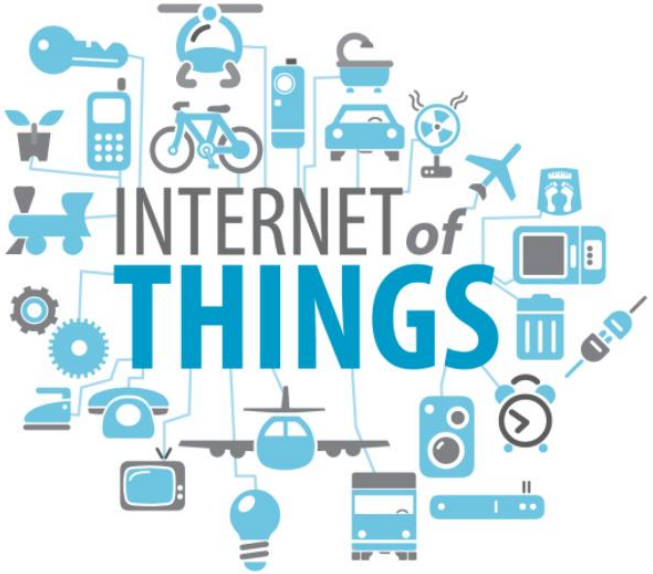
Internet of Things: Protocols and Networks

(CSC2106)

Introduction to IoT

So, what is IoT?

- The Internet of things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet. **(Wikipedia)**
- The Internet of Things (IoT) describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025. **(Oracle)**
- The Internet of Things has become a central and exciting research area encompassing many fields in information and communication technologies and adjacent domains. IoT systems involve interactions with heterogeneous, distributed, and intelligent things, both from the digital and physical worlds including the human in the loop. Thanks to the increasingly wide spectrum of applications and cheap availability of both network connectivity and devices, a number of different stakeholders from industry, academia, society and government are part of the IoT ecosystem. **(IoT Conference 2020)**

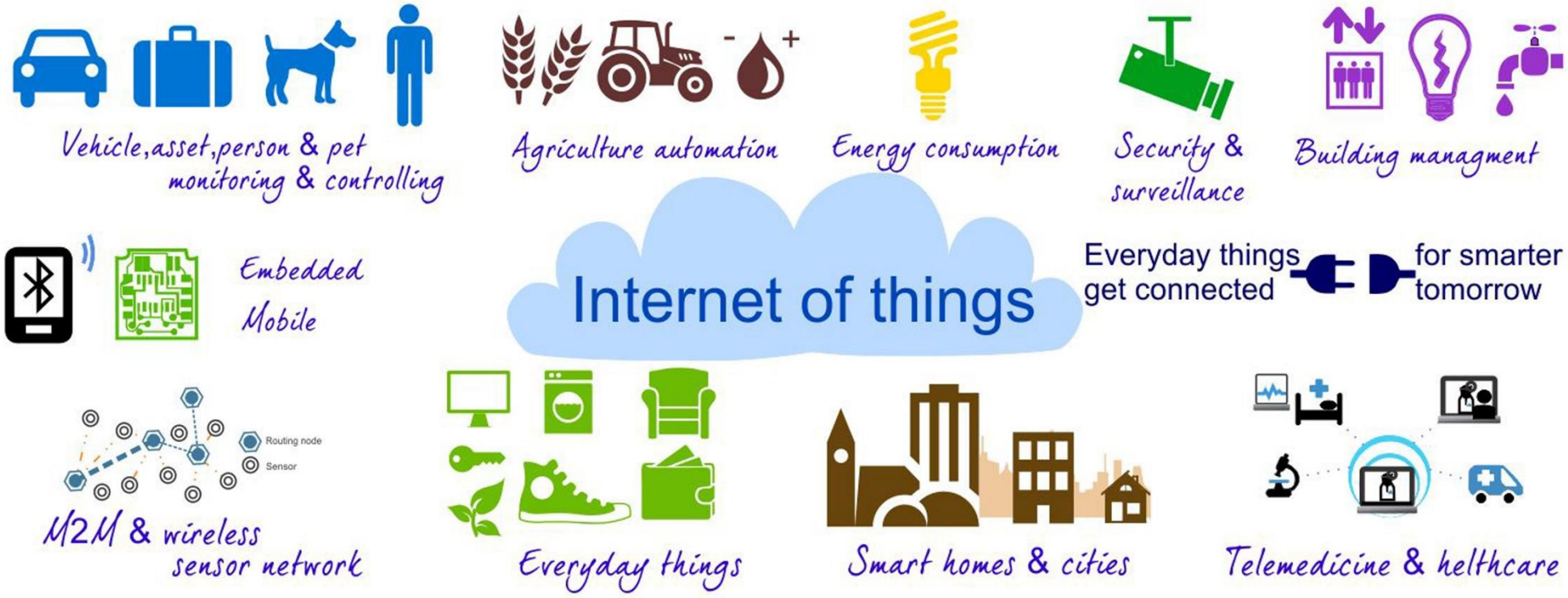


IEEE definition of IoT

"An IoT system is a network of networks where, typically, a massive number of objects, things, sensors or devices are **connected** through communications and information infrastructure to provide value-added services via **intelligent** data processing and management for different **applications** (e.g. smart cities, smart health, smart grid, smart home, smart transportation, and smart shopping)."

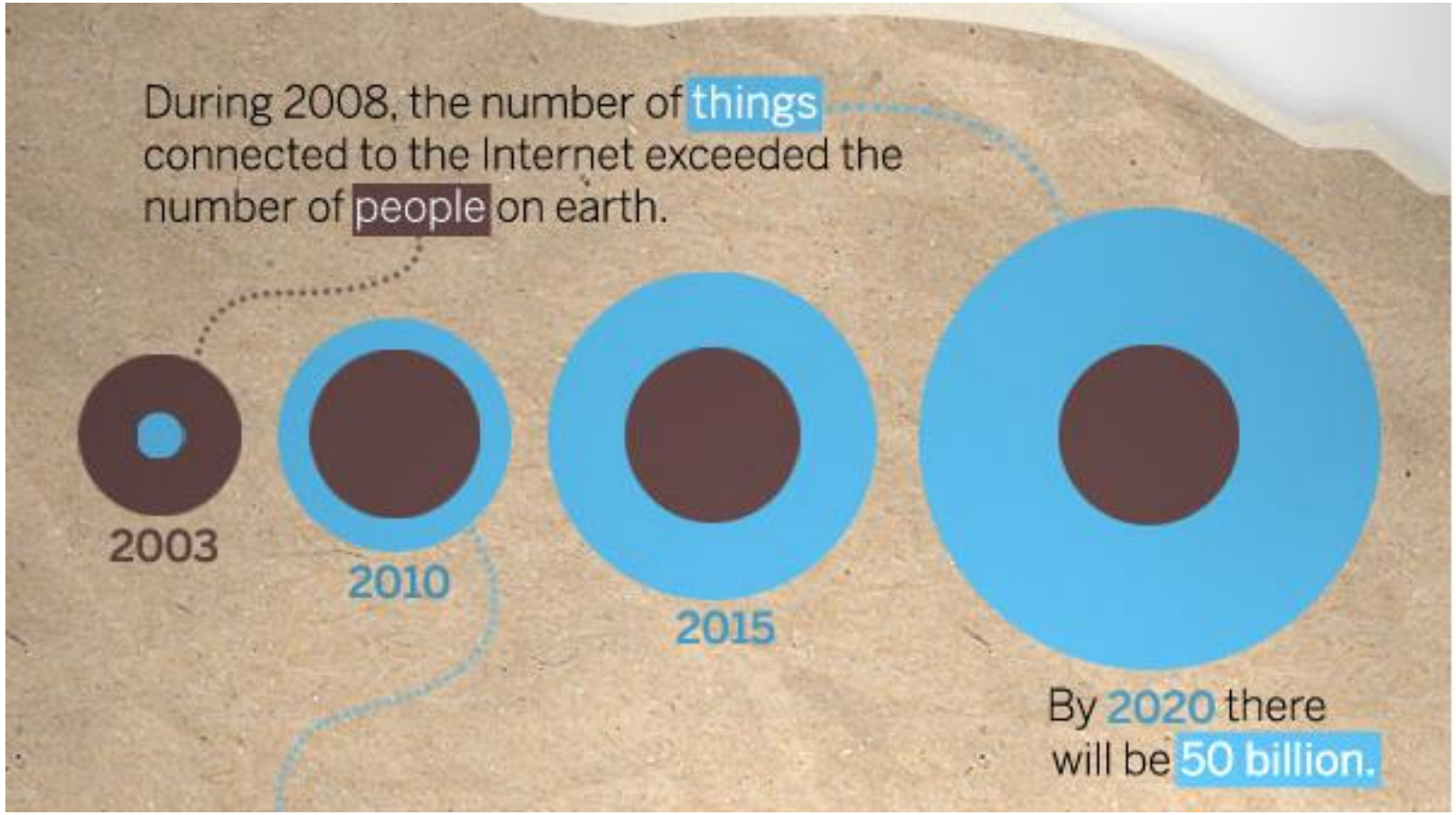
(IEEE Internet of Things Journal)

‘Thing’ in Internet-of-Things (IoT)



[https://inventrom.files.wordpress.com/2014/11/things.jpg]

“Things” connected to the internet



Sources: Cisco IBSG, Jim Cicconi, AT&T , Steve Leibson, Computer History Museum, CNN, University of Michigan, Fraunhofer

Source: CISCO

Internet-of-Things (IoT): Components

Physical object (“thing”)

+

Controller (“brain”)

+

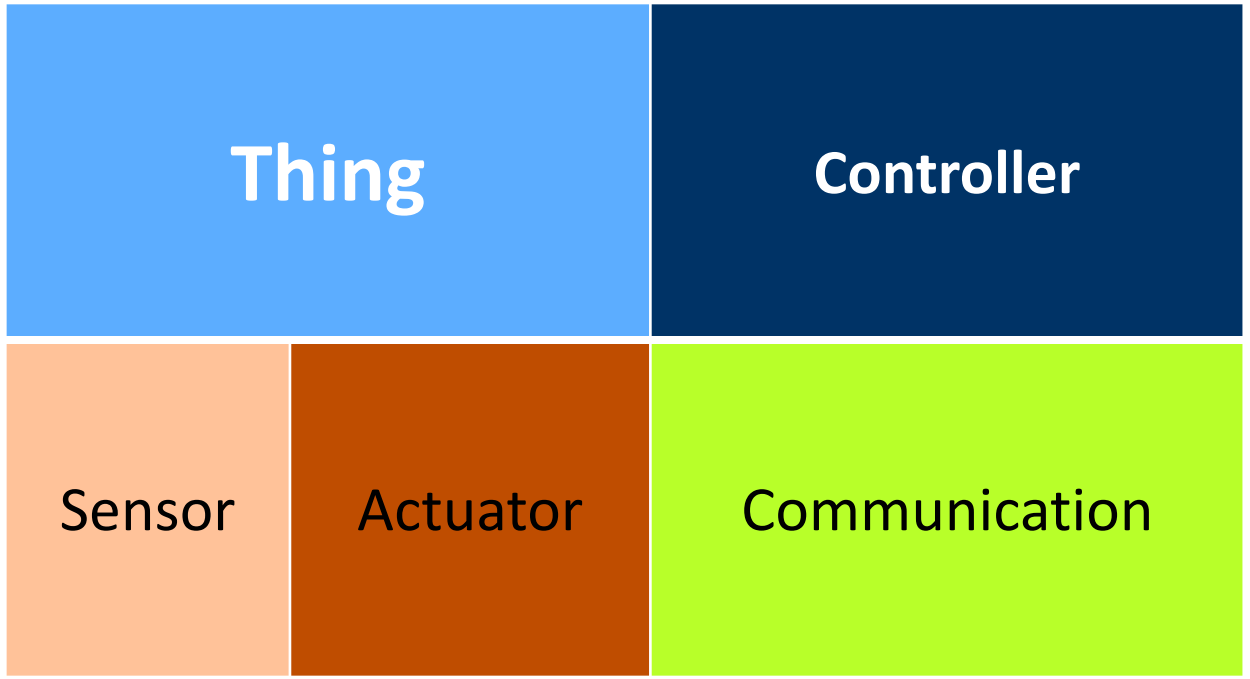
Sensors

+

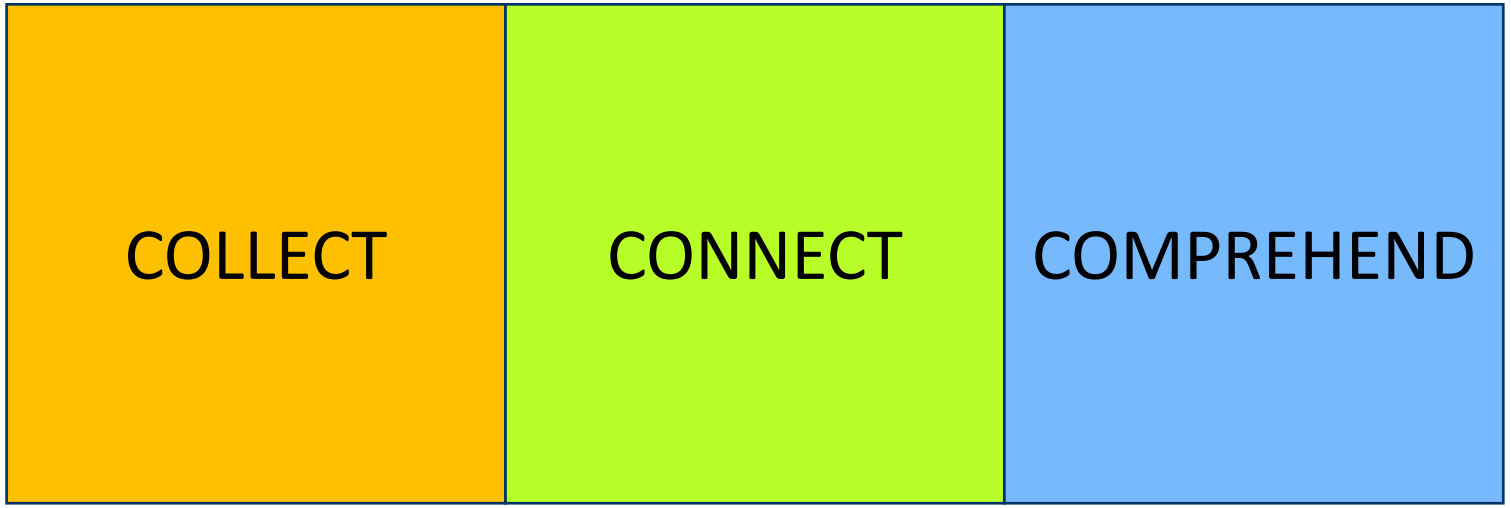
Actuators

+

Networks (Internet)



Internet-of-Things (IoT): Another Perspective



Data vs. Knowledge

"The ultimate goal is transforming the raw data to insights and actionable knowledge and/or creating effective representation forms for machines and human users and creating automation."

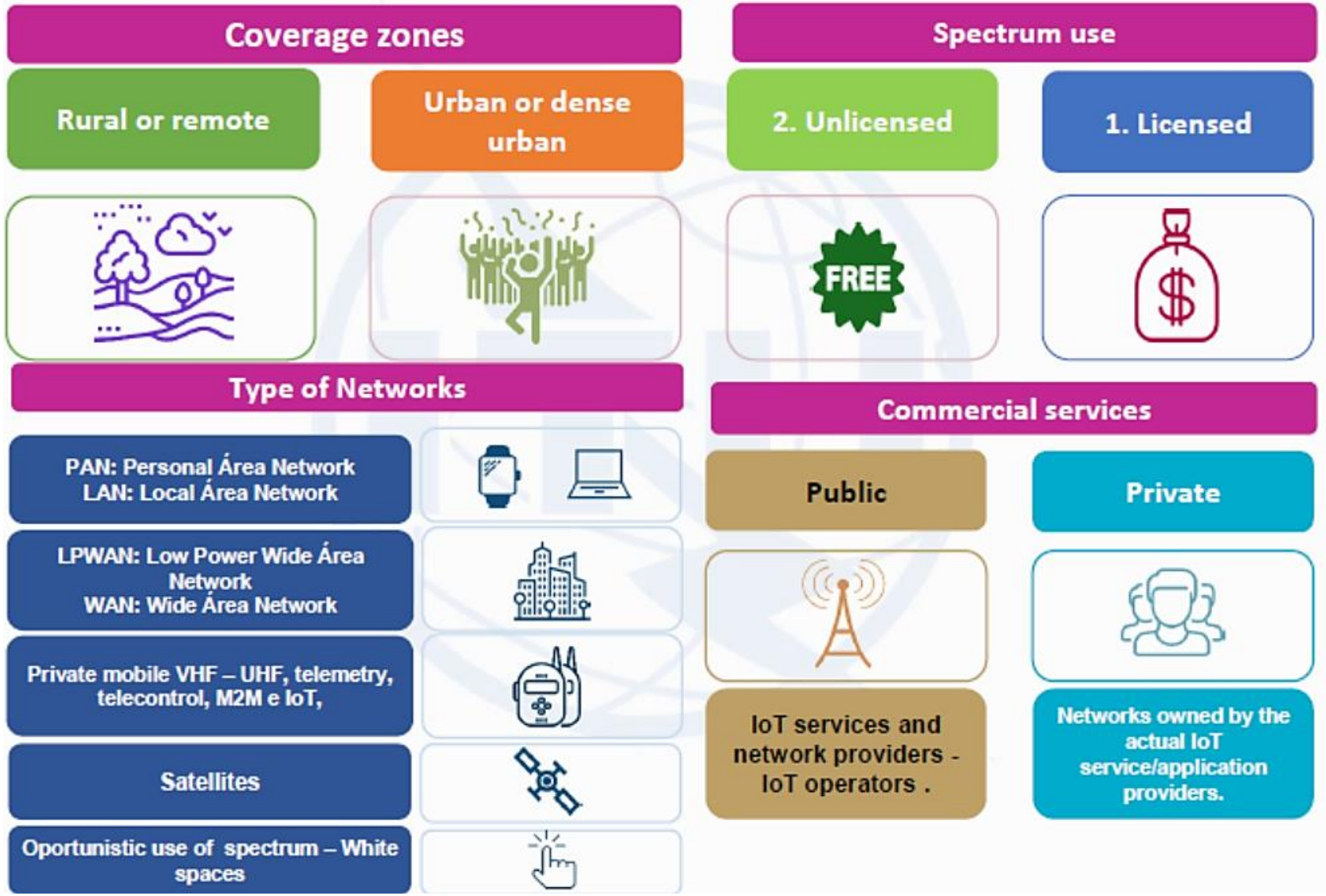
This usually requires data from multiple sources, (near) real-time analytics and visualisation and/or semantic representations.

IoT Usage Categories

Category	Sub-category	
Consumer IoT 	Consumer electronics	Smart TVs, home entertainment (games consoles, speakers), personal entertainment (MP3 players, portable gaming devices), set-top boxes
	Smart home	Home appliances (fridges, washing machines), home infrastructure (routers), home security (alarms), energy monitoring (thermostats)
	Wearables	Fitness trackers (including personal health trackers), smart watches
	Smart vehicles	Connected cars, connected bikes, insurance telematics
	Consumer – others	Trackers for children, the elderly and pets, as well as drones and robots
Industrial IoT 	Smart city	Public transport, surveillance, electric vehicle charging, street lighting, parking, waste management
	Smart utilities	Energy, water and gas smart metering, smart grid
	Smart retail	PoS, digital signage, vending machines, ATMs
	Smart manufacturing	Inventory tracking, monitoring and diagnostics, warehouse management
	Smart buildings	Heating and air con, security, lighting, hot desks, office equipment
	Health	Remote monitoring of medical devices, emergency vehicle infrastructure
	Enterprise – others	Fleet management, applications in agriculture, oil, mining, construction

Source: GSMA Intelligence - IoT: the next wave of connectivity and services

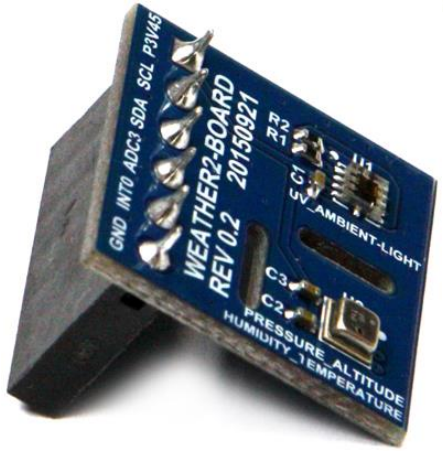
IoT Usage Cases



Source: ITU Workshop on Spectrum Management for Internet of Things Deployment, 22 November 2016, Geneva

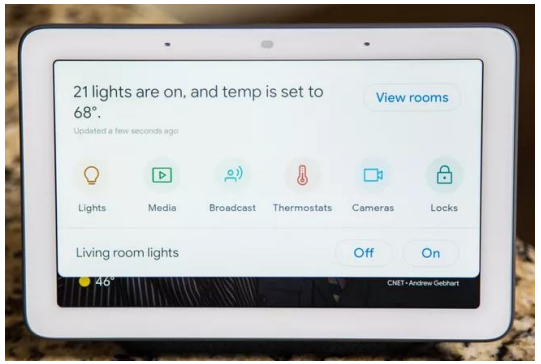
We use so many sensors these days …

- Programmable devices
- Off-the-shelf gadgets/tools



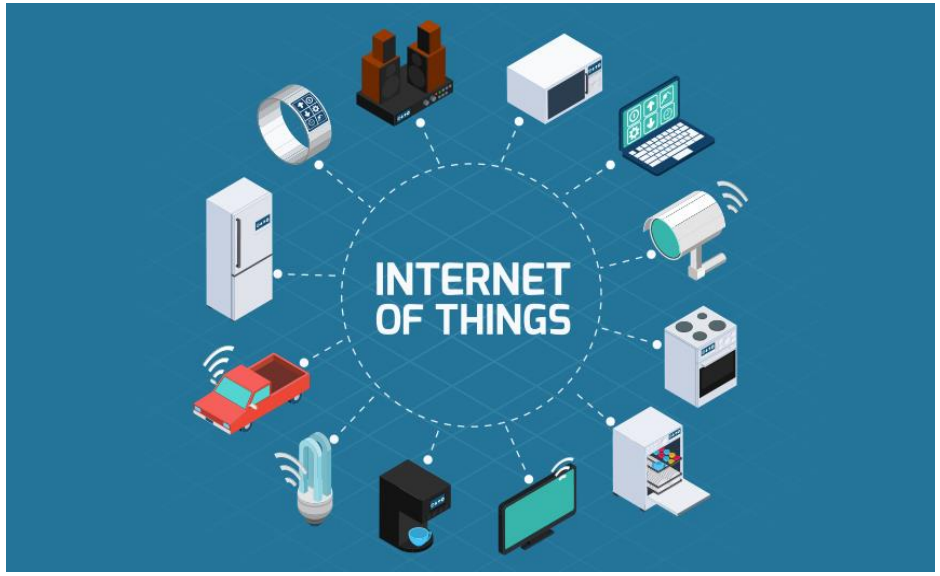
More “Things” are being connected

Home/daily-life devices
Business and
Public infrastructure
Health-care
…



AIoT: Fusing AI with IoT

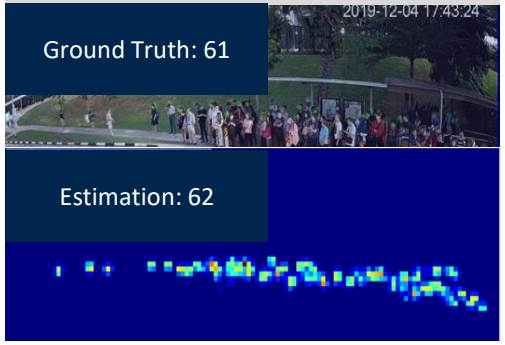
Traditional IoTs



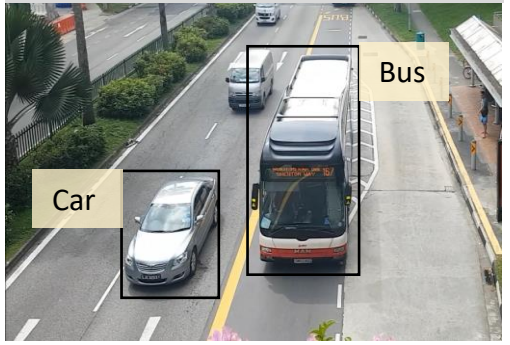
Source: https://www.bankinfosecurity.com/gao-assesses-iot-cybersecurity-other-risks-a-9926

AIoTs

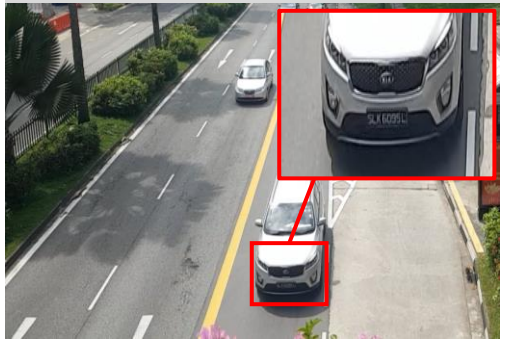
Crowd Counting



Object Localization & Classification

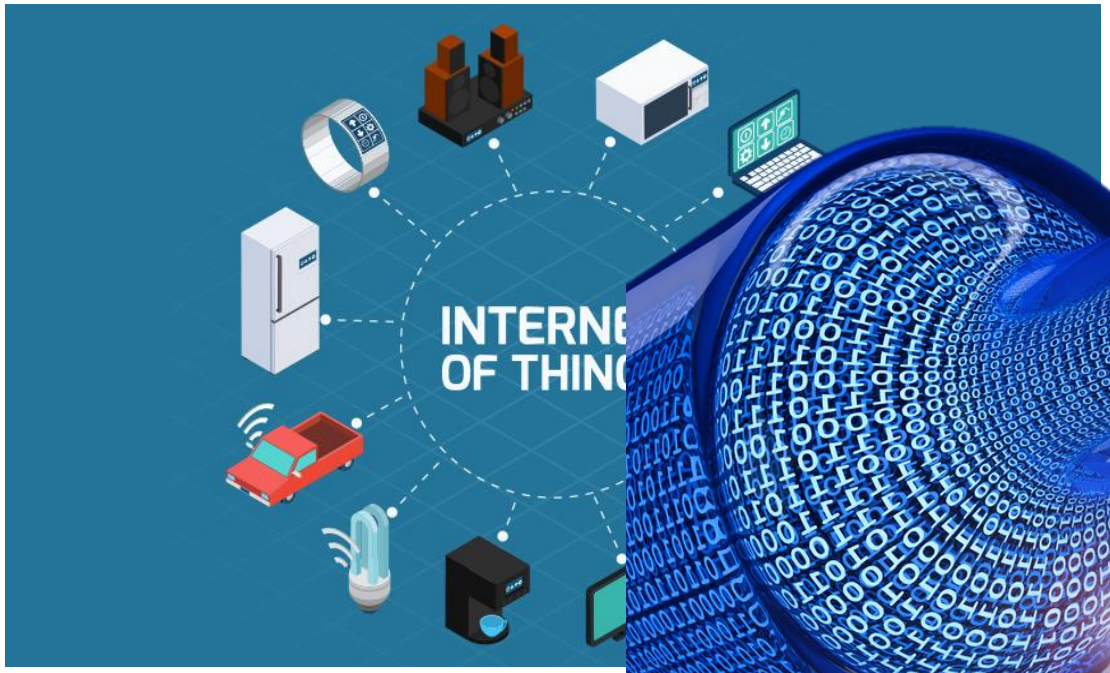


License Pate Recognition

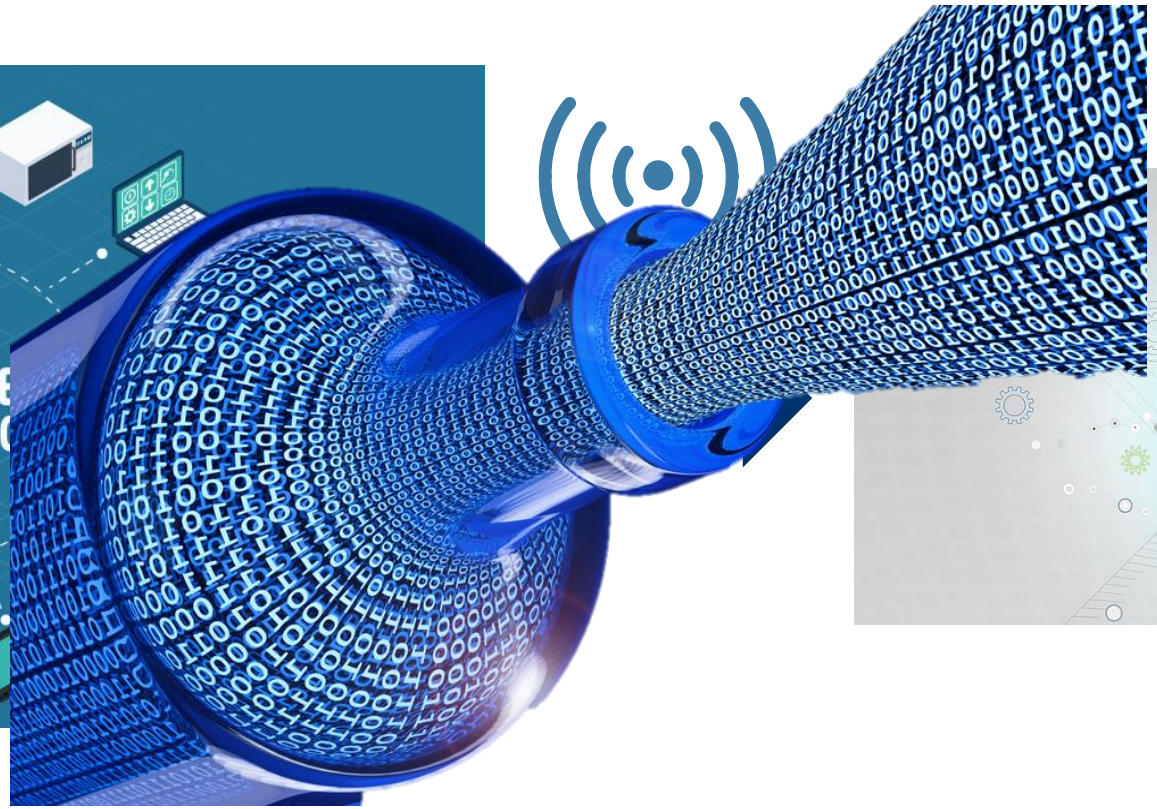


The Need for ‘Edge Computing’

- IDC estimates that there will be **41.6 billion connected IoT** devices generating a whopping **79.4 zettabytes of data** in 2025[1].



Source: https://www.bankinfosecurity.com/gao-assesses-iot-cybersecurity-other-risks-a-9926

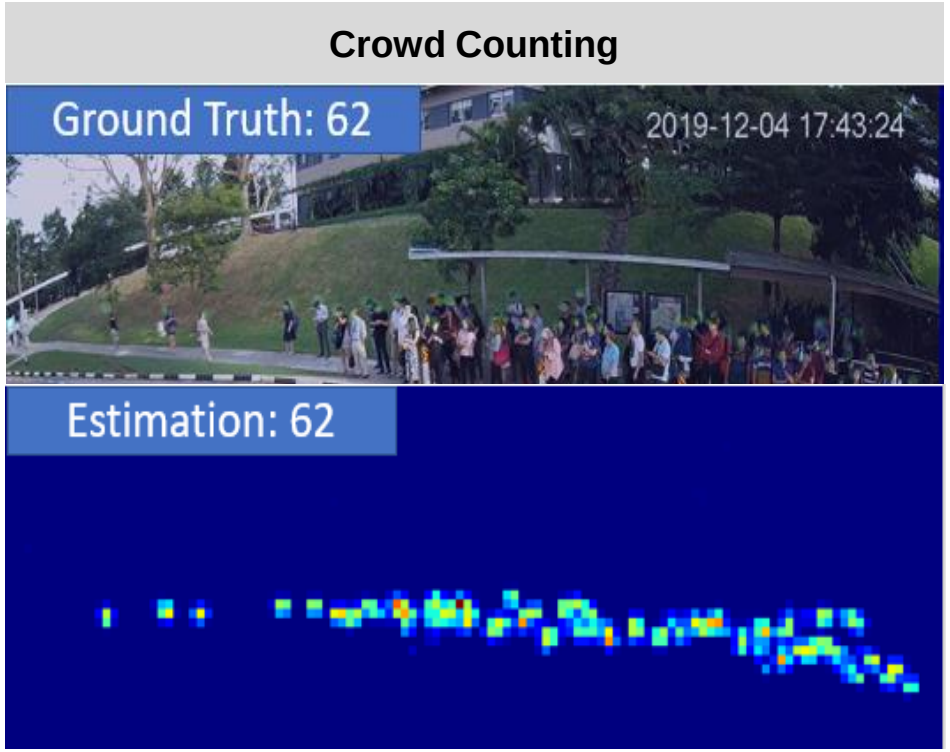


Source: https://www.hpcwire.com/

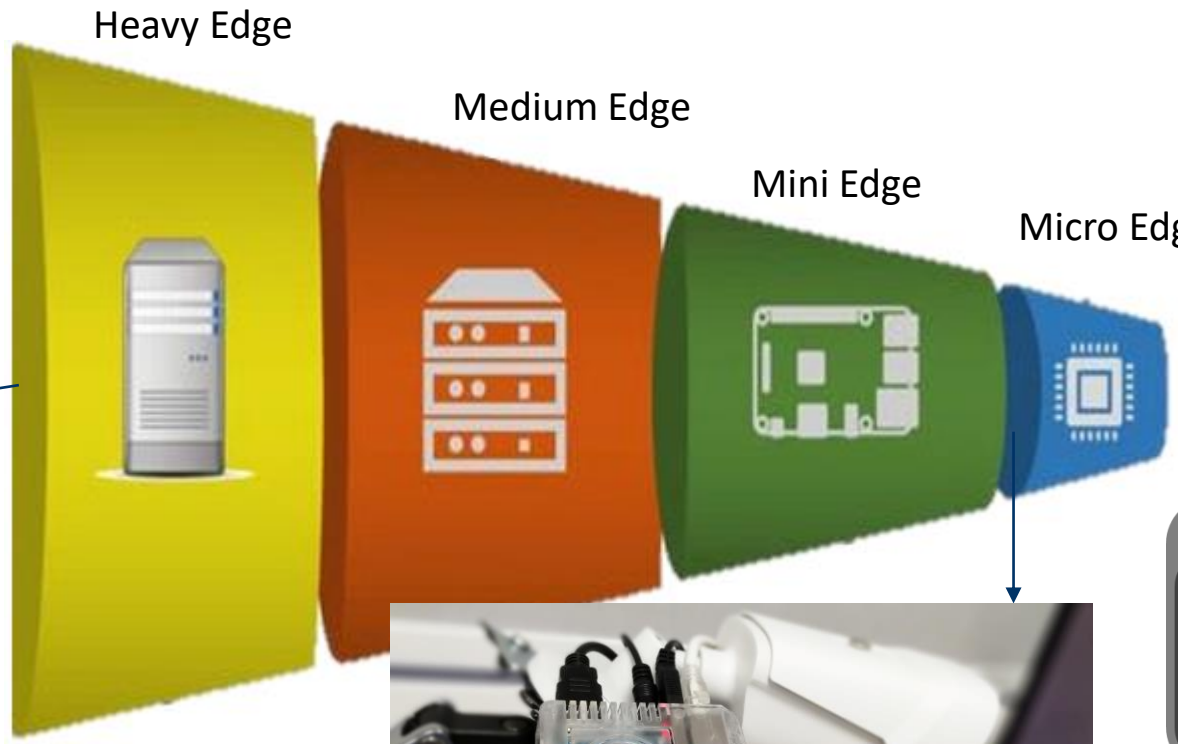
[1] Worldwide Global DataSphere IoT device and data forecast (2019-2023), IDC

Advantages of Edge Computing

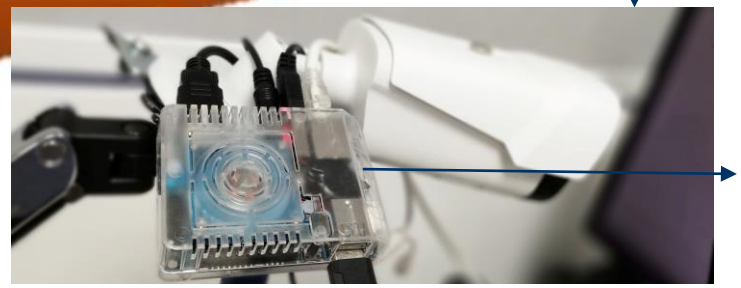
- Reduces Network Bandwidth Requirement
- Faster response time
- Significantly reduced data storage requirements
- …

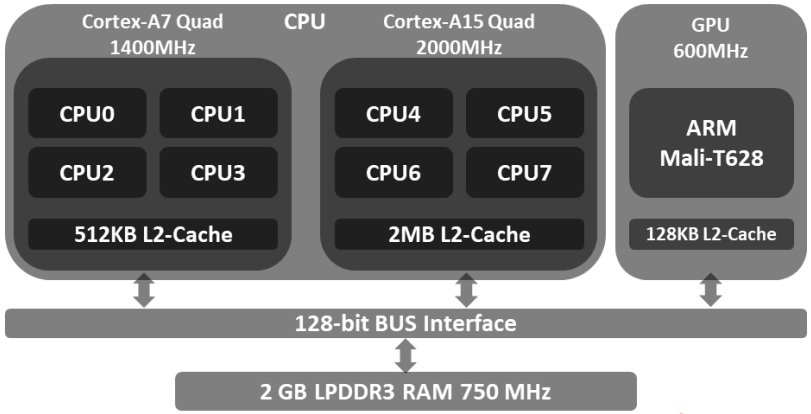


Edge Computing Platforms: Good old Embedded Systems



Credit:
Janakiram.com





Heterogeneous Edge Computing Platforms

So how do we map our applications effectively on such heterogeneous platforms while considering power and performance constraints?

Characteristics of IoT Communications

- **Wireless**
- Low cost
- Low power (long battery duration)
- Low processing capacity
- Low storage capacity
- Extensive network of connections (scalability)
- Various bitrate/bandwidth requirements
- Various range
- Various QoS requirements
- Small size devices (typically)
- Simple network architecture and protocols (arguably)

IoT Connectivity Technologies

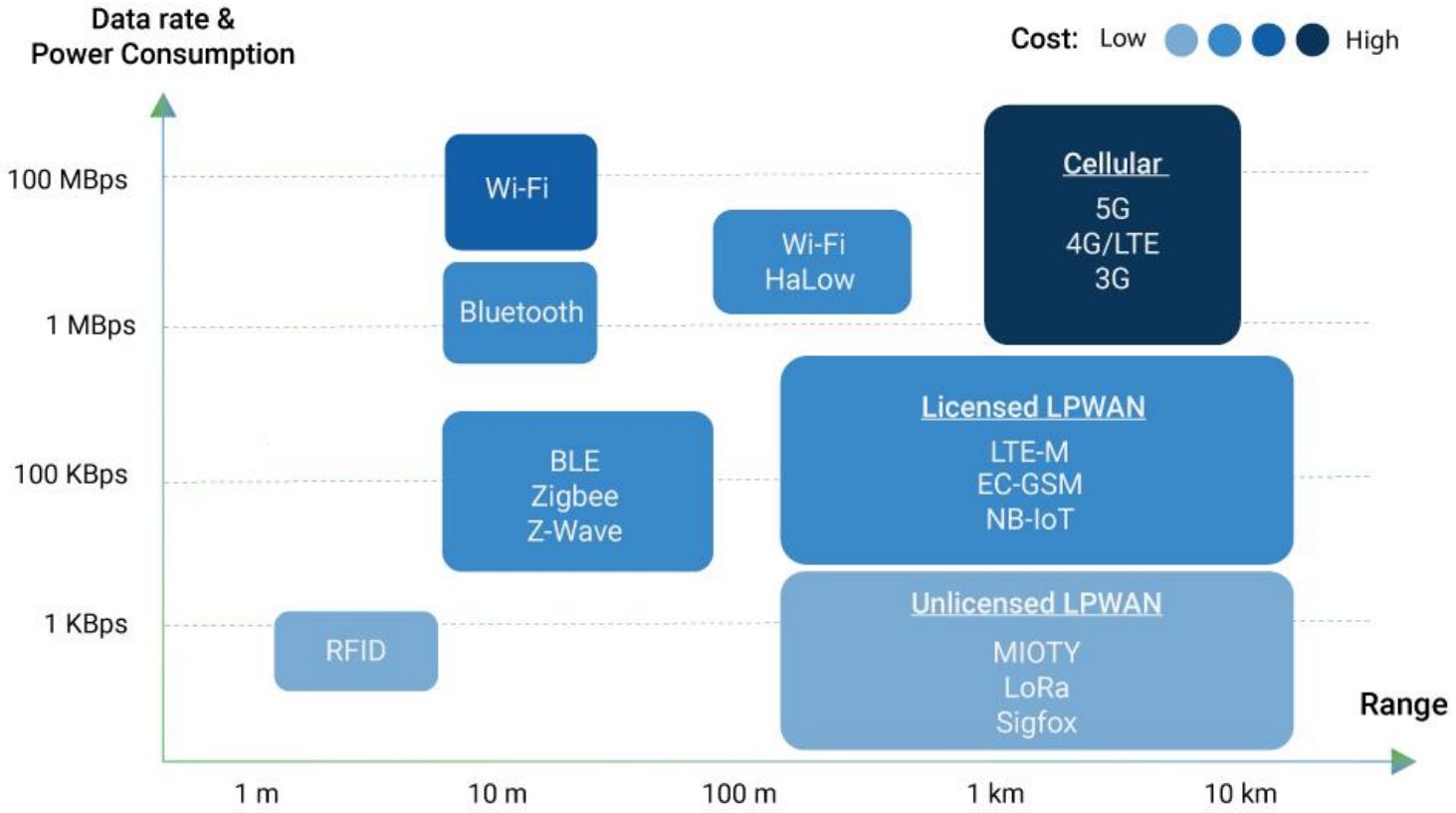


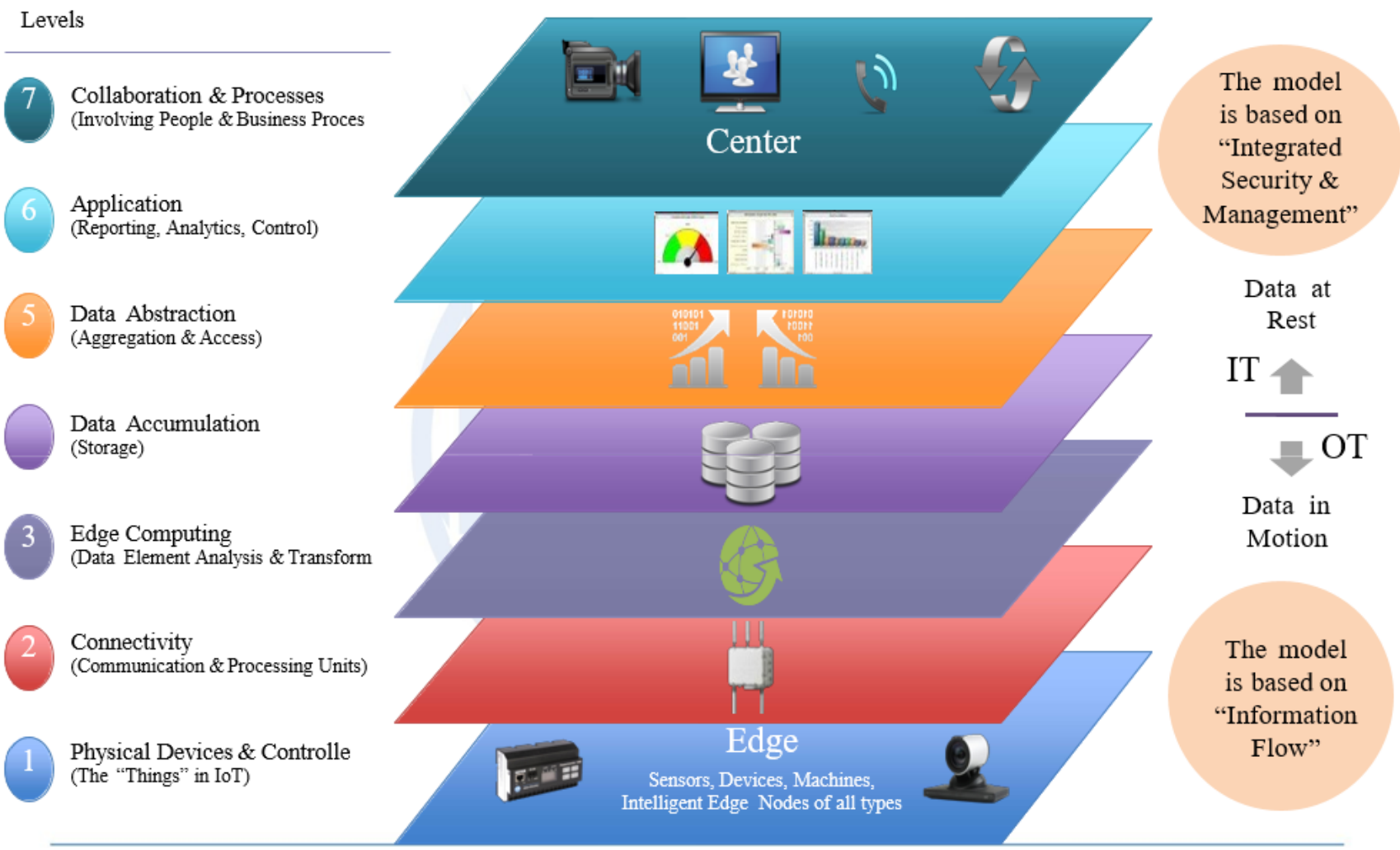
Image @ https://industrytoday.com/best-uses-of-wireless-iot-communication-technology/

Communication

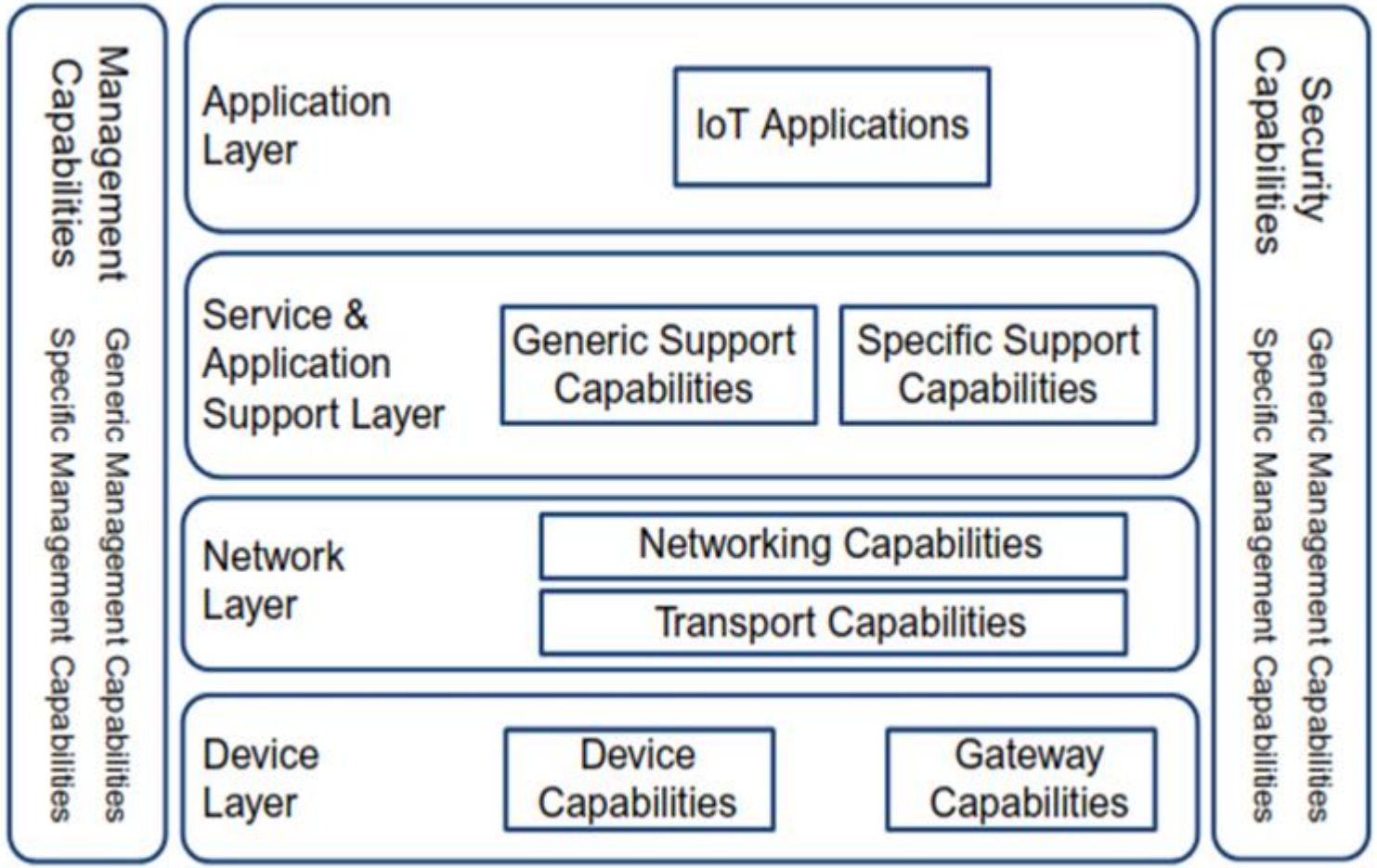
Technology	Frequency	Data Rate	Range	Power Usage	Cost
2G/3G	Cellular Bands	10 Mbps	Several Miles	High	High
Bluetooth/BLE	2.4Ghz	1, 2, 3 Mbps	~300 feet	Low	Low
802.15.4	subGhz, 2.4GHz	40, 250 kbps	> 100 square miles	Low	Low
LoRa	subGhz	< 50 kbps	1-3 miles	Low	Medium
LTE Cat 0/1	Cellular Bands	1-10 Mbps	Several Miles	Medium	High
NB-IoT	Cellular Bands	0.1-1 Mbps	Several Miles	Medium	High
SigFox	subGhz	< 1 kbps	Several Miles	Low	Medium
Weightless	subGhz	0.1-24 Mbps	Several Miles	Low	Low
Wi-Fi	subGhz, 2.4Ghz, 5Ghz	0.1-54 Mbps	< 300 feet	Medium	Low
WirelessHART	2.4Ghz	250 kbps	~300 feet	Medium	Medium
ZigBee	2.4Ghz	250 kbps	~300 feet	Low	Medium
Z-Wave	subGhz	40 kbps	~100 feet	Low	Medium

Source: https://blog.helium.com/802-15-4-wireless-for-internet-of-things-developers-1948fc313b2e

IoT: Reference Model



IoT Reference Model (ITU-T Recommended)



https://www.itu.int/rec/T-REC-Y.2060-201206-I

IoT Design Requirements

IoT Network	Impact on IoT Systems Design
Scale	**Tens of thousand sensors in a given site; or millions distributed geographically** More pressure on application architectures, network load, traffic types, security, non-standard usage pattern
Heterogeneous end-points	**Vast array of sensors, actuators, and smart devices – IP or non-IP** Diverse data rate exchange, form factor, computing and communication capabilities, legacy protocols
Accessibility-Visibility of end-points	**May be deployed before activation, maybe or cannot-be accessed once deployed** Devices deliver services with little or no human control, difficult to correct mistakes, device management is key
Criticality of services	**Human life critical (Healthcare), Critical infrastructure (Smart Grid)** Stringent latency (10ms for SG) and reliability requirements, may challenge/exceed network capabilities of today
Intrusiveness	**Things with explicit intent to better manage end-users (eHealth, Smart Grid)** Issues of Privacy become major obstacles
Geography	**Movement across borders** Issues of numbering for unique identification

Source: ITU CoE training on BB networks planning, Bangkok, Sep 2017

IoT Network Connectivity Requirements

IoT Network	Impact on IoT Systems Design
Resource-constrained endpoints	**Severely resource constrained (memory, compute)** Cost motivation: compute/memory several orders of magnitude lower, limited remote SW update capability, light protocols, security
Low Power	**Some end-point types may be mostly 'sleeping' and awakened when required** • Sensors cannot be easily connected to a power source • Reduced interaction time between devices and applications (some regulations state duty cycle of no more than 1%) • Idle mode most of the time (energy consumption of around 100 µW). Connected mode just for transmission (mA) • < 100 MHz clock frequency • Embedded memory of few Mb
Embedded	**Smart civil infrastructure, building, devices inside human beings** Sensors deployed in secure or hostile operating conditions, difficult to change without impacting system, Security
Longevity	**Deployed for life typically, have to build-in device redundancy** Very different lifetime expectancy, rate of equipment change in IoT business domains much lower than ICT Industry
High Sensitivity on reception	**Gateways and end-devices with a high sensitivity around** -150 dBm/-125 dBm with Bluetooth lower than -95 dBm in in cellular

Source: ITU CoE training on BB networks planning, Bangkok, Sep 2017

Key IoT Network Metrics

- **Latency (Round-Trip Time)**
  - What It Is: Time between sending data and receiving an acknowledgement or echo.
  - Why It Matters: Critical for real-time control or interactive applications.
- **Throughput (Data Rate)**
  - What It Is: Amount of data transferred per unit time (bps, Kbps, Mbps).
  - Why It Matters: Determines how fast you can send sensor readings or firmware updates.
- **Packet Loss**
  - What It Is: Fraction of transmitted packets that never arrive or get acknowledged.
  - Why It Matters: Indicates reliability; high loss can break important IoT workflows.
- **Jitter (Latency Variation)**
  - What It Is: Fluctuation in packet delay over time.
  - Why It Matters: Affects applications sensitive to timing (voice, motion control).

Obtaining These Metrics (No Dedicated Tools)

- **Custom Send-and-Reply Logic**
  - Write a simple application that sends a known number of packets and measures send/receive timestamps.
  - How to Do It:
    1. Start a timer when you send packet #1.
    2. Stop the timer once you receive all echoes (or acknowledgements).
    3. Record how many packets arrived vs. were sent.
    4. Transmit a large volume of packets to thoroughly stress-test the network and obtain more representative average metric readings.
    5. Calculate:
       - Latency: (ReceiveTime - SendTime) for each packet.
       - Throughput: (Total Bytes * 8) / Elapsed Time.
       - Packet Loss: (Sent - Received) / Sent.
       - Jitter: Variation in consecutive packet latencies.

Obtaining These Metrics (No Dedicated Tools)

- **Adapt to Each Protocol**
  - Wi-Fi: Send UDP/TCP data directly over IP.
  - Bluetooth/BLE: Use a custom GATT characteristic to send data and receive notifications.
  - LoRaWAN/Zigbee: Rely on sending data uplinks and receiving confirmations.

- **Practical Constraints**
  - Collect Logs: Store timestamps in your microcontroller or gateway to compute metrics offline.
  - Duty Cycle & Battery: For LoRa/Zigbee, limit how frequently you send.
  - Payload Size Limits: Some protocols allow only small packets
    - segment large data accordingly.
  - Clock Sync (Optional): To measure one-way delay or advanced jitter, ensure devices have a common time reference (NTP, etc.).

[Summary] Factors to Consider

- **Range**: The distance over which the devices need to communicate will influence the protocol choice. Some protocols, such as Bluetooth and Zigbee, have a limited range, while others, like LoRaWAN and Sigfox, can cover much larger distances.
- **Power consumption**: For devices with limited power resources, such as battery-powered devices, the power consumption of the communication protocol is an important consideration. Protocols with low power consumption, like BLE and Zigbee, may be more suitable in these cases.
- **IoT Network Metrics**: Latency (Round-Trip Time), Throughput (Data Rate), Packet Loss, and Jitter (Latency Variation) collectively define the speed, reliability, and consistency of data transmission in wireless IoT systems.
- **Compatibility/Scalability**: It is important to consider the compatibility of the chosen protocol with the devices and the infrastructure that it will be used with.
- **Security**: The security of the communication protocol is an important consideration, especially for applications that involve sensitive data or critical infrastructure. Protocols that offer strong encryption and authentication, such as TLS and DTLS, may be more suitable in these cases.
- **Cost**: The cost of implementing and maintaining the communication protocol should also be considered. Protocols that require specialized hardware or infrastructure may be more expensive to implement than those that use more widely available technologies.