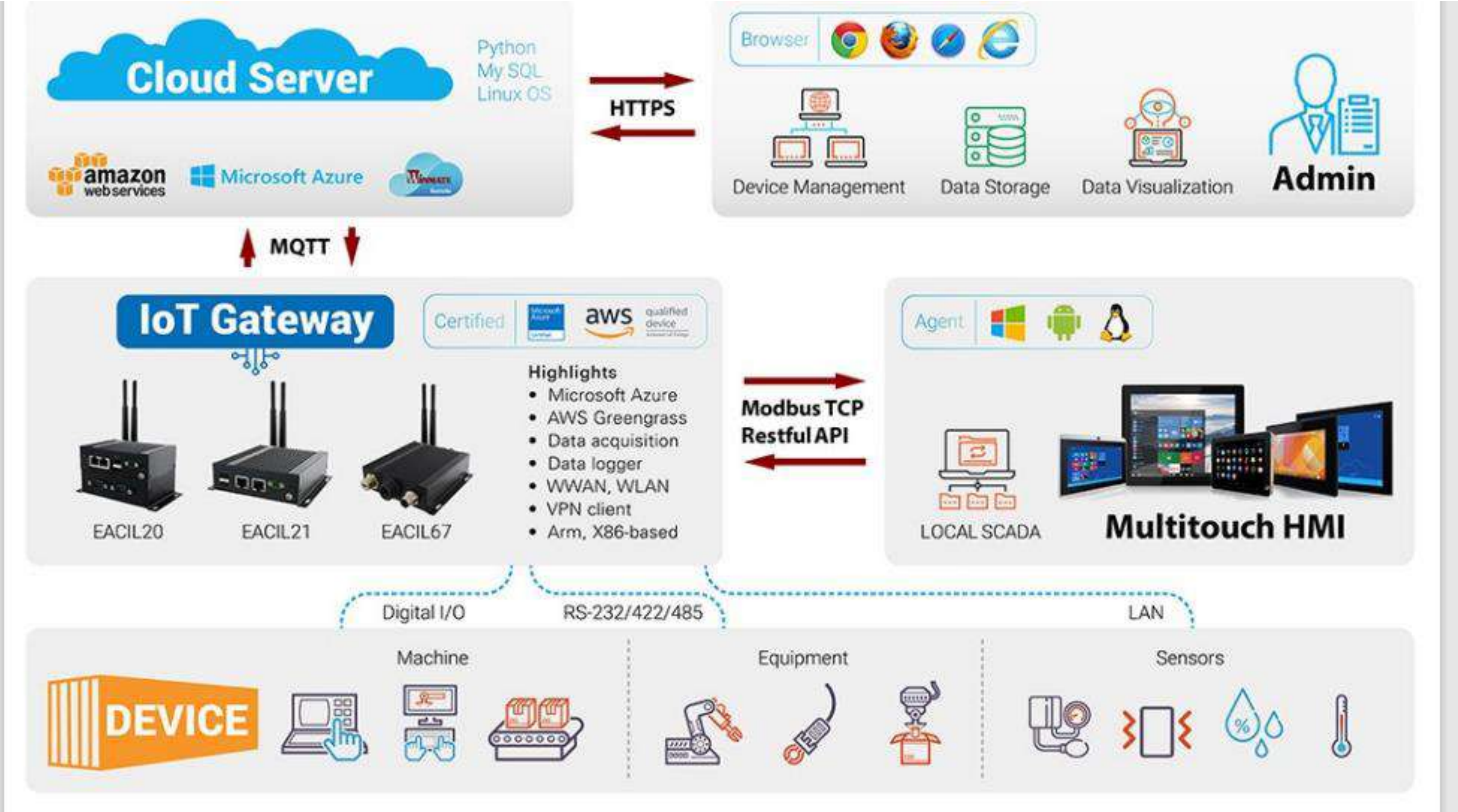


Smart City

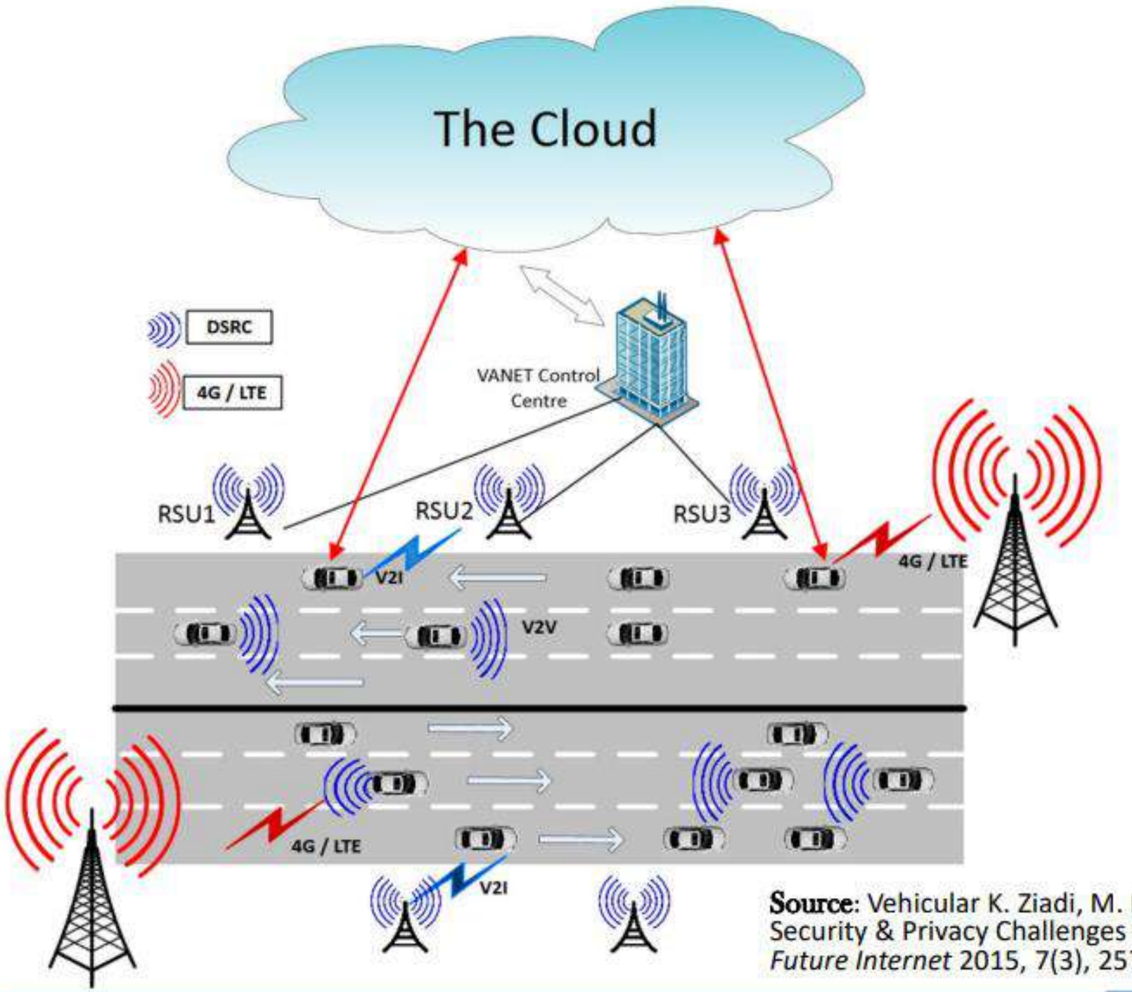
- Transportation:- Smart Traffic Management , Intelligent Parking system, Smart Bike Sharing systems.
- Energy & Utilities:- Smart Grids, Smart Streetlights, Smart Waste Management.
- Public Safety & Security:- Smart Surveillance Systems, Smart crime prevention.
- Waste Management:- Smart Waste Management, Smart Recycling system.
- Environmental Monitoring:- Air Quality Monitoring, Noise Pollution Monitoring, Weather Monitoring.
- Smart Building & Homes:- Smart Energy Management, Smart Home Automation, Smart Building Maintenance.

D:\Reva\ADE
t\Advanced IOT\Vi

Industrial IoT



Connected Cars



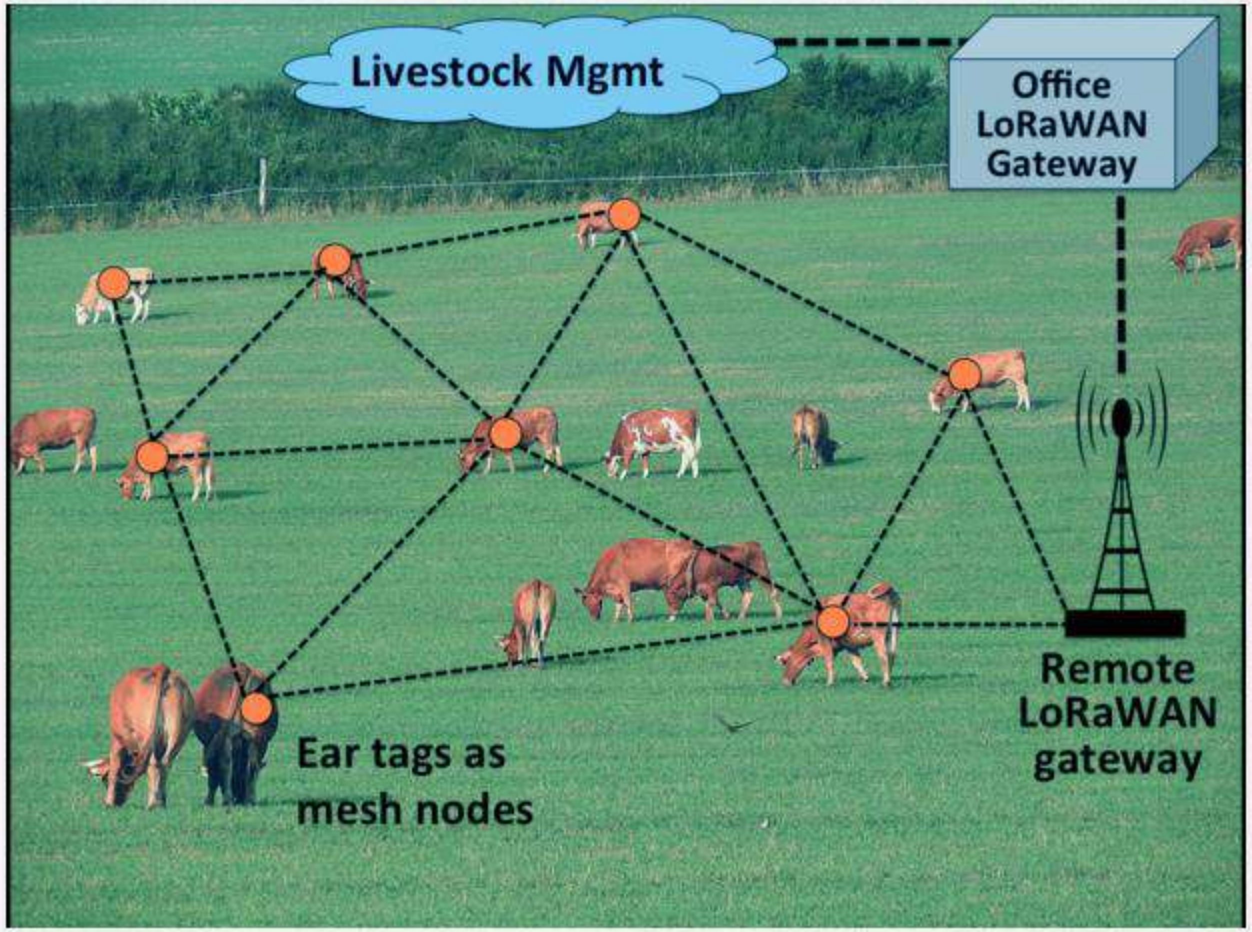
Source: Vehicular K. Ziadi, M. Rajarajan, "Internet: Security & Privacy Challenges and Opportunities", *Future Internet* 2015, 7(3), 257-275.

D:\Reva\ADE
t\Advanced IOT\Vi

Smart Agriculture

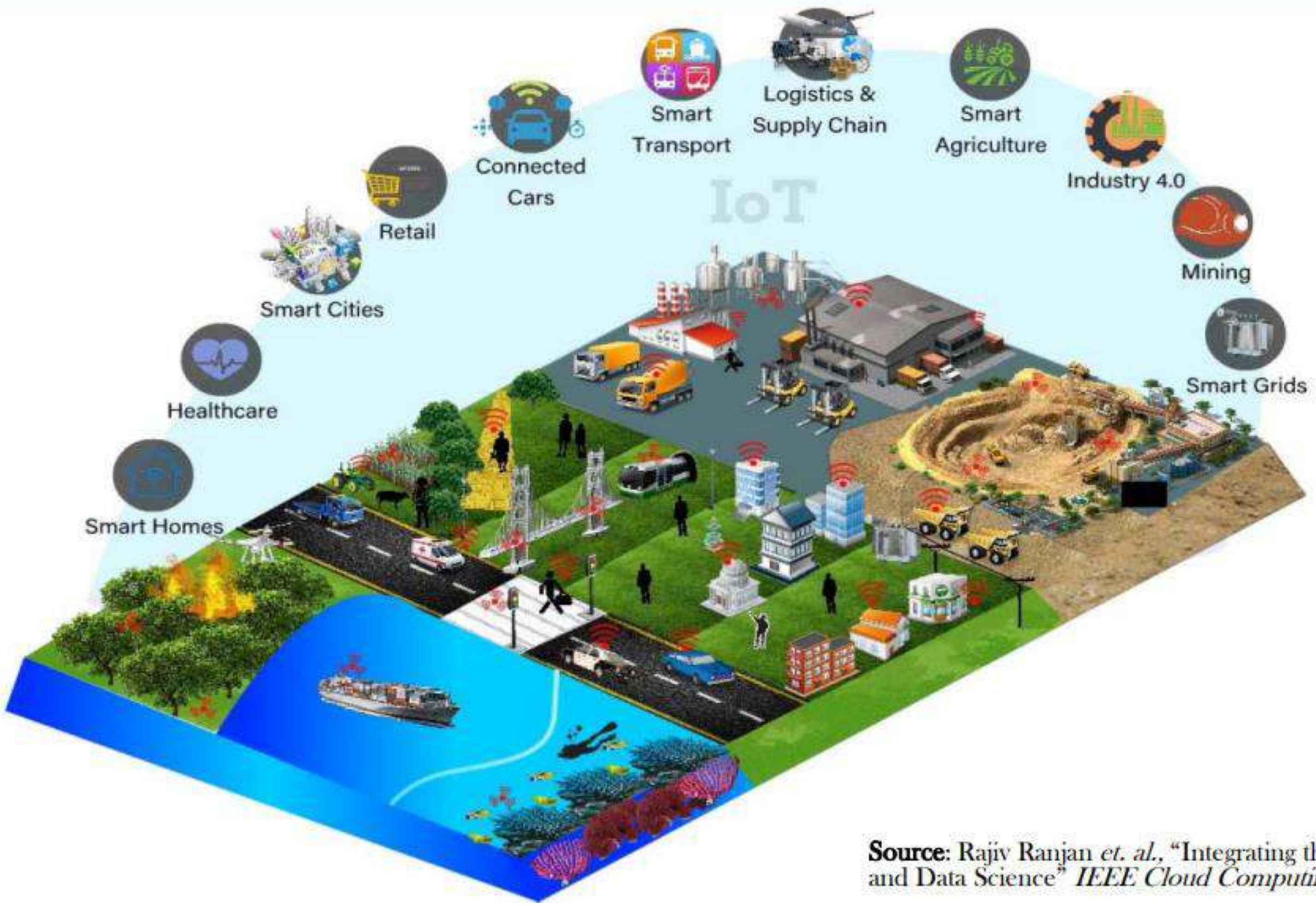
Smart farming – IoT #2.mp4

Livestock Management



D:\Reva\ADE
t\Advanced IOT\Vi

Many More IOT



Source: Rajiv Ranjan *et. al.*, "Integrating the IoT and Data Science" *IEEE Cloud Computing*, 2018

IOT Challenges

Sensors
- Limited resources
- Limited types of sensors

Scale
- millions of devices are connected to form IoT

Privacy
- which personal data to share with whom
- how to control

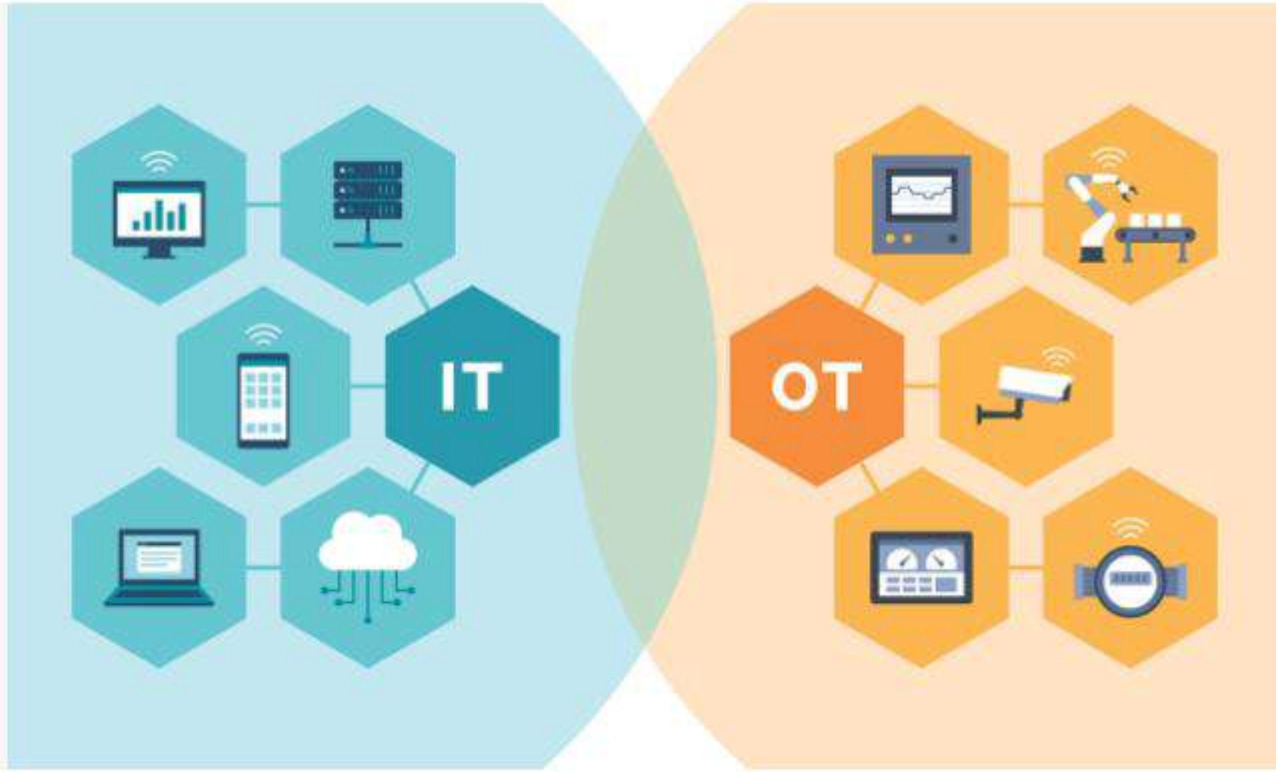
Security
- "things" becomes connected, so security becomes complex

Low Power Network
- Devices should remain connected to the Internet for years
- High network latency

Big data and Data analytics
- massive amount of sensor data
- different sources and various forms
- extract intelligence form the heaps of data

Interoperability
- various protocol, various architecture
- unavailability of standardized platform
- different technology leads to interoperability issue
- Recent IoT standards are minimizing this problem

Convergence of IT (Information Technology) & OT (Operational Technology)



IT/OT convergence is the integration of IT systems with OT systems, enabling data exchange, communication, and collaboration across both domains.

- **Enhanced visibility:** By connecting IT and OT systems, organizations can gain a holistic view of their operations and performance across the entire value chain. This enables them to monitor key performance indicators (KPIs), identify issues and opportunities, and make informed decisions.
- **Improved efficiency:** By integrating IT and OT systems, organizations can automate workflows, optimize processes, and reduce waste and downtime. This enables them to increase productivity, quality, and profitability.
- **Increased innovation**: By leveraging IT and OT systems, organizations can access new sources of data and insights, create new products and services, and explore new business models. This enables them to differentiate themselves from competitors and meet changing customer demands.

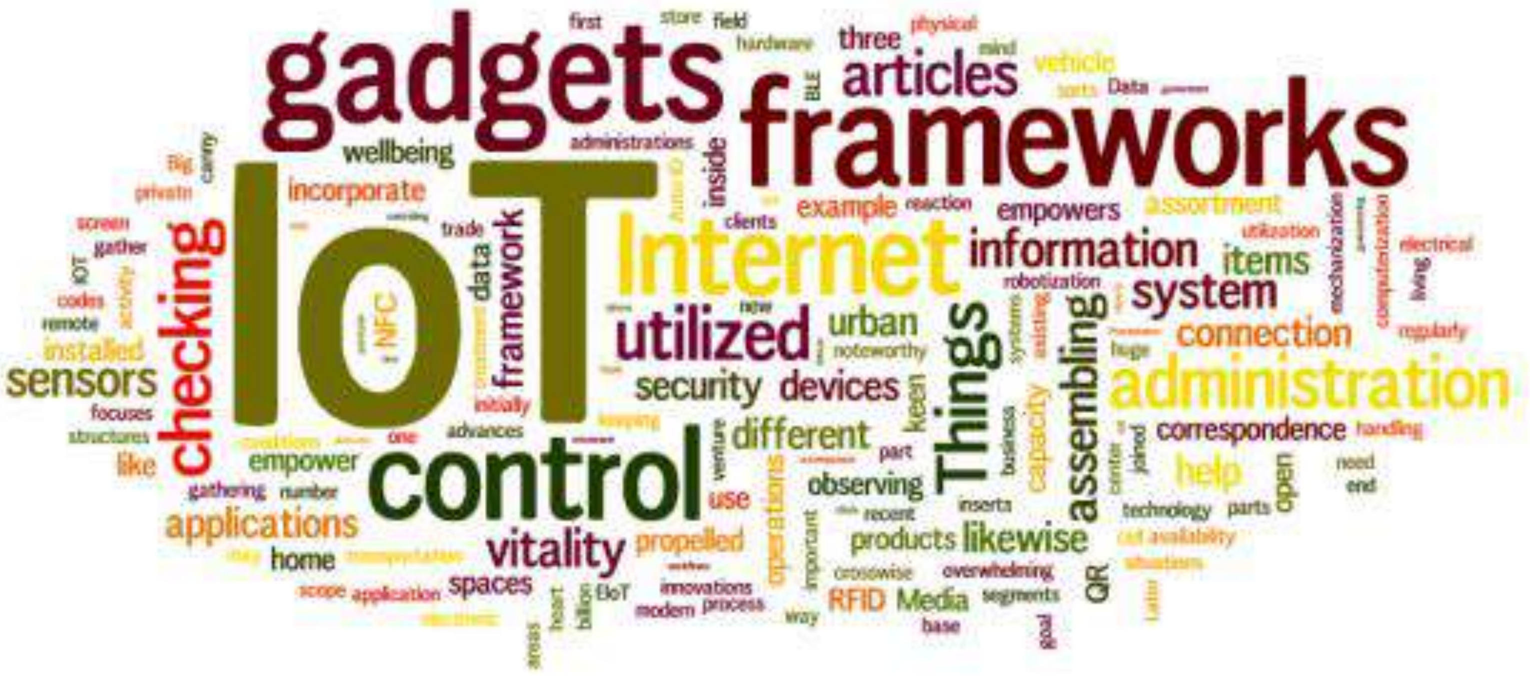
IT-OT Comparison

Criterion	Industrial OT Network	Enterprise IT Network
Operational focus	Keep the business operating 24x7	Manage the computers, data, and employee communication system in a secure way
Priorities	1. Availability 2. Integrity 3. Security	1. Security 2. Integrity 3. Availability
Types of data	Monitoring, control, and supervisory data	Voice, video, transactional, and bulk data
Security	Controlled physical access to devices	Devices and users authenticated to the network
Implication of failure	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible
Network upgrades (software or hardware)	Only during operational maintenance windows	Often requires an outage window when workers are not onsite; impact can be mitigated
Security vulnerability	Low: OT networks are isolated and often use proprietary protocols	High: continual patching of hosts is required, and the network is connected to Internet and requires vigilant protection

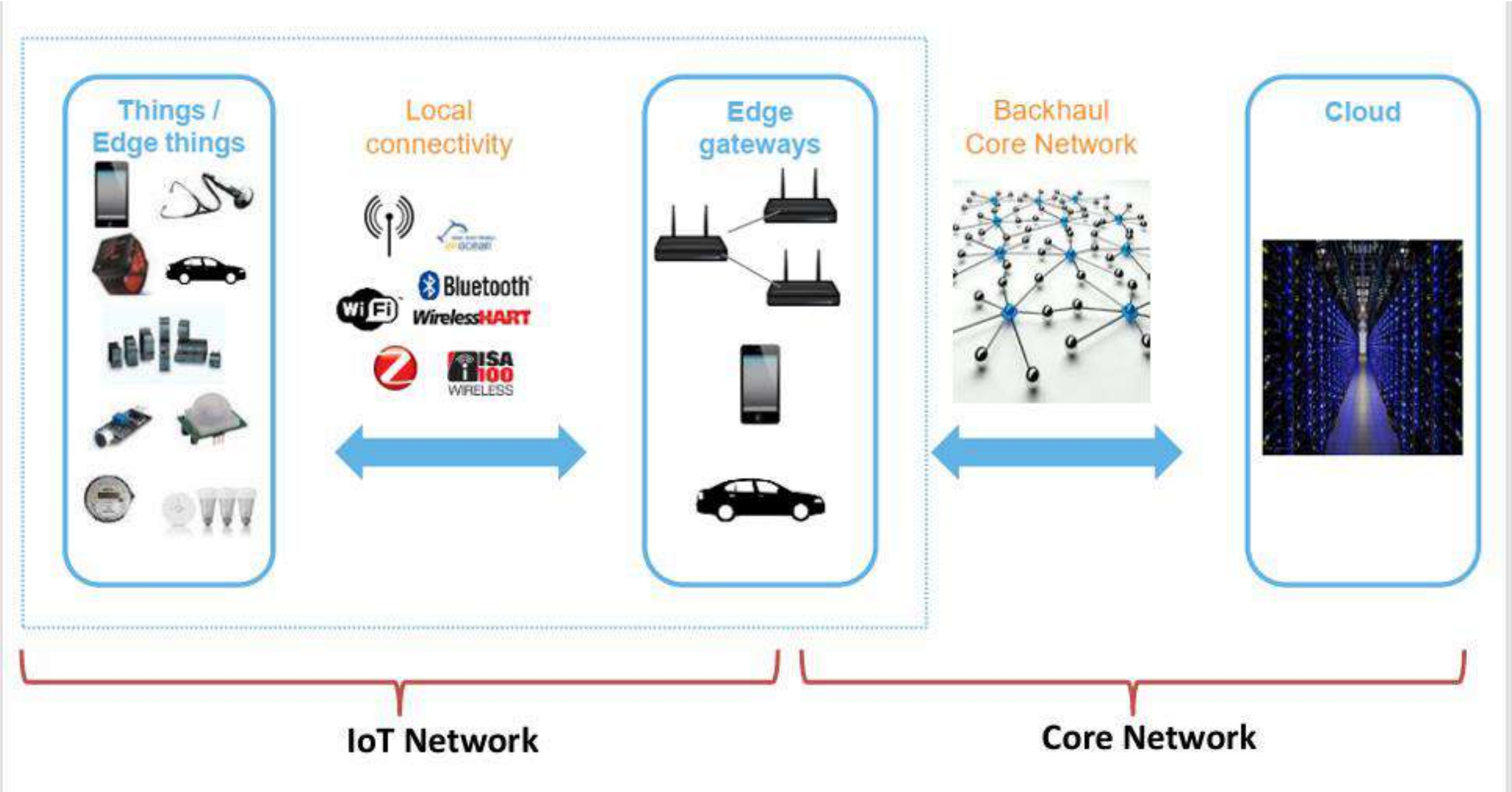
Summary

- This chapter provides an introductory look at the Internet of Things and answers the question “What is IoT?” IoT is about connecting the unconnected, enabling smart objects to communicate with other objects, systems, and people.
- The end result is an intelligent network that allows more control of the physical world and the enablement of advanced applications. This chapter also provides a historical look at IoT, along with a current view of IoT as the next evolutionary phase of the Internet
- . This chapter details a few high-level use cases to show the impact of IoT and some of the ways it will be changing our world. A number of IoT concepts and terms are defined throughout this chapter
- . The differences between IoT and digitization are discussed, as well as the convergence between IT and OT.
- The last section details the challenges faced by IoT. This chapter should leave you with a clearer understanding of what IoT is all about. In addition, this chapter serves as the foundational block from which you can dive further into IoT in the following chapters

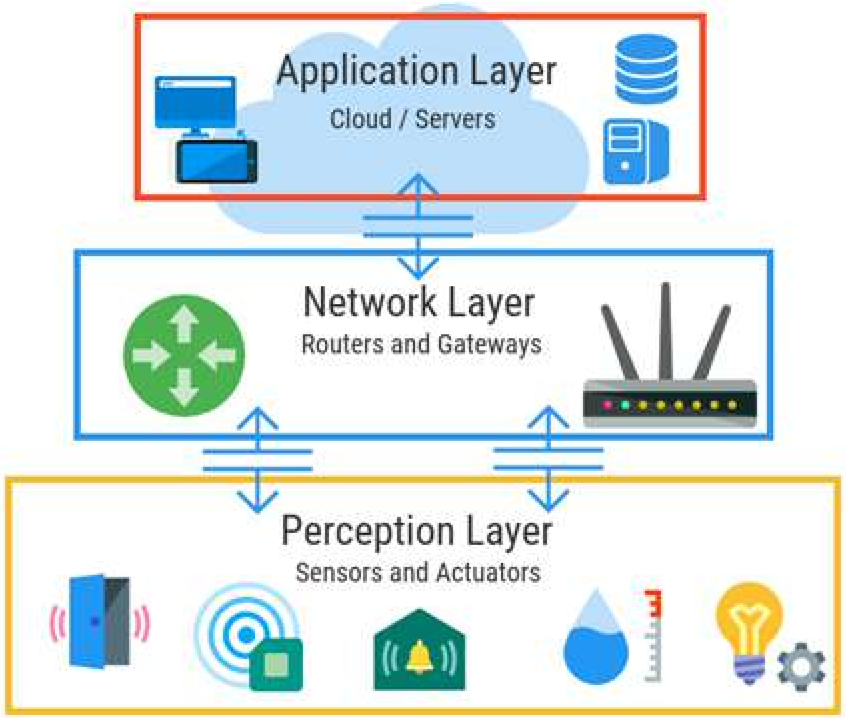
IOT Architecture



Traditional Data Flow in IOT



Basic 3 Layer Architecture



- **Perception layer** is the physical layer, which has sensors for sensing and gathering information about the environment.
- **Network layer** is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.
- **Application layer** is responsible for delivering application specific services to the user.
  - For example, smart homes, smart cities, smart health, etc.

Emergence of Standard IOT Architecture

Basic 3 Layer Architecture However does not address many issues such as Compatibility, Security, Re-usability, Heterogeneity etc which gives a thought that there is no dedicated architecture for IOT as such.

So in past few years, Certain Architectural standards & frameworks have emerged.

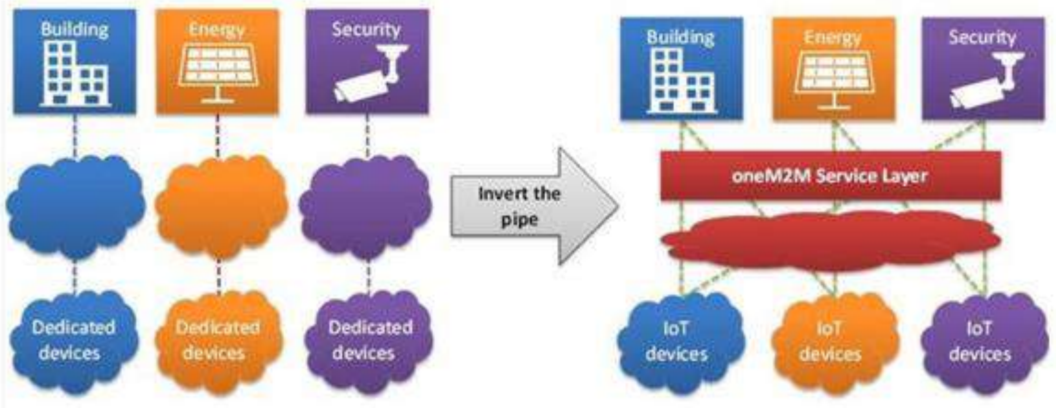
Two Best Known Architecture

- OneM2M Architecture
- IOT World Forum Architecture

oneM2M Architecture

Goal of **oneM2M** architecture:

- to create a common services layer, which can be readily embedded in **field devices** to allow communication with application servers.

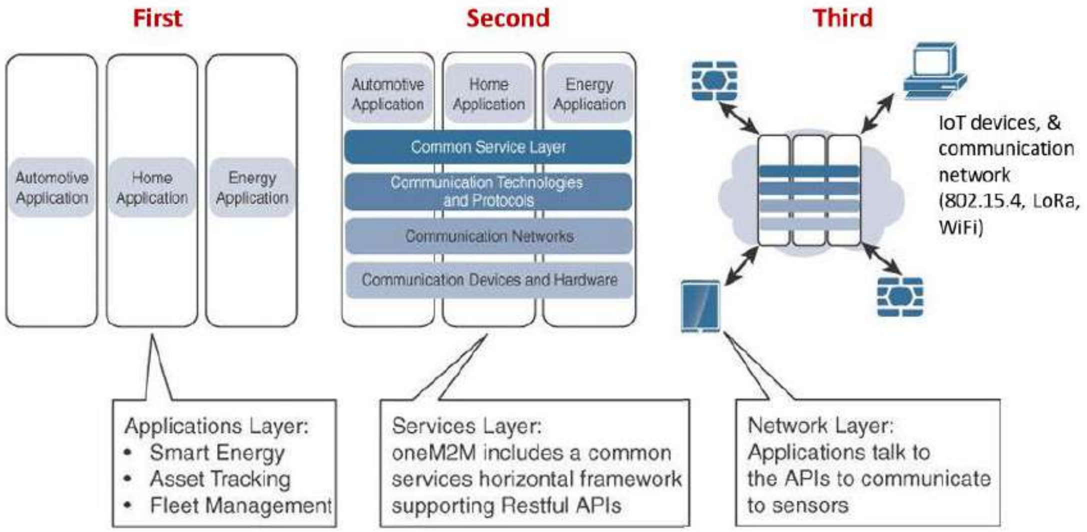


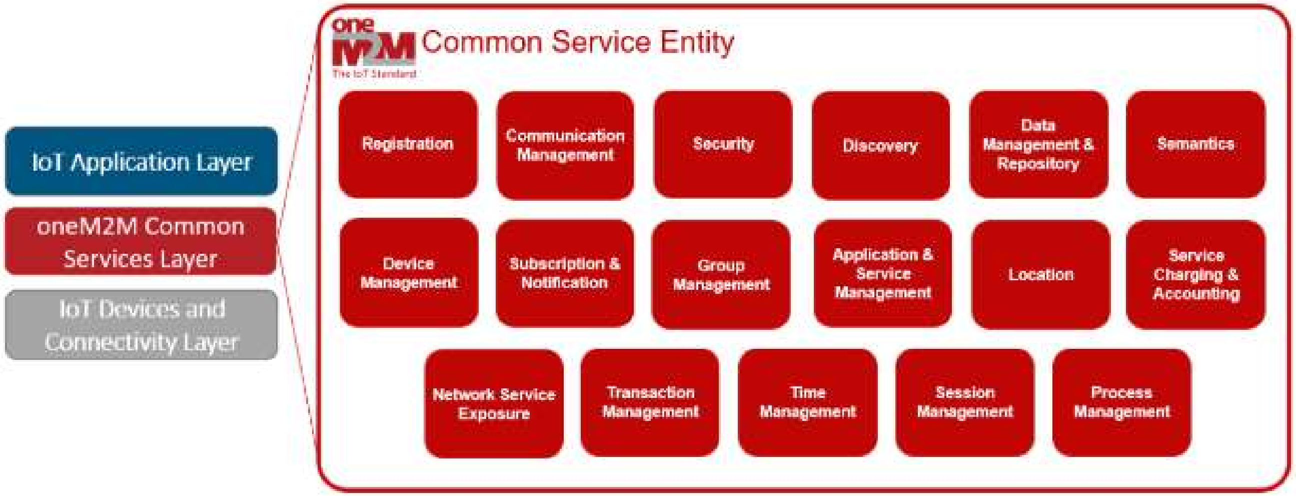
Challenges in IoT Architecture:

- heterogeneity of devices,
- heterogeneity of software,
- Heterogeneity of access methods

- Using the smart building use case, a security application can detect when nobody is in the building.
- It could then trigger lights to be switched off and for the HVAC system to operate on a reduced setting.

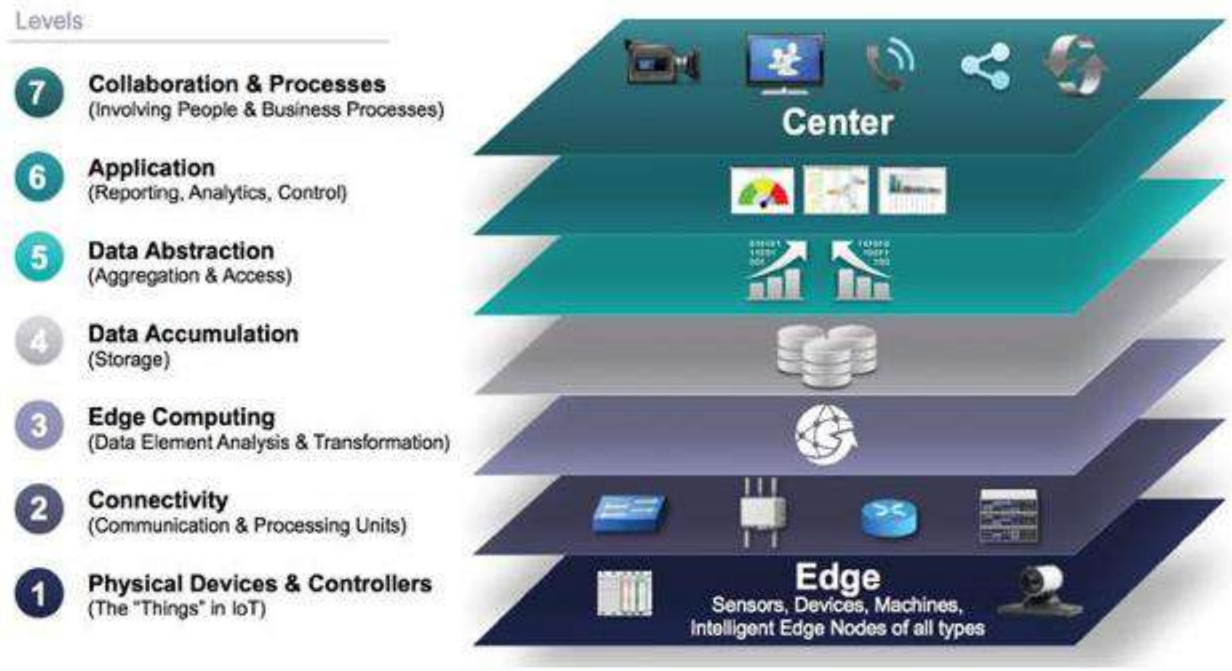
oneM2M Architecture





- Attempts to standardize **Northbound API** commonly used in Software Defined Networking.
- A northbound interface is an application programming interface that allows a lower-level network component to communicate with a higher-level or more central component.
- In SDN, the operator or orchestration software does not directly issue commands or configurations to the network nodes. Instead, the operator uses the application layer to issue commands to the control layer over the northbound interface.
- A RESTful API uses HTTP requests to GET, PUT, POST and DELETE data.

IoTWFArchitecture – 7 Layer Stack



- The IoT World Forum (IoTWF) Standardised Architecture is a set of rules that enable those who deal with the Internet of Things (IoT) to accomplish their jobs better.

- These recommendations were developed in 2014 by a consortium of large corporations, including Cisco and IBM.

- **Accomplishment with IOTWF Model**

-We can examine the many technologies employed at each phase and their interaction. It's just like knowing the ingredients needed for each part of a recipe.

-We may create our IoT system using components from several vendors. It's like designing a car with one company's engine and another's tires.

We can divide the complex IoT challenge into smaller, more manageable components. It's similar to slicing a large pizza into slices to make it easier to consume.

Layer 1 &2

Layer 1: Physical Devices and Controllers Layer

- home of the “things” in IoT
- “things” can be from a microscopic sensors to giant machines in a factory
- primary function is generating data
- capable of being queried and/or controlled over a network.

Layer 2: Connectivity Layer

- focus is on connectivity

② **Connectivity**
(Communication and Processing Units)

Layer 2 Functions:

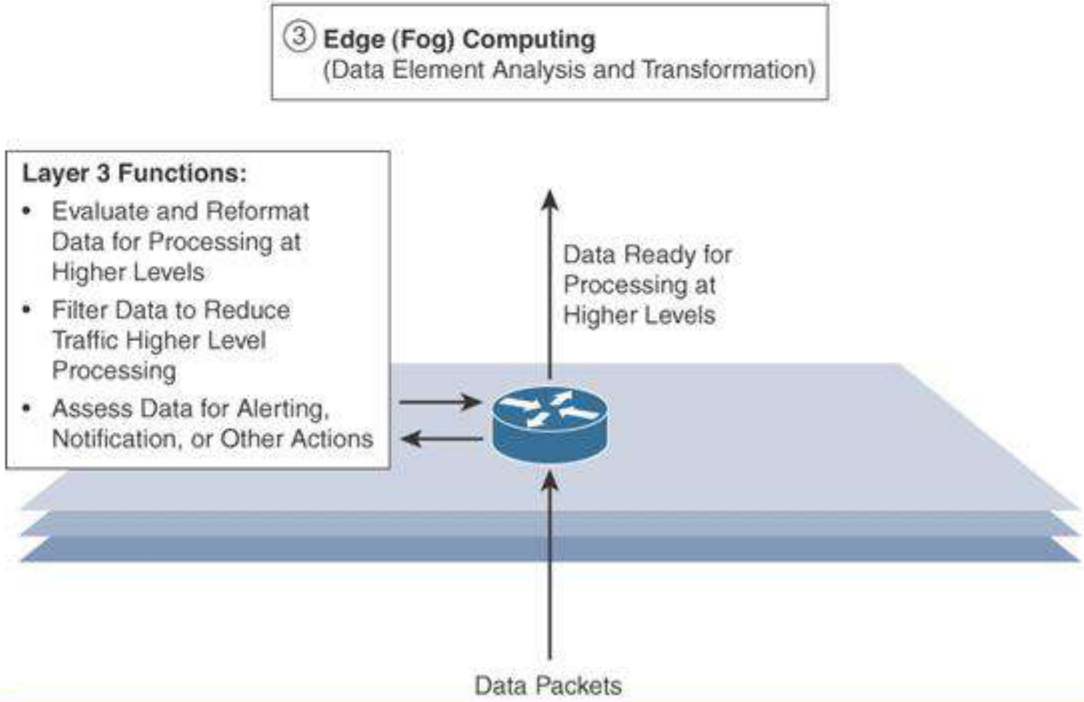
- Communications Between Layer 1 Devices
- Reliable Delivery of Information Across the Network
- Switching and Routing
- Translation Between Protocols
- Network Level Security

Layer 3: Edge Computing Layer

- often referred to as the "fog" layer
- emphasis is on
  - Data reduction by filtering and cleaning up
  - Reformatting and compressing data
  - Initial processing of data (e.g. alert generation, data validation, etc)

Basic principle:

information processing is initiated as early and as close to the edge of the network as possible.



Upper Layers: Layers 4-7

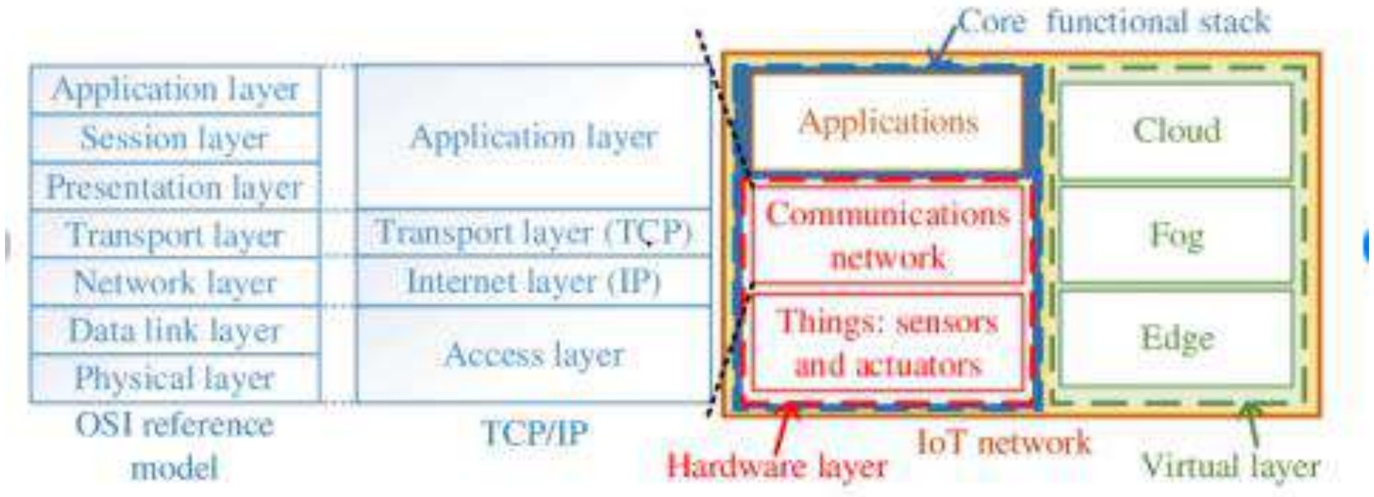
Layers	Functions
Layer 4 : Data Accumulation	IoT systems create large amounts of data, and this layer acts as a data storage warehouse. It is necessary since this layer stores incoming data and prepares data for future processing. Once the data is ready, it is sent to the next levels for analysis and decision-making
Layer 5: Data Abstraction	We're finally making sense of the data. We collect similar data from a variety of sources, prioritise critical information, and prepare data for a variety of applications.
Layer 6: Application Layer	Interpret data using Software Applications. Based on Data Analysis Application will Monitor, Control & provide report of the data.
Layer 7: Collaboration & Processes	Finally, this layer integrates everything. It is the point at which individuals engage with the IoT system. Data and apps are used to make choices, optimize operations, and generate value. This layer connects technology to real-world advantages such as enhancing businesses or improving our lives.

Simplified IoT Architecture

- It highlights the fundamental building blocks that are common to most IoT systems and which is intended to help in designing an IoT network.
- IoT architectural framework is presented as two parallel stacks

-> Core IoT Functional Stack

- >IoT Data Management and Compute Stack (Virtual Layer)



Simplified IoT Architecture along with the OSI reference model and TCP/IP layers.

Core IOT Functional Stack- Layer 1
Things: Sensors & Actuators Layer

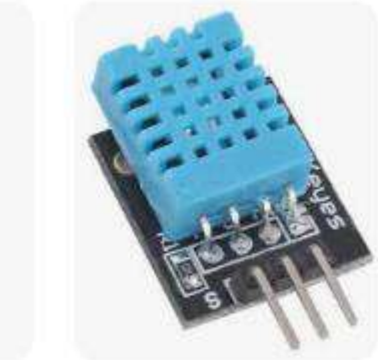
- Battery Powered or Power connected
- Mobile or Static
- Low or High reporting frequency
- Simple or Rich Data
- Report Range
- Object density per cell.

Viscosity sensor

Location sensor

Rust Sensor

Motion Sensor

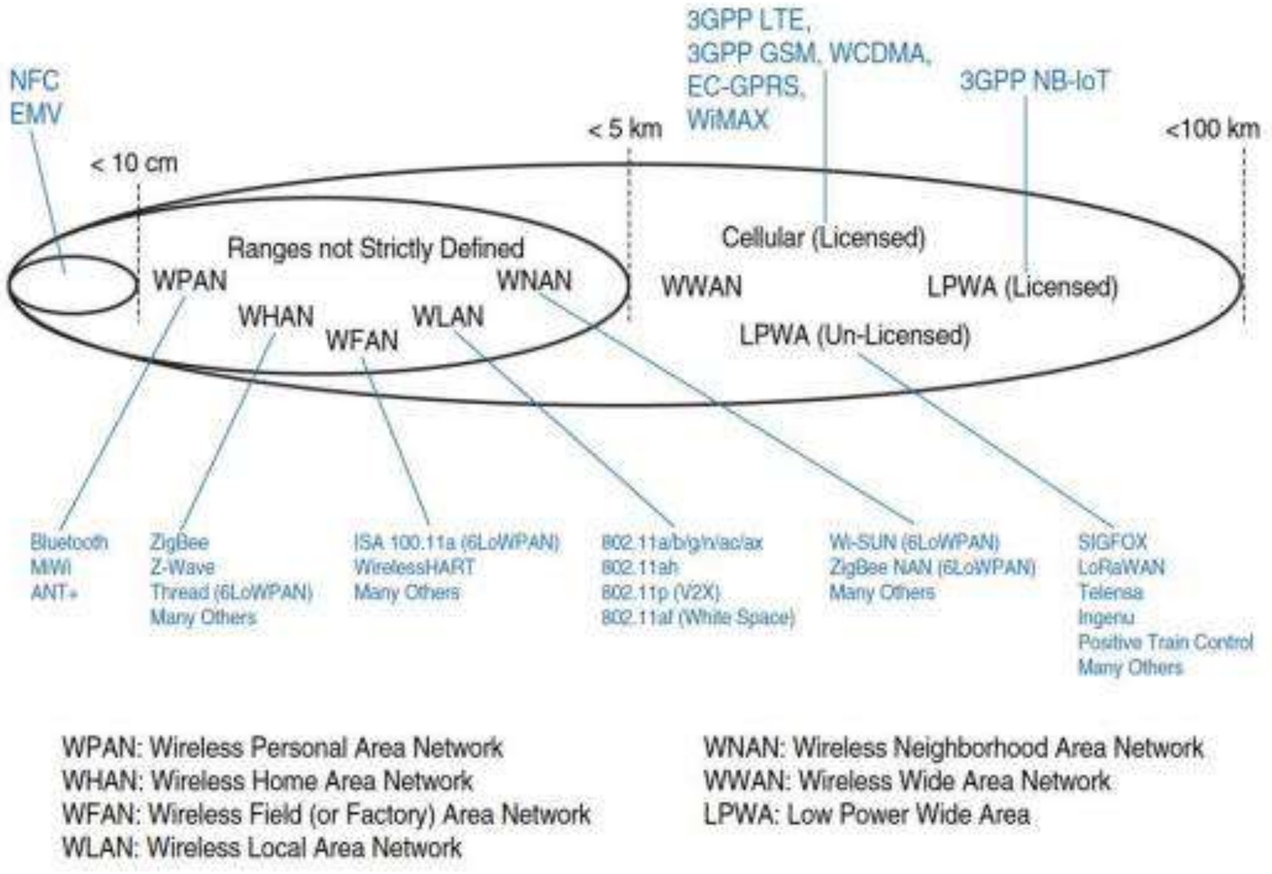


Temperature & Humidity Sensor

Gravity Sensor

Vibration Sensor

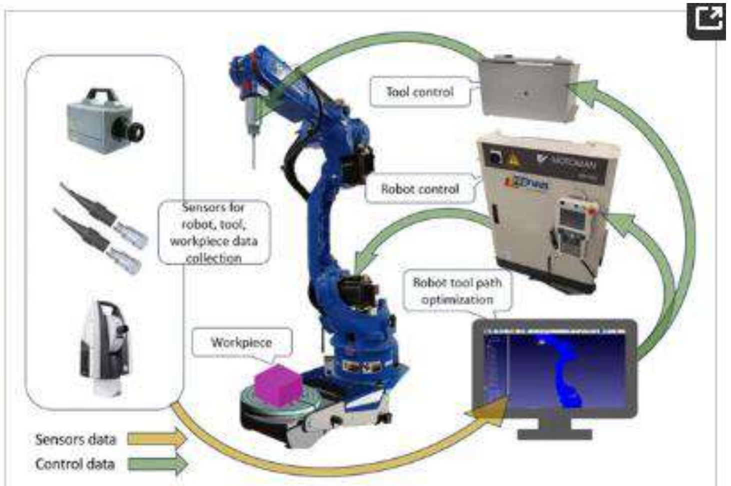
Core IOT Functional Stack- Layer 2 Communications Network Layer



Core IOT Functional Stack- Layer 3 Application & Analytics Layer

Monitoring & Data logging

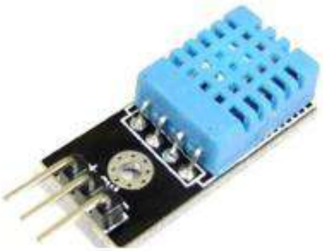
Water Flow control



“Things” in IoT– Sensors

MQ135 - Air Quality Gas Sensor

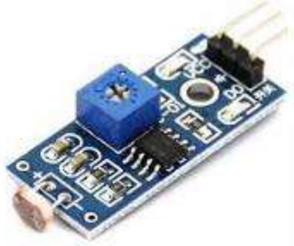
Sound Detection Sensor



DHT11 - Temperature and Humidity Sensor

PIR Motion Detector Sensor

Pulse Sensor



LDR Light Sensor

Ultrasonic Distance Sensor

IR Sensor

“Things” in IoT– Actuators

4 Channel 5V Relay

Servo Motor

DC Motor

Solenoid valve

Linear Actuators

LED

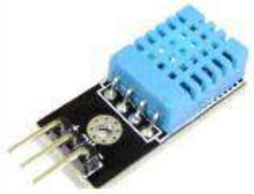
LCD Diplay

The "Things"

- Sensors & Actuators are the fundamental building blocks of IoT
  - Sensor senses
  - Actuator acts

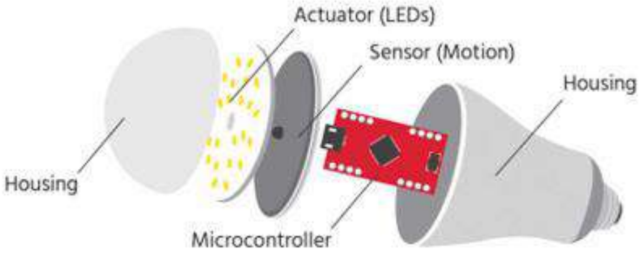
- Smart objects are any physical objects that contain
  - Embedded technology
    - Microcontroller unit, memory storage, power supply, communication ports, input and output, timer or counter
  - Sensors and/or actuators

- Smart objects are to sense and/or interact with their environment in a meaningful way
  - being interconnected, and
  - enabling communication among themselves or with external agent.



Sensor

Actuator



Smart Object

Sensors

- It **measures some physical quantity** and converts that measurement into analog/digital form

- There are a number of ways to group and cluster sensors into different categories

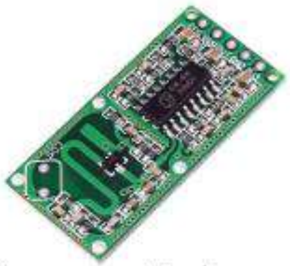
  - Based on external energy requirement
    - Active / Passive
  - Based on placement location
    - Invasive / Non-invasive
  - Based on distance from the sensing object
    - Contact / No-contact
  - Based on application industry
    - Medical / Manufacturing / Agriculture / etc.
  - Based on measuring scale
    - Absolute / Relative
  - Based on sensing mechanism
    - Thermoelectric / Electromechanical / Piezo resistive / Optic / Electric / Fluid mechanics / Photoelastic / etc.
  - Based on sensing parameter
    - Position / Occupancy / Motion / Velocity / Force / Pressure / Flow / Humidity / Light / Temperature / Acoustic / Radiation / Chemical / Biosensors / etc.

Sensor Types

Sensor Type	Description	Example
Position	• Measures the position of an object • Position could be absolute/relative • Position sensor could be linear, angular, or multi-axis	• Proximity sensor • Potentiometer • Inclinometer
Occupancy	• Detects the presence of people and animals in a surveillance area • Generates signal even when a person is stationary	• Radar Sensor
Motion	• Detects the movement of people and objects	• Passive Infrared (PIR) Sensor

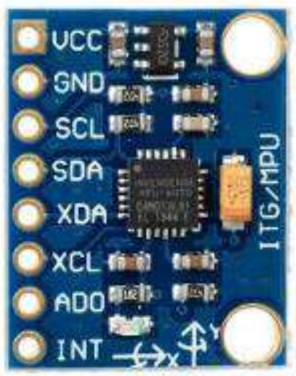

Ultrasonic Proximity Sensor


Infrared Proximity Sensor


Microwave Radar Sensor


PIR Motion Sensor

Sensor Type	Description	Example
Velocity and Acceleration	• Velocity sensor measures how fast an object moves • Acceleration sensor measures the changes in velocity	• Gyroscope • Accelerometer
Force	• Detects whether a physical force is applied and the magnitude of the force	• Tactile sensor • Viscometer
Pressure	• Measuring the force applied by liquids or gases • It is measured as force per unit area	• Barometer • Piezometer



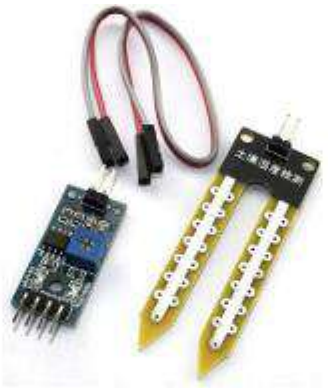
Gyroscope

Capacitive Touch Sensor

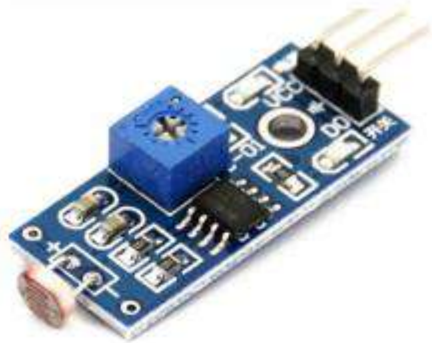
Barometric Pressure Sensor

Sensor Type	Description	Example
Flow	• Detects the rate of fluid flow through a system in given period of time	• Water meter • Anemometer
Humidity	• Detects amount of water vapour in the air • Can be measured in absolute/relative scale	• Hygrometer • Soil moisture sensor
Light	• Detects the presence of light	• LDR light sensor • Photodetector • Flame Sensor

Water meter



Soil moisture sensor

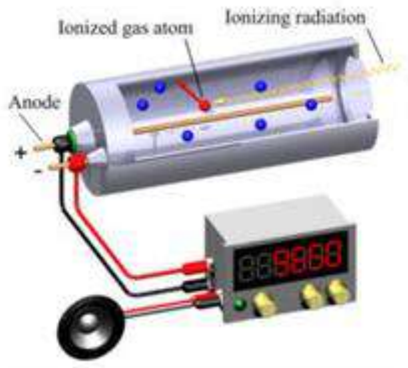


LDR light sensor

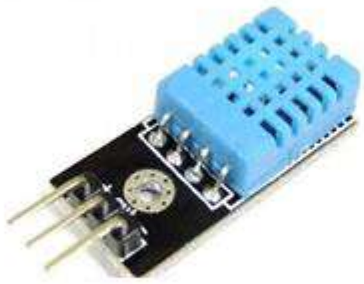
Flame sensor

Sensor Type	Description	Example
Radiation	• Detects the radiation in the environment	• Neutron detector • Geiger-Muller counter
Temperature	• Measures the amount of heat or cold present in the system • Two type: contact / non-contact	• Thermometer • Temperature gauge • Calorimeter

Neutron detector



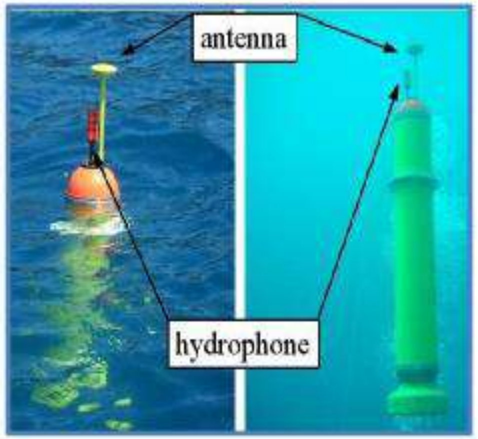
Geiger-Muller counter



Temperature Sensor

Thermo-Hygrometer

Sensor Type	Description	Example
Acoustic	• Measures sound level	• Microphone • Hydrophone
Chemical	• Measures the concentration of a chemical (e.g. CO_2) in a system	• Smoke detector • Breathalyzer
Biosensor	• Detects various biological elements, such as organisms, tissues, cells, enzymes, antibodies, nucleic acid, etc.	• Pulse oximeter • Electrocardiograph (ECG) • Blood glucose biosensor

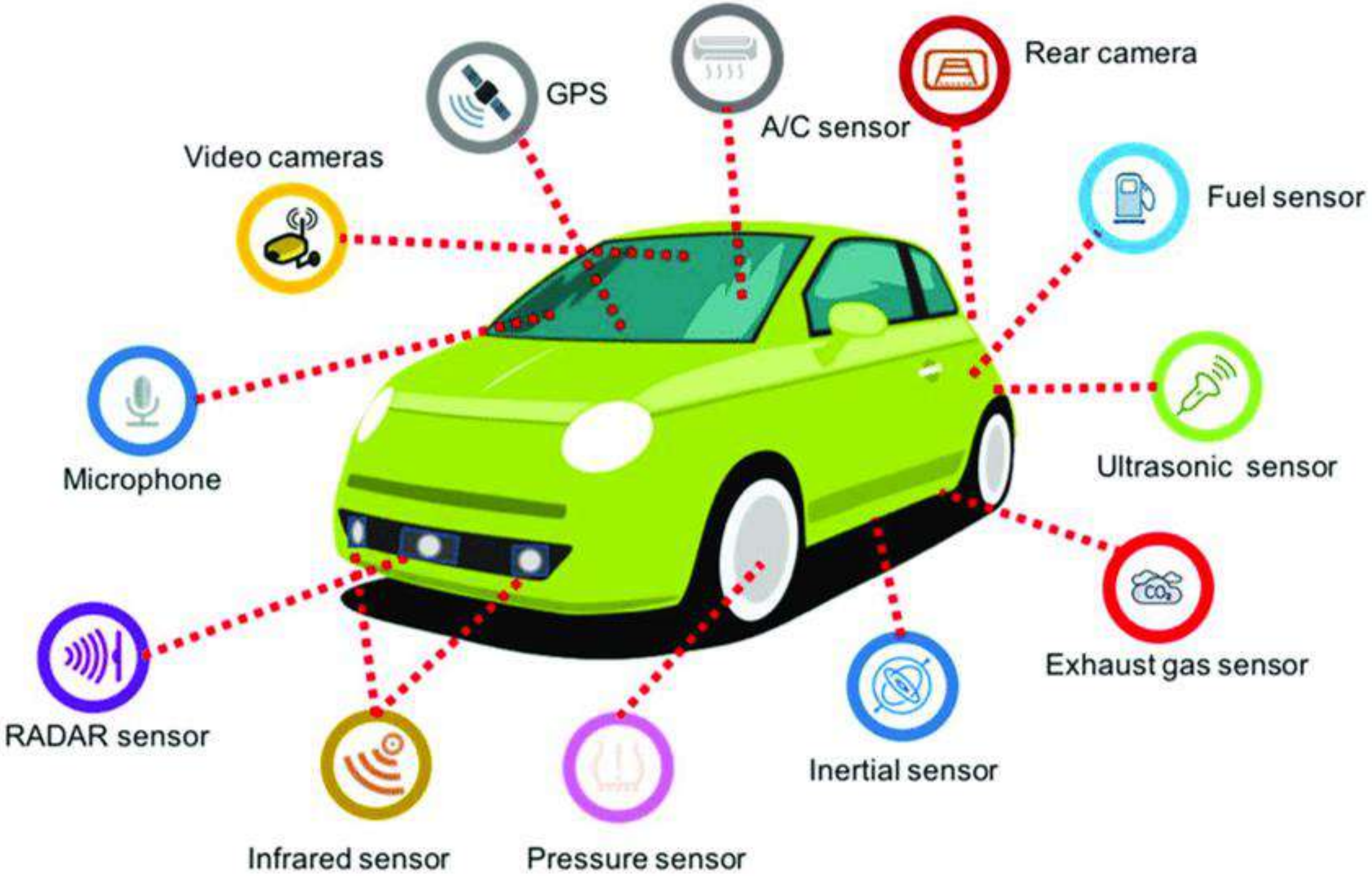


Hydrophone

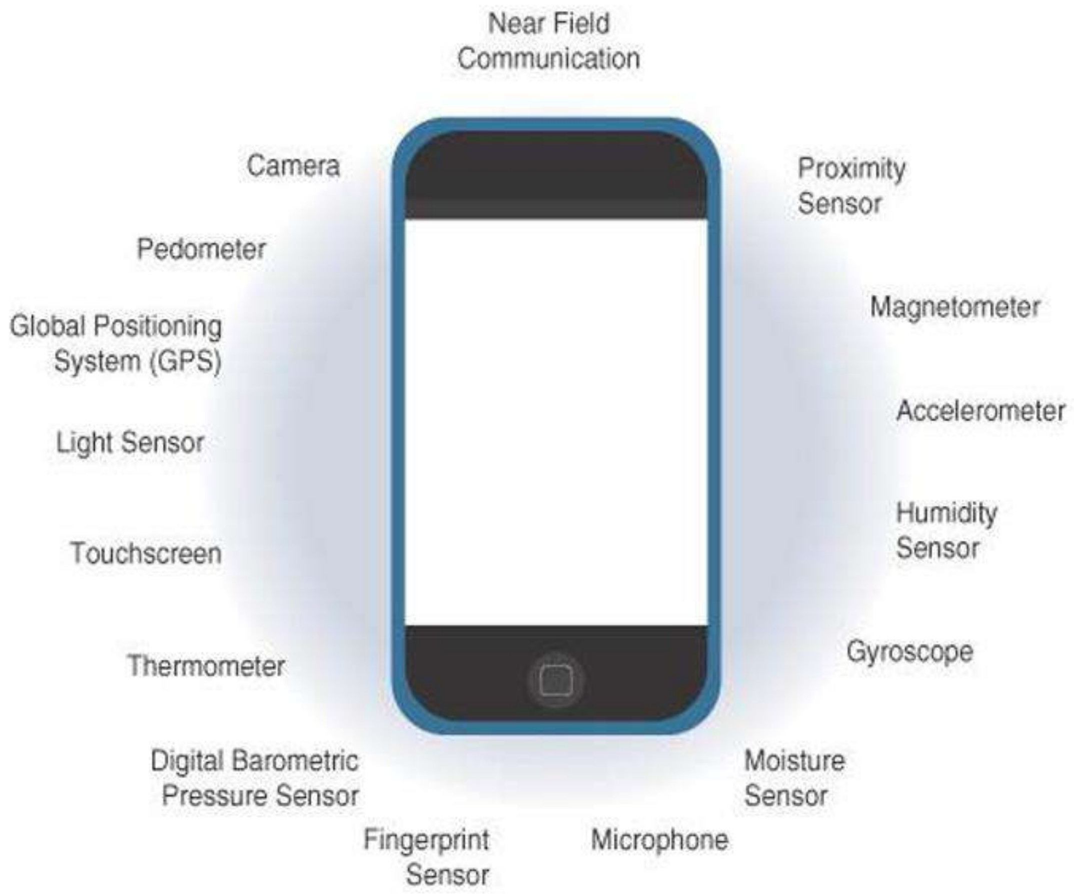
Breathalyzer

Pulse oximeter

Sensors in Smart Car

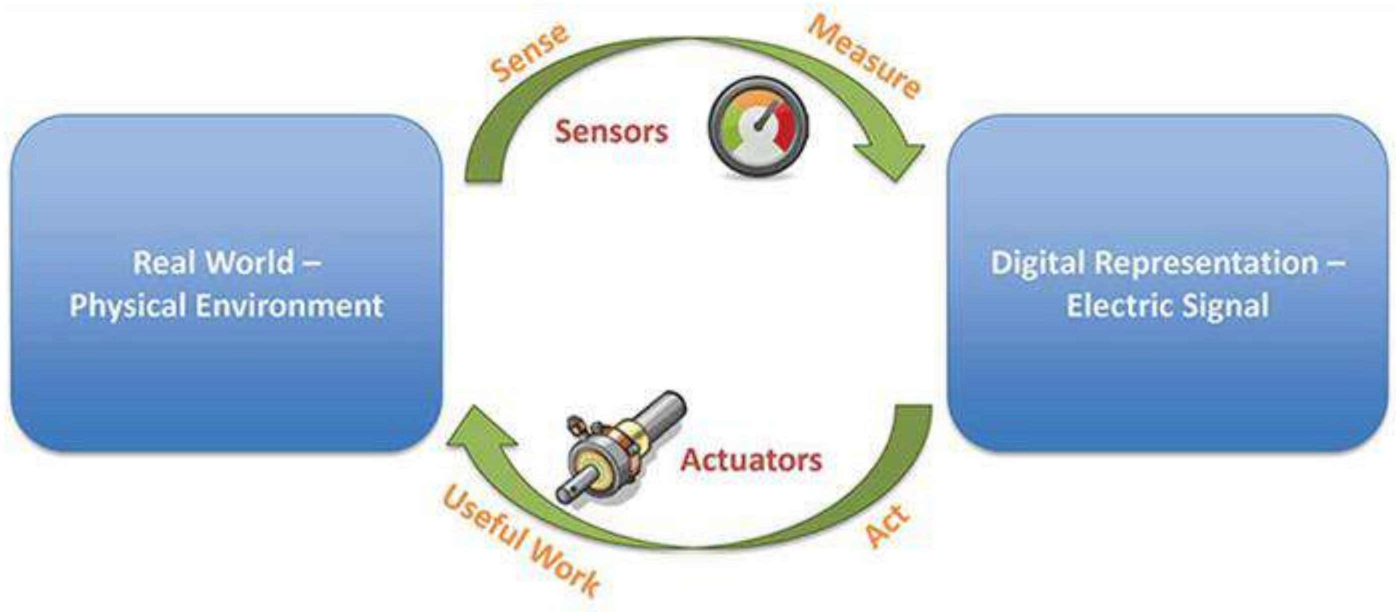


Sensors in a Smartphone



Actuators

- Sensors are designed to sense and measure the surrounding environment.
- Actuators receive some type of control signal (commonly an electrical signal or digital command) that triggers a physical effect, usually some type of motion, force etc.



Access Technologies in IoT

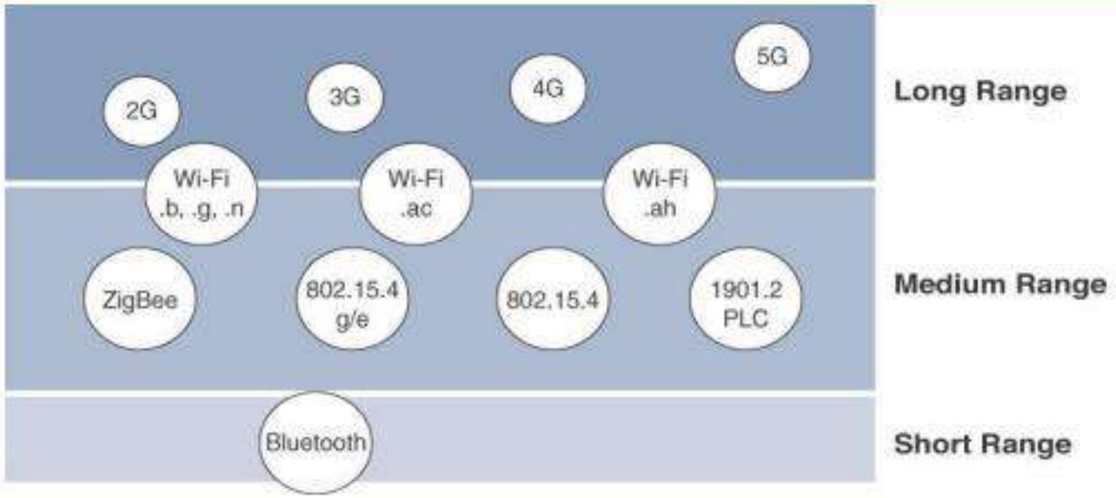
Communication Criteria

- Range
- Frequency Bands
- Power Consumption
- Topology
- Constrained Devices
- Constrained-Node Networks

IoT Access Technologies

LoRaWAN
ZigBee
Sub-1GHz
6LoWPAN
Bluetooth
sigfox
NB-IoT
NFC
ZWAVE
WiFi
THREAD
nwave
5G

Range



Short range: – 0-10 m
Connectivity:- Often considered as an alternative to serial cable

Medium range – 10-100 meters between two devices

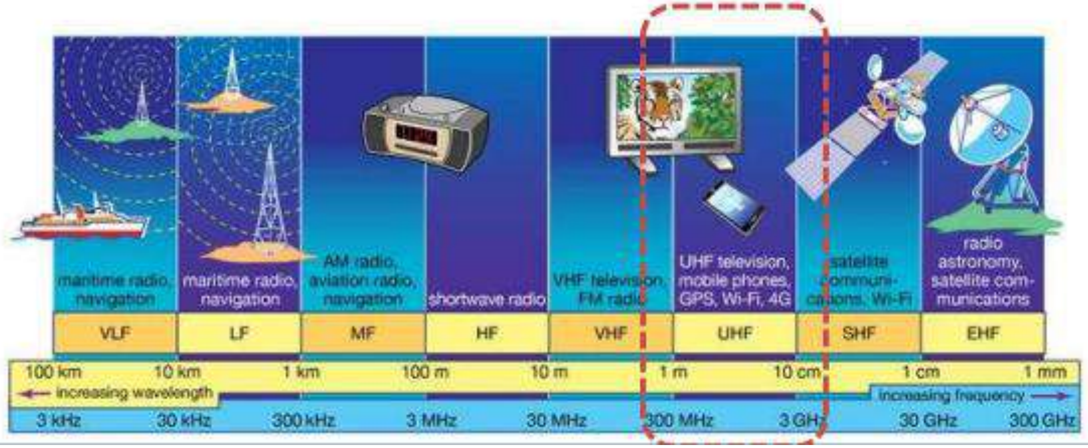
Wireless:- Wifi, WPAN
Wired :-
- IEEE 802.3 Ethernet,
- IEEE 1901.2 Narrowband Power Line Communications (PLC)

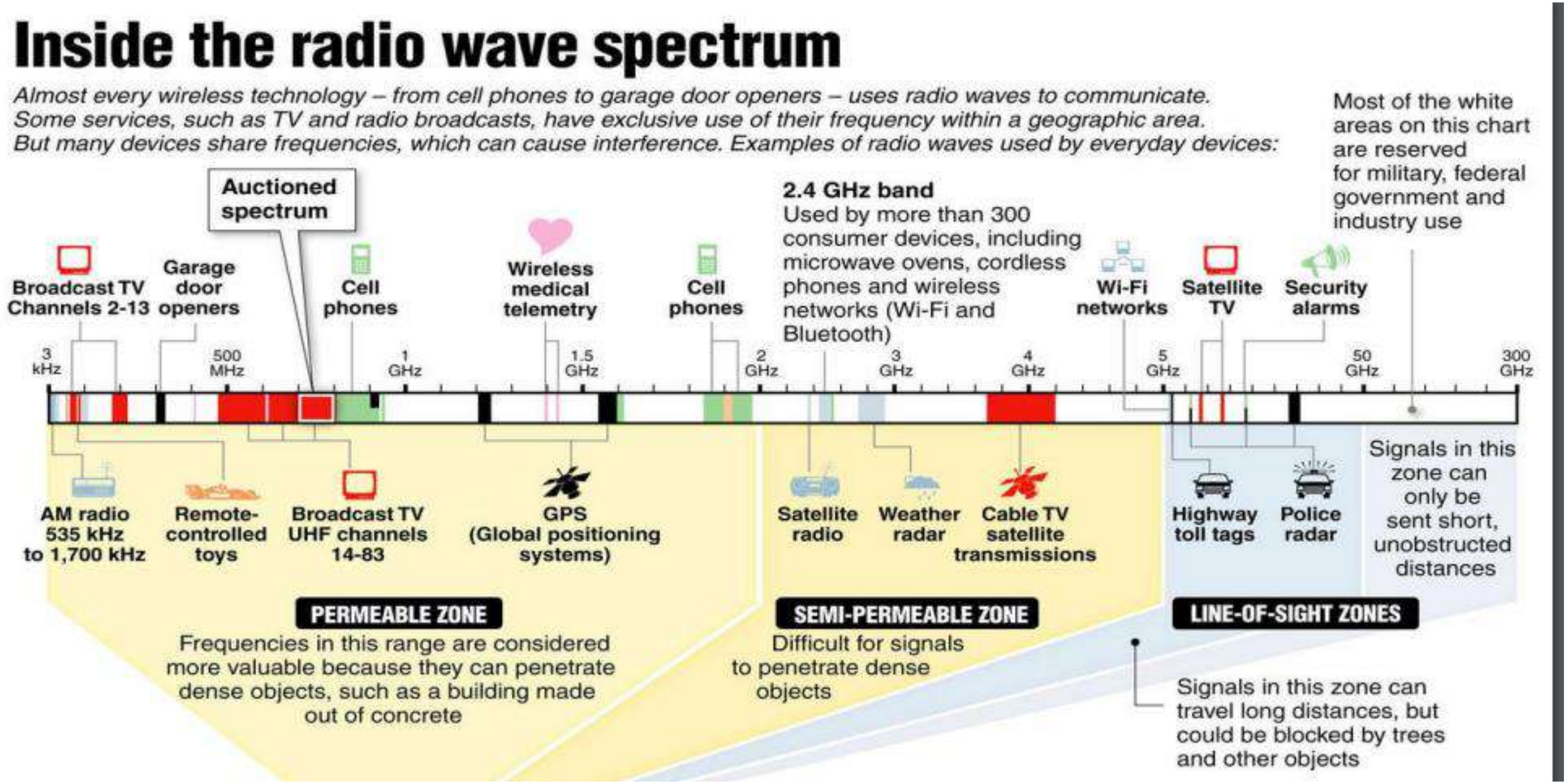
Long range – Greater than 1 mile (1.6 km) between two devices
– Wireless : • 2G, 3G, 4G,LPWAN
– Wired :
- IEEE 802.3 ethernet over optical fiber,
- IEEE 1901.2 Broadband PLC

Frequency Bands

- Radio spectrum is regulated by countries and/or organizations
  - e.g. International Telecommunication Union (ITU), Federal Communications Commission (FCC), Telecom Regulatory Authority of India (TRAI)
- Frequency bands leveraged by wireless communications are split between:

1. **Licensed**
   - applicable to long-range access technologies
   - users must subscribe to services
   - common licensed spectrum for IoT :
     - Cellular (900-2100 MHz),
     - NB-IoT (700-900 MHz)
2. **Unlicensed**
   - *Unlicensed* means that no guarantees or interference protections are offered
   - industrial, scientific, and medical (ISM) portions of the radio bands
   - well-known ISM bands for IoT :
     - 2.4 GHz, 5 GHz, 915 MHz for WiFi, BLE, ZigBee;
     - 868 MHz for LoRa




Inside the radio wave spectrum
Almost every wireless technology – from cell phones to garage door openers – uses radio waves to communicate. Some services, such as TV and radio broadcasts, have exclusive use of their frequency within a geographic area. But many devices share frequencies, which can cause interference. Examples of radio waves used by everyday devices:
Most of the white areas on this chart are reserved for military, federal government and industry use
Auctioned spectrum
2.4 GHz band
Used by more than 300 consumer devices, including microwave ovens, cordless phones and wireless networks (Wi-Fi and Bluetooth)
Broadcast TV Channels 2-13
Garage door openers
Cell phones
Wireless medical telemetry
Cell phones
Wi-Fi networks
Satellite TV
Security alarms
3 kHz
500 MHz
1 GHz
1.5 GHz
2 GHz
3 GHz
4 GHz
5 GHz
50 GHz
300 GHz
AM radio 535 kHz to 1,700 kHz
Remote-controlled toys
Broadcast TV UHF channels 14-83
GPS (Global positioning systems)
Satellite radio
Weather radar
Cable TV satellite transmissions
Highway toll tags
Police radar
Signals in this zone can only be sent short, unobstructed distances
PERMEABLE ZONE
Frequencies in this range are considered more valuable because they can penetrate dense objects, such as a building made out of concrete
SEMI-PERMEABLE ZONE
Difficult for signals to penetrate dense objects
LINE-OF-SIGHT ZONES
Signals in this zone can travel long distances, but could be blocked by trees and other objects

ISM Bands in India

ISM Bands - Industrial, Scientific and Medical

900MHz vs. 2.4GHz vs. 5GHz

900MHz

Advantages:
- More robust, less prone to interference
- Lower attenuation, travels further through more obstacles

Disadvantages:
- Low bandwidth prevents large data transfer, speed
- Components are larger at lower frequencies

2.4GHz

Advantages:
- Higher bandwidth allows large data transfer, speed
- Components are smaller, cheaper

Disadvantages:
- Congested band due to abundance of Wi-Fi, Bluetooth, microwaves, cordless phones
- Attenuates much more quickly, will not pass through metal

5GHz

Advantages:
- Higher bandwidth allows large data transfer, speed
- Less congested, few RF devices in this band

Disadvantages:
- Low transmit power limitations
- High attenuation in cables, requires very high gain antennas

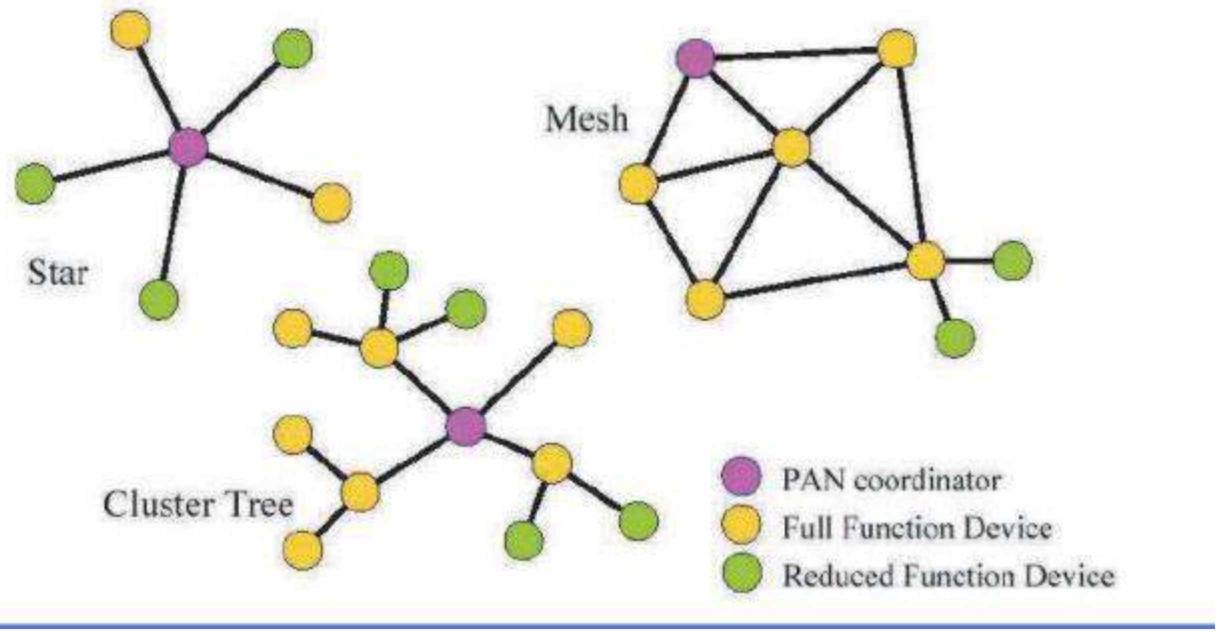
Topology

Three main topology schemes are dominant: –

star, mesh, and peer-to-peer (cluster tree)

• For long-range and short-range technologies: – star topology is prevalent

• For medium-range technologies: – star, peer-to-peer, or mesh topology is common



Constrained Devices

- RFC 7228 defines three classes for constrained nodes: Class 0, 1, 2

	RAM	Flash Storage	IP stack	Security Scheme	Example
Class 0	< 10 KB	< 100 KB	Not present	No	Push button
Class 1	> 10 KB	> 100 KB	Optimized IP stack	Light	Sensors
Class 2	> 50 KB	> 250 KB	Full IP stack	Yes	Smart meter

Constrained Networks

Constrained-node networks are often referred to as low-power and lossy networks (LLNs).

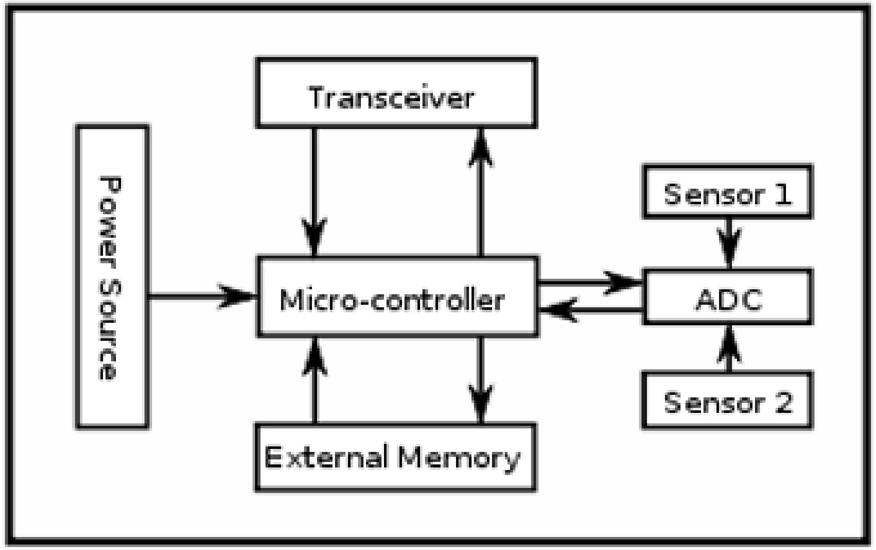
Layer 1 and Layer 2 protocols must be evaluated in using the following characteristics:
– data rate and throughput
– latency and determinism
– overhead and payload.

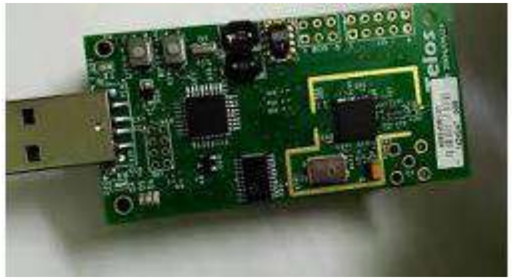
- Data rate & throughput:
  - data rates available from 100 bps to tens of Mbps
  - actual throughput is less, sometimes much less, than the data rate
- Latency & determinism:
  - When latency is a strong concern, emergent access technologies such as Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e should be considered.
- Overhead & Payload
  - The minimum IPv6 MTU size is expected to be **1280 bytes**.
  - MTU size for IEEE 802.15.4 is **127 bytes**; payload in LoRaWAN may **be from 19 to 250 bytes**
  - So, the fragmentation of the IPv6 payload has to be performed by the link layer

Comparison of Key Attributes

	WiFi	BLE	Thread	Sub-GHz: TI	Sigfox	Zigbee	LoRa
Max. Data throughput	72 Mbps	2 Mbps	250 Kbps	200 Kbps	100 bps	250 Kbps	50 Kbps
Range	100 m	750 m	100 m	4 km	25 km	130 m	10 km
Topology	Star	P2P/ Mesh	Mesh/ Star	Star	Star	Mesh/ Star	Star of Star
Frequency	2.4 GHz	2.4 GHz	2.4 GHz	Sub-GHz	Sub-GHz	2.4 GHz	Sub-1GHz
Power consumption	1 Year (AA battery)	Up to years on a coin-cell battery for limited range					Few Years (AA battery)
IP at the device node	Yes	No	Yes	No	No	No	No
Deployed Devices	AP	smart phones	No	No	No	No	No

Smart Objects



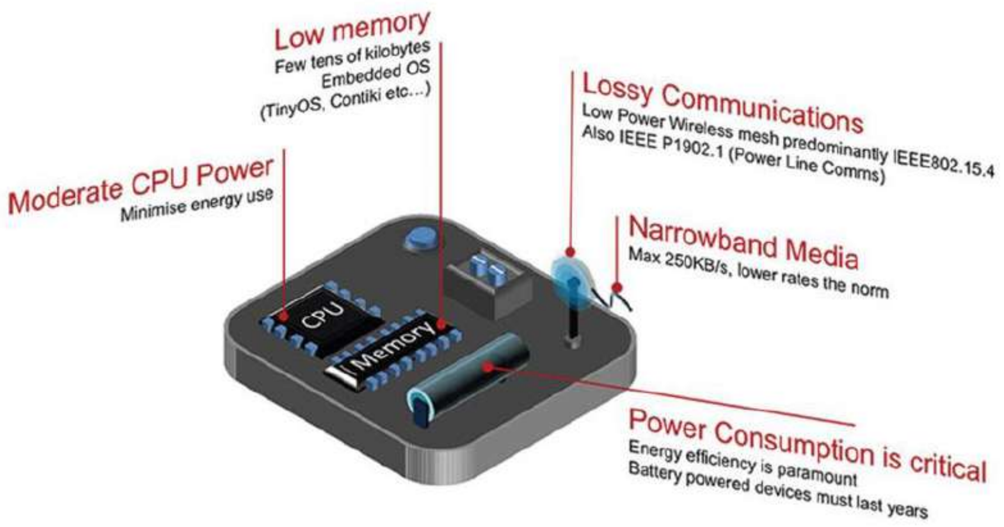


Smart object has the following five characteristics:

- 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

Trends in Smart Object

- Size is decreasing
- Power consumption is decreasing
- Processing power is increasing
- Communication capabilities are improving
- Communication is being increasingly standardized



Thank You