



EEM602 Internet of Things

Lecture # 2 IoT architecture

Prof. Mohab Abd-Alhameed Mangoud

Professor, Electrical Engineering

University of Bahrain

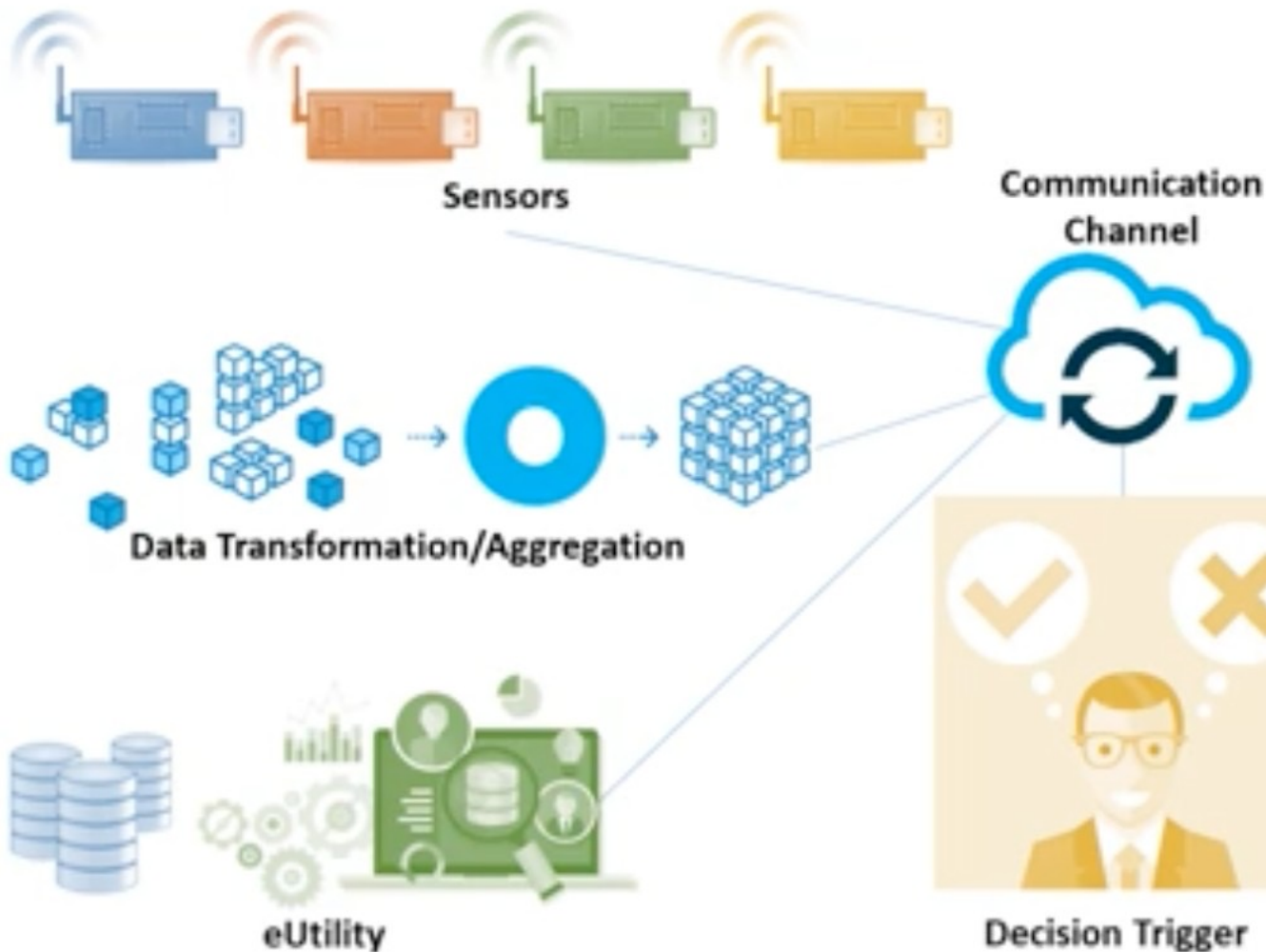
College of Engineering,

Department of Electrical and Electronics Engineering,

[mmangoud@uob.edu,bh](mailto:mmangoud@uob.edu.bh)

mangoud.com

The Internet of Things (IoT)

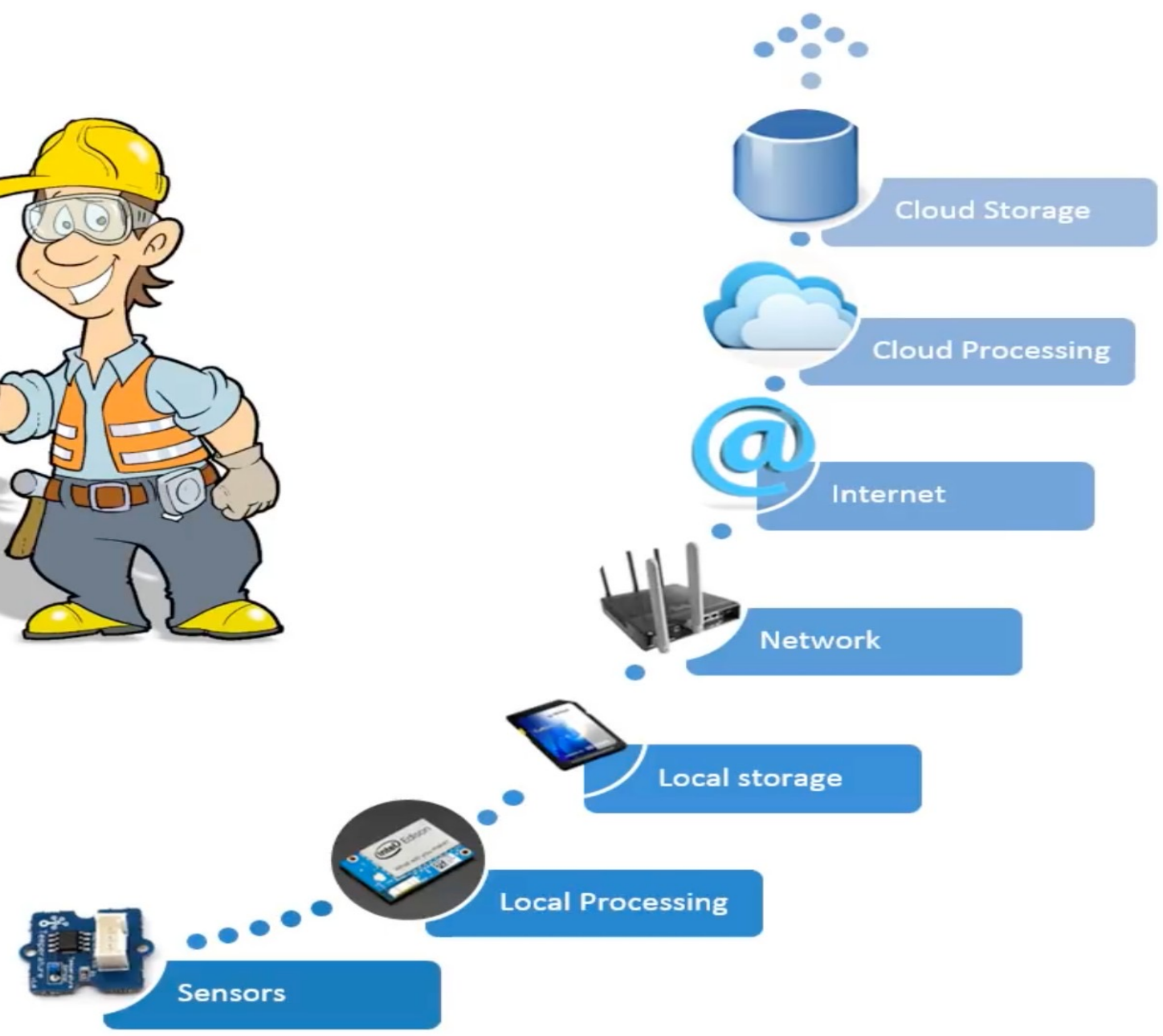


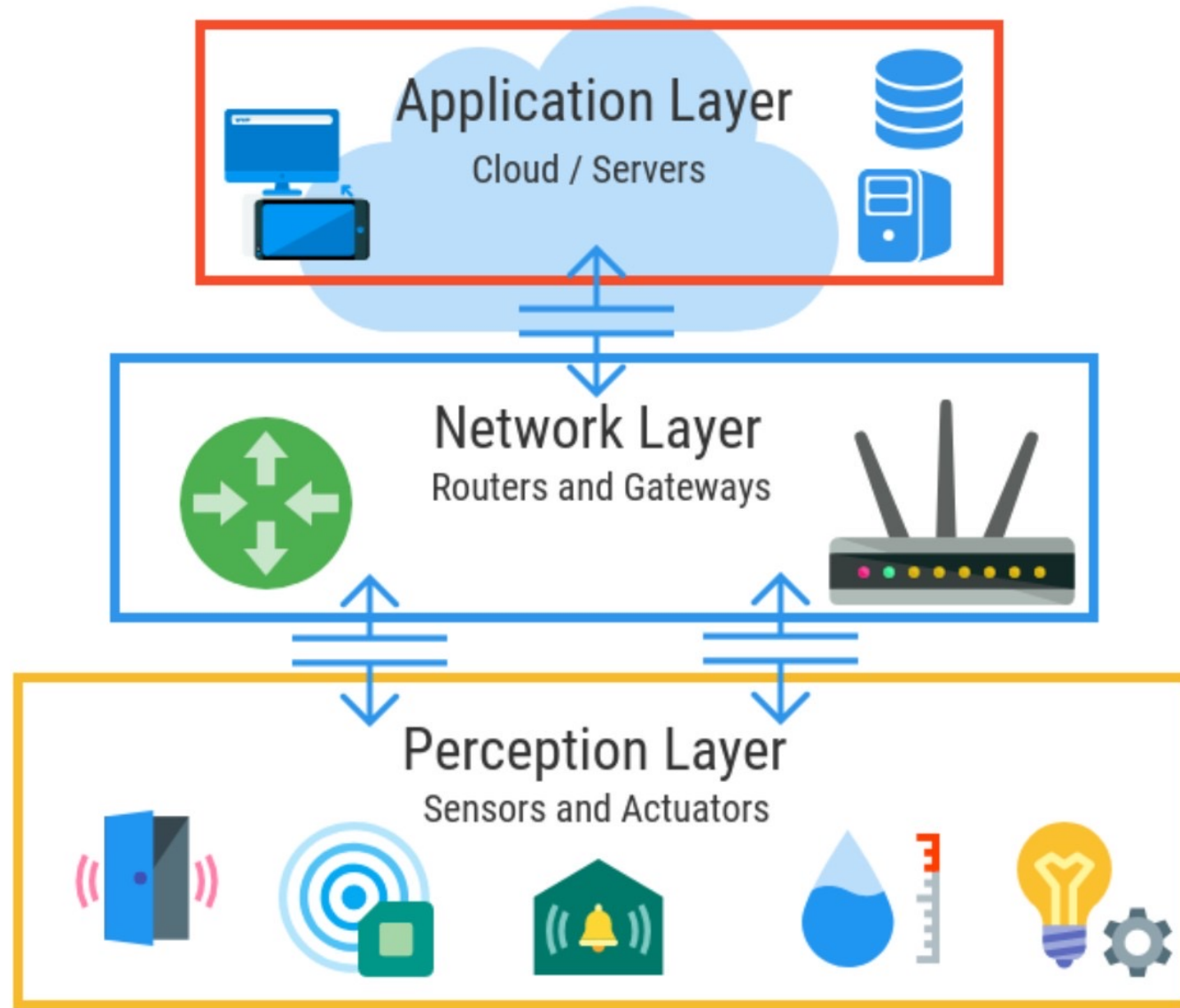
Five Knowledge Areas of IoT

Sensors
Aggregators
Communication Channels
eUtility
Decision Trigger

CWNP Official: The *Internet of Things (IoT)* is the application of connected objects (cyber-physical systems and other objects) that use Internet technologies for automation, reporting, and human interaction.





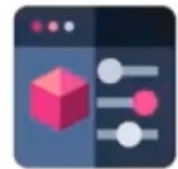


Three-tier IoT architecture

IoT Ecosystem

There is no single consensus on architecture for IoT, which is agreed universally

Basic Architecture



Application
Layer

*Responsible for delivering application specific services to the user.
Defines applications in which the Internet of Things can be
deployed.*



Network
Layer

*Responsible for connecting smart things, network devices, and
servers. Also used for transmitting and processing sensor data.*



Perception
Layer

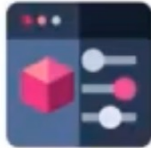
*Sensors sense and gather information about the environment.
Senses physical parameters or identifies other objects in the
environment.*

IoT Ecosystem – 5 Layer Architecture



Business
Layer

Manages the whole IoT system, including applications, business and profit models, and users' privacy.



Application
Layer

Responsible for delivering application specific services to the user.



Processing
Layer

Stores, analyses, and processes huge amounts of data. Employs databases, cloud computing, & big data processing modules.



Transport
Layer

Transfers the sensor data between different layer through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.



Perception
Layer

Sensors sense and gather information about the environment.

Application layer

IoT application

Software that coordinates the interaction of people, systems, and things/devices for a given purpose

Analytics and data management

Software components to store, process, and analyze a vast amount of time-series-based machine data

Process management

Software components to define, execute, and monitor processes across people, systems, and things/devices

Application platform

Application development and execution environment to create IoT applications

Thing/device communications and management

Software components to communicate with, as well as provision and manage, things/devices

Connectivity layer

Network communication

Protocols that enable communication between things/devices, backbone infrastructure, and/or the cloud

Things/device layer

Thing/device Software

Embedded software that runs on the physical thing to manage and operate its functionality

IoT components

Embedded sensors, actuators, processors, and connectivity ports/antennas

Thing/device hardware

Core hardware components

Figure 1.2 High-level view of an IoT architecture.

Application Layer



Smart Home



Smart Transport



Smart Buildings



Smart healthcare

Middle-ware Layer



API



Web Service



Datacenter



Cloud

Network Layer



Transmission



Internet



WiFi



Routing

Sensing Layer



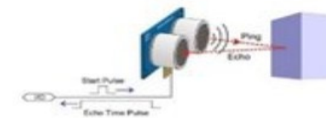
Temperature
Sensor



Actuator
[22]

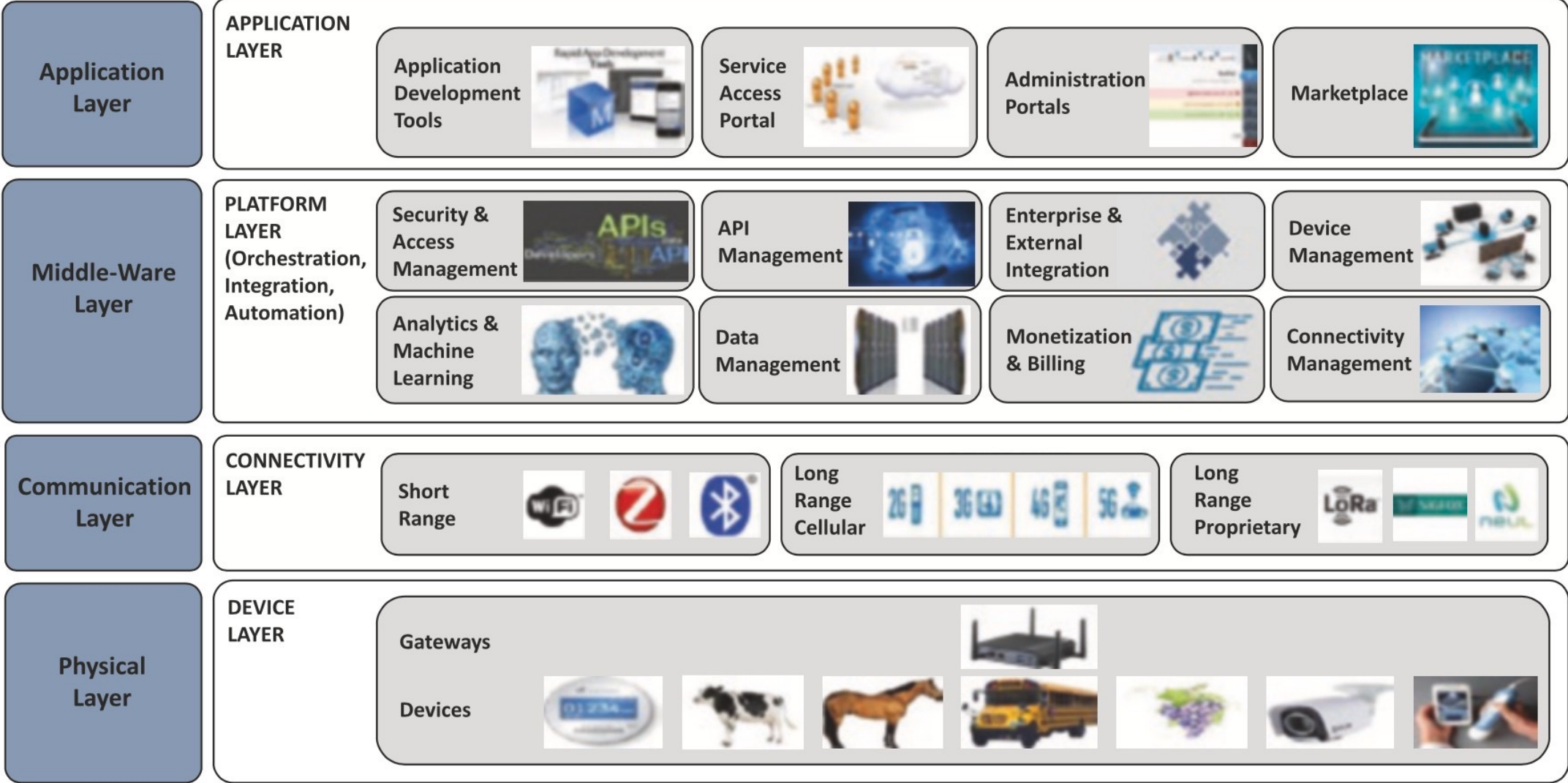


Smart Smoke
Detection [21]



Ultrasonic
Sensors [23]

IOT Reference Architecture



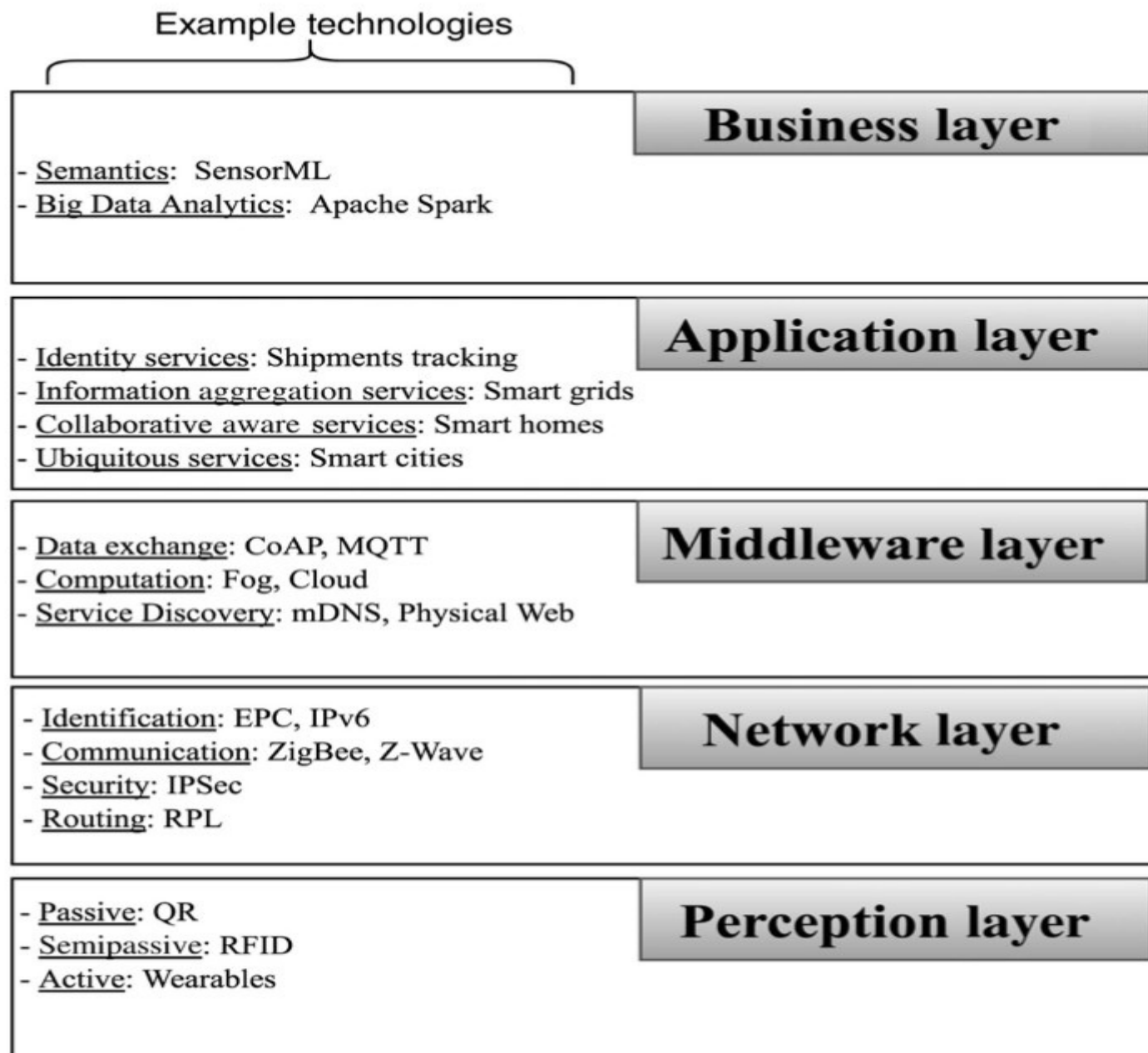
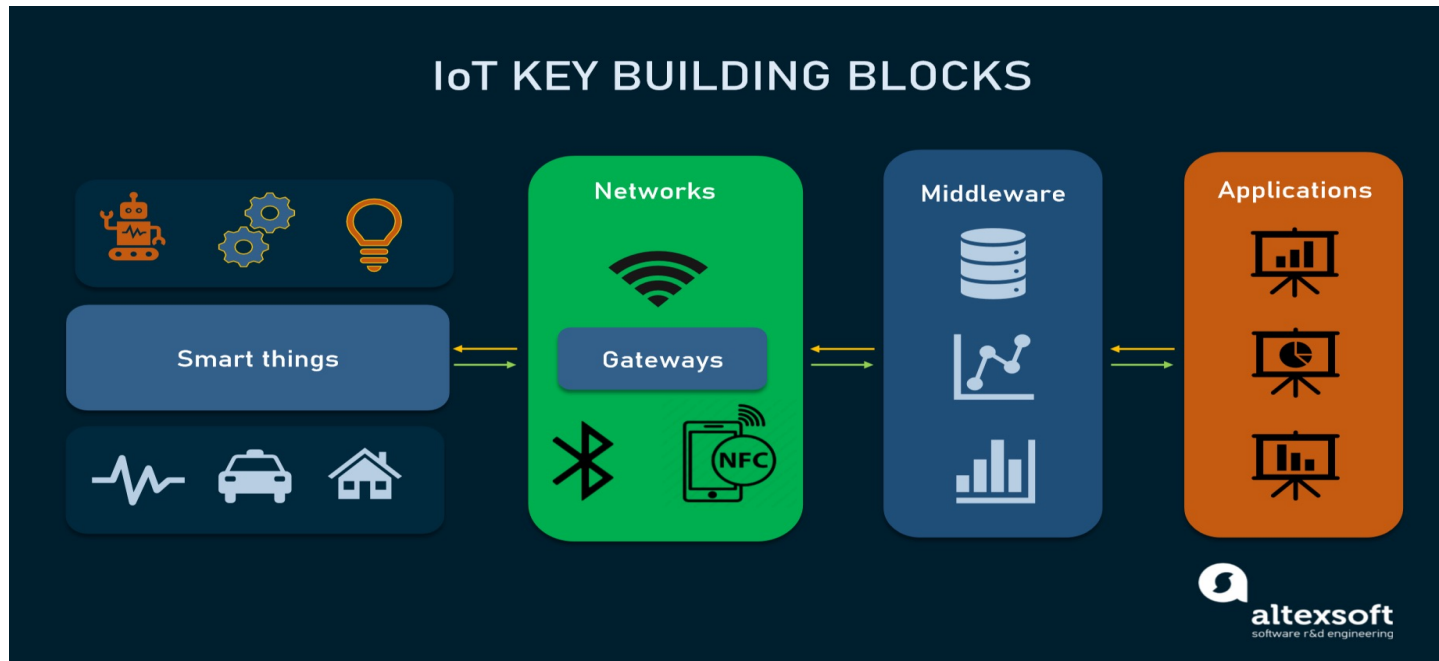


Figure 3.1 The IoT five-layer architectural model. (Reproduced with permission from IEEE Press.)

Major IoT building blocks and layers

the key building blocks of any IoT structure are always the same, namely:

- **Smart things**
- **Networks** and **gateways** enabling low-power devices (which is often the case in IoT) to enter the big Internet;
- **Middleware** or **IoT platforms** providing data storage spaces and advanced computing engines along with analytical capabilities;
- **Applications**, allowing end users to benefit from IoT and manipulate the physical world.

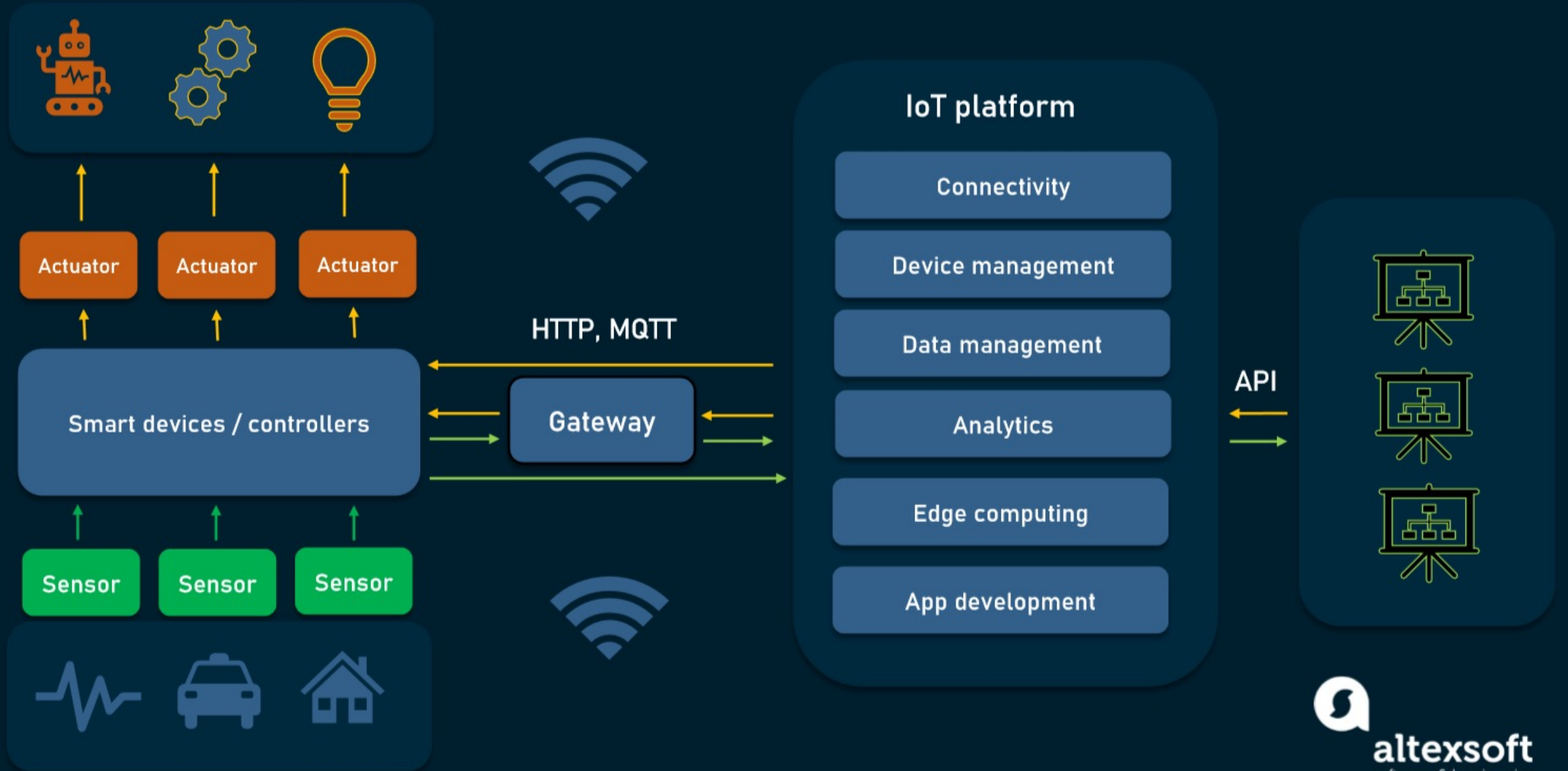


The skeleton of an IoT system.

- **Perception layer** hosting smart things;
- **Connectivity or transport layer** transferring data from the physical layer to the cloud and vice versa via networks and gateways;
- **Processing layer** employing IoT platforms to accumulate and manage all data streams; and
- **Application layer** delivering solutions like analytics, reporting, and device control to end users.

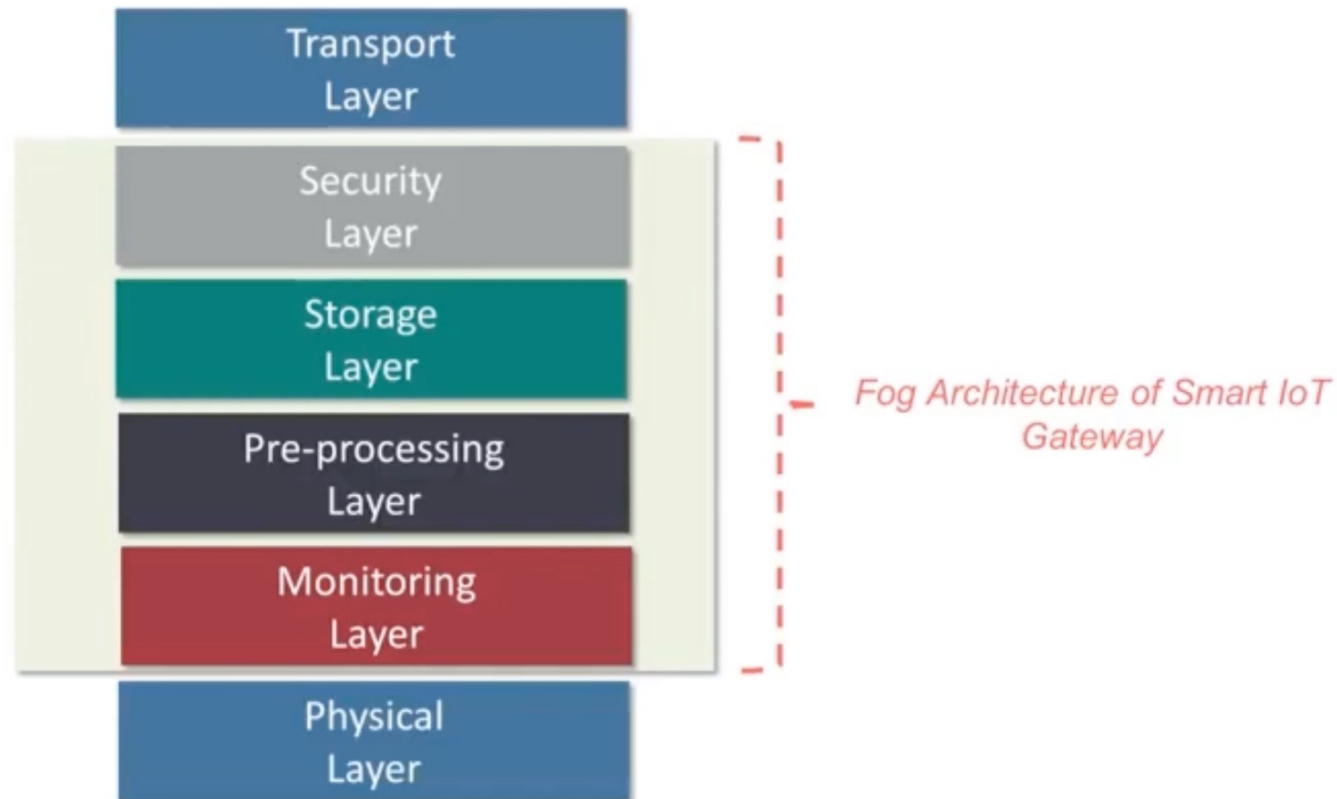
<https://www.altexsoft.com/blog/iot-architecture-layers-components/>

IoT infrastructure



Fog Computing in IoT

Fog architecture presents a layered approach, which *inserts monitoring, preprocessing, storage, and security layers* between the *physical* and *transport layers*.



☞ *Monitoring and pre-processing are done on the edge of the network before sending data to the cloud.*

Three additional layers:

- The **edge or fog computing layer** performing data preprocessing close to the edge, where IoT things collect new information. Typically, edgy computing occurs on gateways;
- The **business layer** where businesses make decisions based on the data; and
- The **security layer** encompassing all other layers.

Perception layer

converting analog signals into digital data and vice versa

The initial stage of any IoT system embraces a wide range of “things” or endpoint devices that act as a bridge between the real and digital worlds. They vary in form and size, from tiny silicon chips to large vehicles. By their functions, IoT things can be divided into the following large groups.

Sensors such as probes, gauges, meters, and others. They collect physical parameters like temperature or humidity, turn them into electrical signals, and send them to the IoT system. IoT sensors are typically small and consume little power.

Actuators, translating electrical signals from the IoT system into physical actions. Actuators are used in motor controllers, lasers, robotic arms.

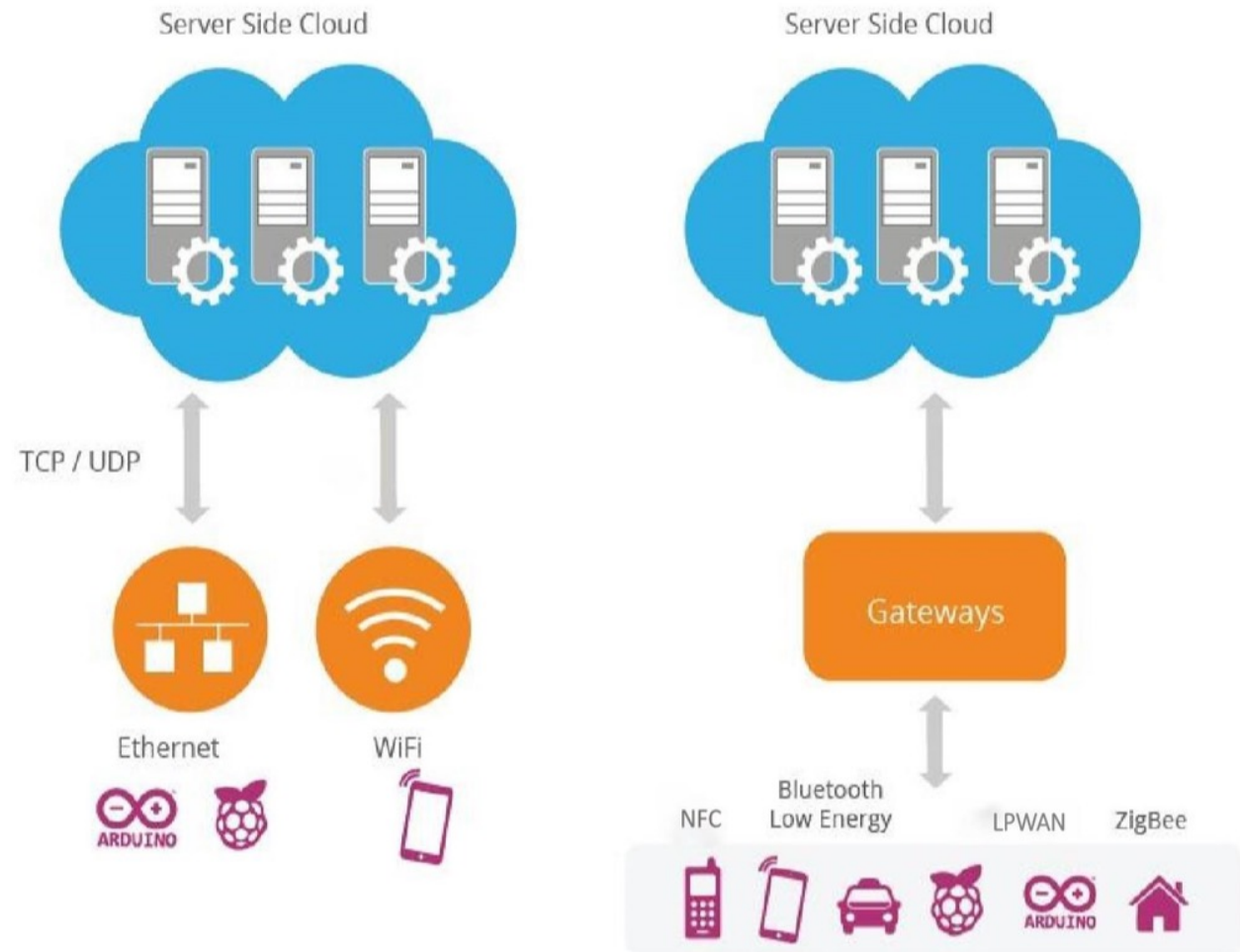
Machines and devices connected to sensors and actuators or having them as integral parts.

It's important to note that the architecture puts no restriction on the scope of its components or their location. The edge-side layer can include just a few “things” physically placed in one room or myriads of sensors and devices distributed across the world.

Connectivity layer: enabling data transmission

The second level is in charge of all communications across devices, networks, and cloud services that make up the IoT infrastructure. The connectivity between the physical layer and the cloud is achieved in two ways:

- **directly**, using TCP or UDP/IP stack;
- **via gateways** — hardware or software modules performing translation between different protocols as well as encryption and decryption of IoT data.



Two key models of connectivity between physical and cloud levels in IoT. Source:

The **communications** between devices and cloud services or gateways involve different networking technologies.

Ethernet connects stationary or fixed IoT devices like security and video cameras, permanently installed industrial equipment, and gaming consoles.

WiFi, the most popular technology of wireless networking, is a great fit for data-intensive IoT solutions that are easy to recharge and operate within a small area. A good example of use is smart home devices connected to the electrical grid.

NFC (Near Field Communication) enables simple and safe data sharing between two devices over a distance of 4 inches (10 cm) or less.

Bluetooth is widely used by wearables for short-range communications. To meet the needs of low-power IoT devices, the Bluetooth Low-Energy (BLE) standard was designed. It transfers only small portions of data and doesn't work for large files.

LPWAN (Low-power Wide-area Network) was created specifically for IoT devices. It provides long-range wireless connectivity on low power consumption with a battery life of 10+ years. Sending data periodically in small portions, the technology meets the requirements of smart cities, smart buildings, and smart agriculture (field monitoring).

ZigBee is a low-power wireless network for carrying small data packages over short distances. The outstanding thing about ZigBee is that it can handle up to 65,000 nodes. Created specifically for home automation, it also works for low-power devices in industrial, scientific, and medical sites.

Cellular networks offer reliable data transfer and nearly global coverage. There are two cellular standards developed specifically for IoT things. LTE-M (Long Term Evolution for Machines) enables devices to communicate directly with the cloud and exchange high volumes of data. NB-IoT or Narrowband IoT uses low-frequency channels to send small data packages.

NETWORKING TECHNOLOGIES USED in IoT

Network	Connectivity	Pros and Cons	Popular use cases
Ethernet	Wired, short-range	<ul style="list-style-type: none"> ☺ High speed ☺ Security ☹ Range limited to wire length ☹ Limited mobility 	Stationary IoT: video cameras, game consoles, fixed equipment
WiFi	Wireless, short-range	<ul style="list-style-type: none"> ☺ High speed ☺ Great compatibility ☹ Limited range ☹ High power consumption 	Smart home, devices that can be easily recharged
NFC	Wireless, ultra-short-range	<ul style="list-style-type: none"> ☺ Reliability ☺ Low power consumption ☹ Limited range ☹ Lack of availability 	Payment systems, smart home
Bluetooth Low-Energy	Wireless, short-range	<ul style="list-style-type: none"> ☺ High speed ☺ Low power consumption ☹ Limited range ☹ Low bandwidth 	Small home devices, wearables, beacons
LPWAN	Wireless, long-range	<ul style="list-style-type: none"> ☺ Long range ☺ Low power consumption ☹ Low bandwidth ☹ High latency 	Smart home, smart city, smart agriculture (field monitoring)
ZigBee	Wireless, short-range	<ul style="list-style-type: none"> ☺ Low power consumption ☺ Scalability ☹ Limited range ☹ Compliance issues 	Home automation, healthcare and industrial sites
Cellular networks	Wireless, long-range	<ul style="list-style-type: none"> ☺ Nearly global coverage ☺ High speed ☺ Reliability ☹ High cost ☹ High power consumption 	Drones sending video and images

Edge or fog computing layer: reducing system latency

This level is essential for enabling IoT systems to meet the speed, security, and scale requirements of the 5th generation mobile network or 5G.

The new wireless standard promises faster speeds, lower latency, and the ability to handle many more connected devices, than the current 4G standard.

The idea behind edge or fog computing is to process and store information as early and as close to its sources as possible.

This approach allows for analyzing and transforming high volumes of real-time data locally, at the edge of the networks.

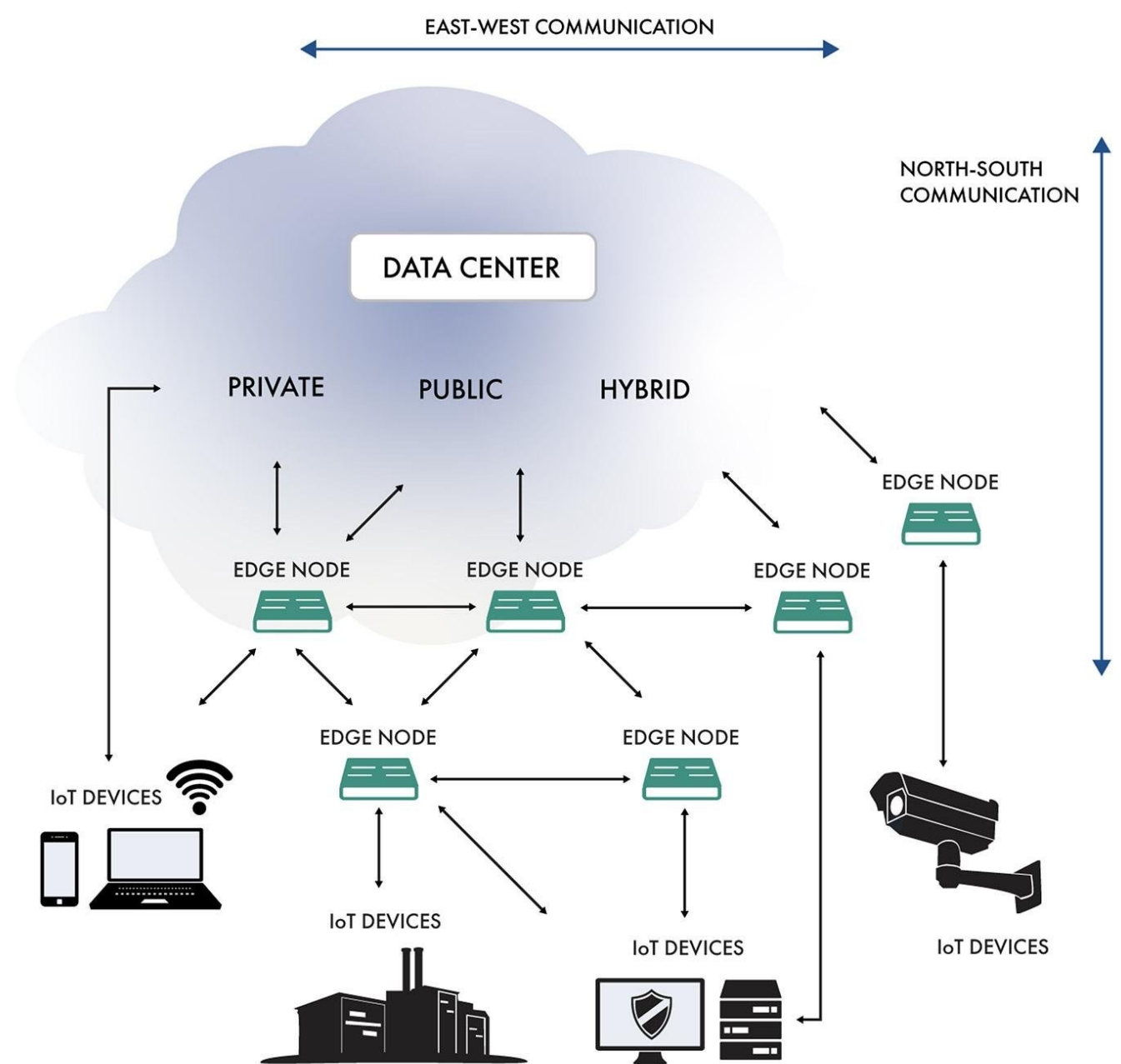
Thus, you save the time and other resources that otherwise would be needed to send all data to cloud services.

The result is reduced system latency that leads to real-time responses and enhanced performance.

Edge computing occurs on gateways, local servers, or other edge nodes scattered across the network. At this level, data can be:

- evaluated to determine if it needs further processing at higher levels,
- formatted for further processing,
- decoded,
- filtered, and
- redirected to an additional destination

To sum up, the first three layers see data in motion, as it is constantly moving and altering. Only on hitting the next level, is data finally at rest and available for use by consumer applications.



The scheme of communications between IoT devices, edge nodes, and cloud data centers. Source: [DesignNews](#)

Processing layer: making raw data useful

The processing layer accumulates, stores, and processes data that comes from the previous layer. All these tasks are commonly handled via IoT platforms and include two major stages.

Data accumulation stage

The real-time data is captured via an API and put at rest to meet the requirements of non-real-time applications. The data accumulation component stage works as a transit hub between event-based data generation and query-based data consumption.

Among other things, the stage defines whether data is relevant to the business requirements and where it should be placed. It saves data to a wide range of storage solutions, from data lakes capable of holding unstructured data like images and video streams to event stores and telemetry databases. The total goal is to sort out a large amount of diverse data and store it in the most efficient way.

Data abstraction stage

Here, data preparation is finalized so that consumer applications can use it to generate insights. The entire process involves the following steps:

- combining data from different sources, both IoT and non-IoT, including ERM, ERP, and CRM systems;
- reconciling multiple data formats; and
- aggregating data in one place or making it accessible regardless of location through data virtualization.

Similarly, data collected at the application layer is reformatted here for sending to the physical level so that devices can “understand” it.

Together, the data accumulation and abstraction stages veil details of the hardware, enhancing the interoperability of smart devices. What’s more, they let software developers focus on solving particular business tasks — rather than on delving into the specifications of devices from different vendors.

Application layer: addressing business requirements

At this layer, [information is analyzed by software to give answers to key business questions](#). There are hundreds of IoT applications that vary in complexity and function, using different technology stacks and operating systems. Some examples are:

- device monitoring and control software,
- mobile apps for simple interactions,
- business intelligence services, and
- analytic solutions using machine learning.

Currently, applications can be built right on top of IoT platforms that offer software development infrastructure with ready-to-use instruments for data mining, advanced analytics, and [data visualization](#). Otherwise, IoT applications use APIs to integrate with middleware.

Business layer: implementing data-driven solutions

The information generated at the previous layers brings value if only it results in problem-solving solution and achieving business goals.

New data must initiate collaboration between stakeholders who in turn introduce new processes to enhance productivity.

The decision-making usually involves more than one person working with more than one software solution.

For this reason, the business layer is defined as a separate stage, higher than a single application layer

Security layer: preventing data breaches

It goes without saying that there should be a security layer covering all the above-mentioned layers. IoT security is a broad topic worthy of a separate article. Here we'll only point out the basic features of the safe architecture across different levels.

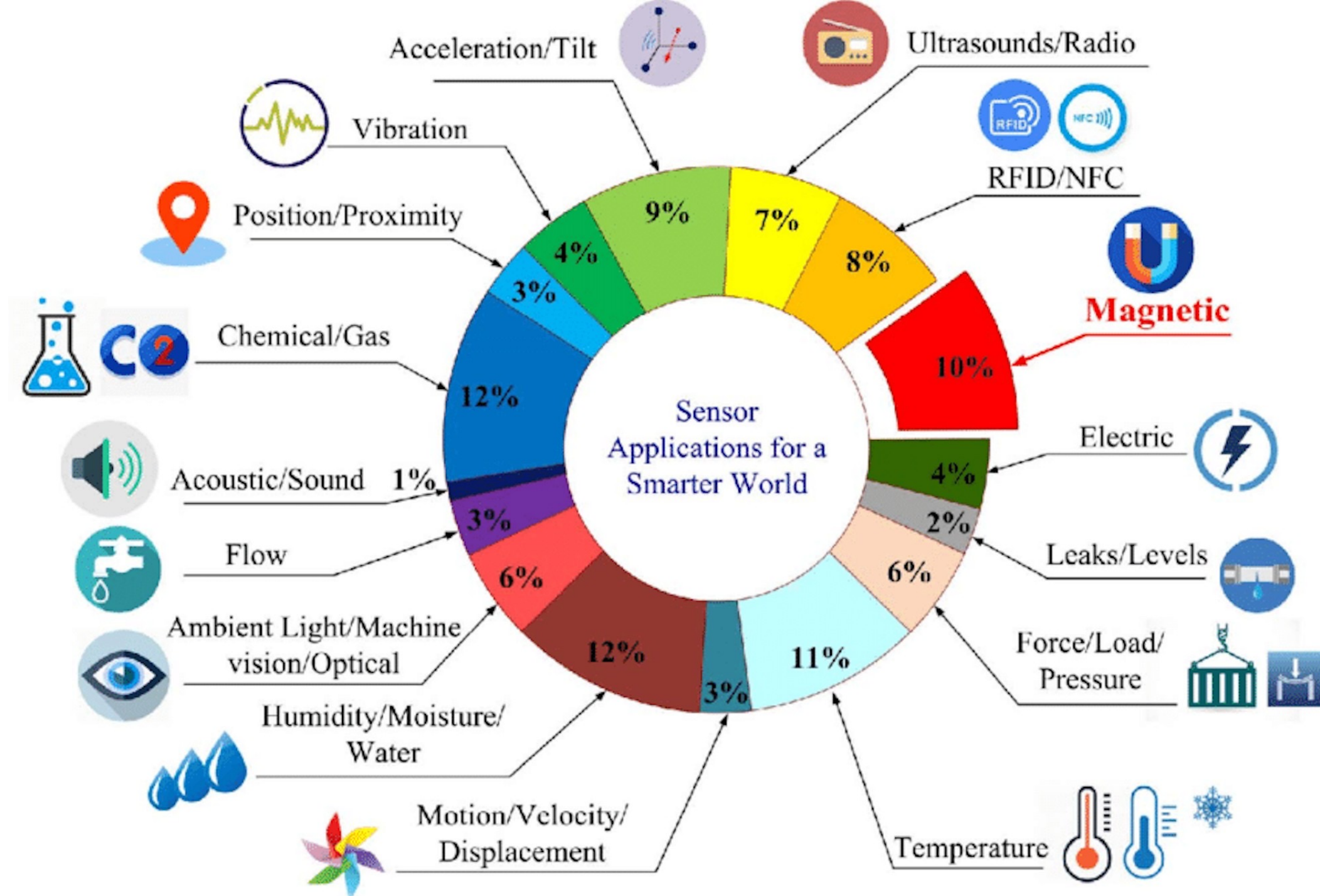
Device security. Modern manufacturers of IoT devices typically integrate security features both in the hardware and firmware installed on it. This includes

- embedded TPM (Trusted Platform Module) chips with cryptographic keys for authentication and protection of endpoint devices;
- a secure boot process that prevents unauthorized code from running on a powered-up device;
- updating security patches on a regular basis; and
- physical protection like metal shields to block physical access to the device.

Connection security. Whether data is being sent over devices, networks, or applications, it should be encrypted. Otherwise, sensitive information can be read by anybody who intercepts information in transit. IoT-centric messaging protocols like MQTT, AMQP, and DDS may use standard Transport Layer Security (TLS) cryptographic protocol to ensure end-to-end data protection.

Cloud security. Data at rest stored in the cloud must be encrypted as well to mitigate risks of exposing sensitive information to intruders. Cloud security also involves authentication and authorization mechanisms to limit access to the IoT applications. Another important security method is device identity management to verify the device's credibility before allowing it to connect to the cloud.

The good news is that IoT solutions from large providers like Microsoft, AWS, or Cisco come with pre-built protection measures including end-to-end data encryption, device authentication, and access control. However, it always pays to ensure that security is tight at all levels, from the tiniest devices to complex analytical systems.



Sensors

Measure values

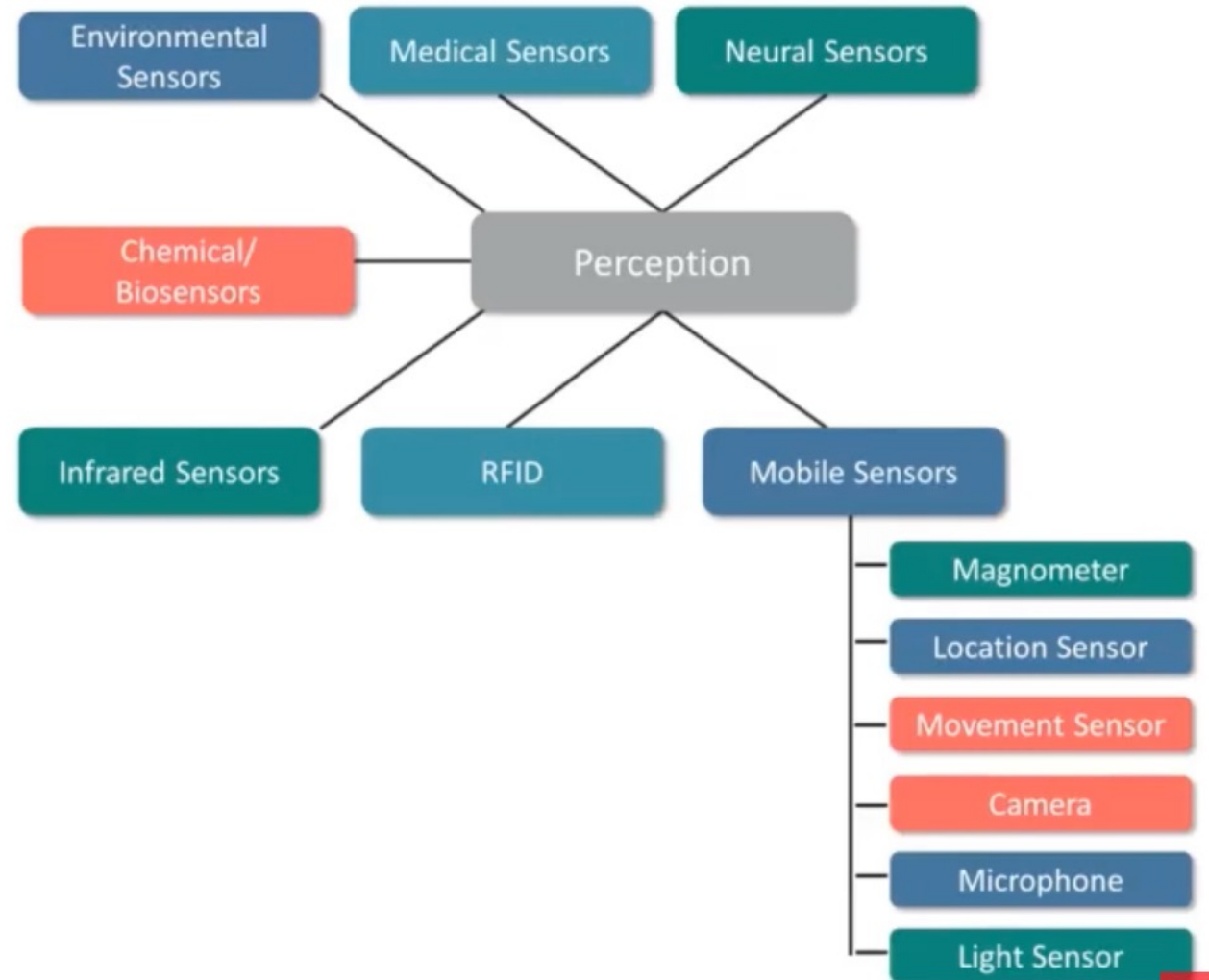
Send raw data

Low power



Perception

- IoT applications need *one* or *more sensors* to collect *data from the environment*
- Sensors are *small in size* , *low cost* & *consumes low energy*
- *Various types of sensors* are *used* in building Smart Application



1.5.4 Sensors

- **Sensors** are technical components for the qualitative or quantitative measurement of **certain chemical or physical variables and properties**, for example, **temperature**, **light** (intensity and color), **acceleration**, **electricity**, and so on.
- The recorded measured values are usually converted into electronic signals. Currently, we are already surrounded by sensors in many places.
- For example, modern automobiles contain hundreds of sensors, for example, rain sensors for windshield wiper systems, crash sensors for air bag release systems, and lane and parking-assist sensors.
- A sensor node's primary function is to collect, preprocess, and transmit sensor data from its environment to other sensor nodes or a base station. Examples of sensor categories include the following:

Location: GPS, GLONASS, Galileo

Biometric: fingerprint, iris, face

Acoustic: microphone

Environmental: temperature, humidity, pressure **Motion:** accelerometer, gyroscope

- Sensor nodes can form Wireless Sensor Networks (WSN) by means of their transmission unit. For example, these are utilized to
 - (i) detect earthquakes, forest fires, avalanches, as well as terrorist attacks;
 - (ii) monitor vehicle traffic, particularly in tunnels;
 - (iii) track the movements of wild animals;
 - (iv) protect property;
 - (v) operate and manage machines and vehicles efficiently;
 - (vi) establish security areas;
 - (vii) monitor supply chain management; and
 - (viii) discover chemical, biological, and radiological material.

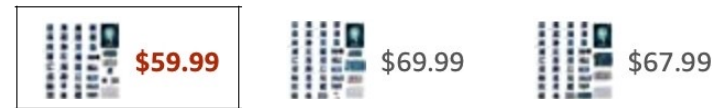
SunFounder Ultimate Sensor Kit for Arduino R3 Mega2560 Mega328 Nano - Including 98 Page Instructions Book

Visit the [SunFounder Store](#)

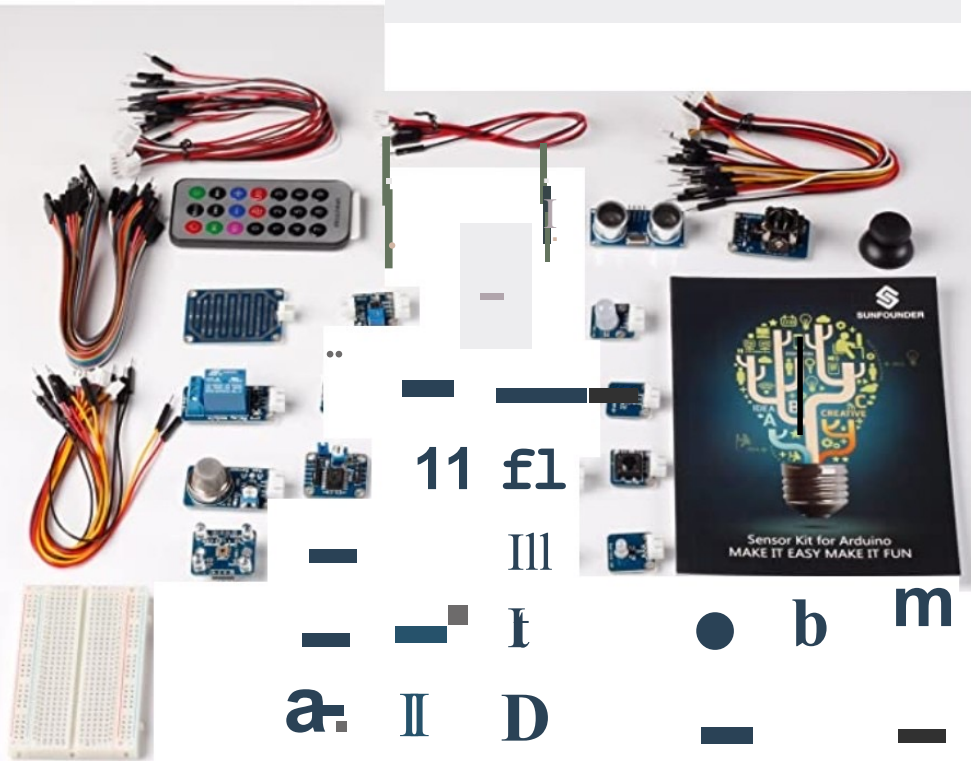
4.2 212 ratings | 42 answered questions

Price: **\$59.99** + No Import Fees Deposit & \$21.68 Shipping to Bahrain [Details](#)

Color: **Sensor Kit**



- Premium SunFounder kit of up to 37 self-designed sensor modules for you to learn basic knowledge for Arduino and sensors.
- With detailed user manual containing 35 projects, covering description and breadboard images; provides code, Fritzing images, datasheets, and so on.
- The user manual [PDF] can be downloaded from Technical Specification in the Product Information.
- Well-designed case for with 8 grids for storing the components by category; with anti-reverse cables {pin socket soldered on the modules}.
- The R3 control board is not included



Roll over image to zoom in

1.5.5 Actuators

- Actuators convert electrical signals (e.g., commands emanating from the control computer) into mechanical motion or other physical variables (e.g., pressure or temperature), and thus actively intervene with the control system and/or set variables.
- In the field of measurement and control engineering, actuators are the signal-related counterparts to sensors. Types of actuators include hydraulic, pneumatic, electric, mechanical, and piezoelectric. They convert signals or setting and regulation specifications of a control into (mostly) mechanical work.

- A simple example of this is the opening and closing of a valve, for example, in a heating system or in the case of engine controls. The output of optical (via displays) or acoustic signals can also be subsumed under actuators, since they can trigger an effect in the real environment. In robotics, the term *effector* is often used as an equivalent for actuators. Effectors allow a robot to grasp and manipulate objects, and thus produce an effect.
- In a computerized world of things, actuators play an increasingly important role in the realization of actions and effects as a counterpart to the (previously) sensory-detected corresponding contexts. Actuators are a key building block in more recent perceptions of the “Fourth Industrial Revolution” in manufacturing as an Industry 4.0 conceptualization postulate.

1.5.6 Power Supply

- A very limiting factor of the mobility of smart objects **is their energy supply**. **Although batteries are becoming smaller and more powerful, today's mobile devices still have very limited battery capacities.**
- The heavy research on improved battery technologies has only produced relatively mild progress in battery performance. In fact, it is continually falling behind other relevant technological developments.
- To counteract these challenges, several avenues of research are being pursued, including intelligent designs that require less battery power.

- This can be achieved by departing from the idea that everything has to be online all of the time. Sometimes, it is sufficient to only occasionally know about a status shift of an object.
- This can be communicated with much less relative effort and demand on bandwidth and energy. Another strategy is to harvest energy “on the fly.” The development of technologies for the utilization of alternative sources of energy, such as the sun, wind, and water is progressing rapidly, partly due to political pressure.
- Moreover, approaches to extracting energy from the external sources of solar, thermal, piezoelectric, mechanical, and kinetic energy are already established, referred to as *energy harvesting*.

Cloud Computing in IoT

In some system *architectures* the *data processing* is done in a *large centralized fashion* on *cloud*



☞ Cloud centric architecture keeps the cloud at the center, applications above it, and the network of smart things below it

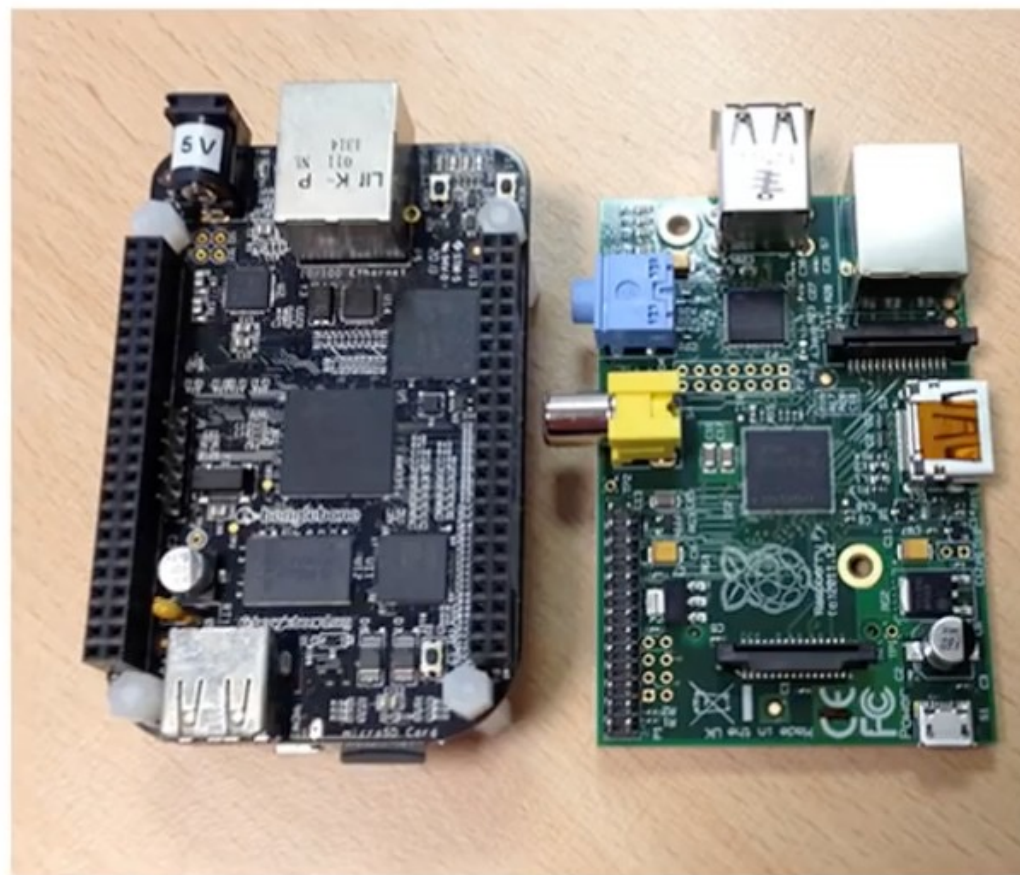
Local Processing and Local Storage

Get data from sensors

Process

Send some data to

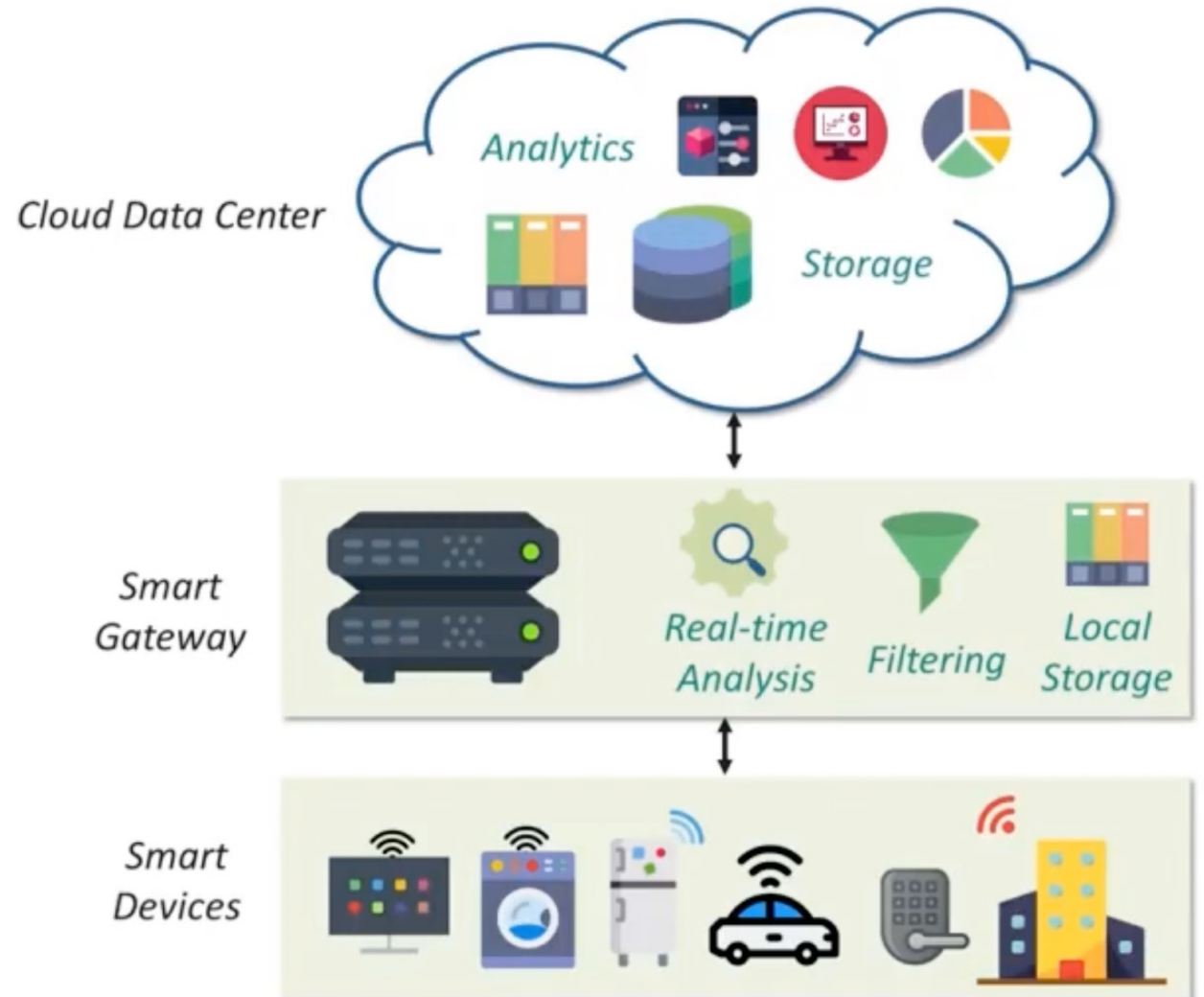
Edge/**Fog** Computing



Pre-processing

Limitations of processing everything in Cloud

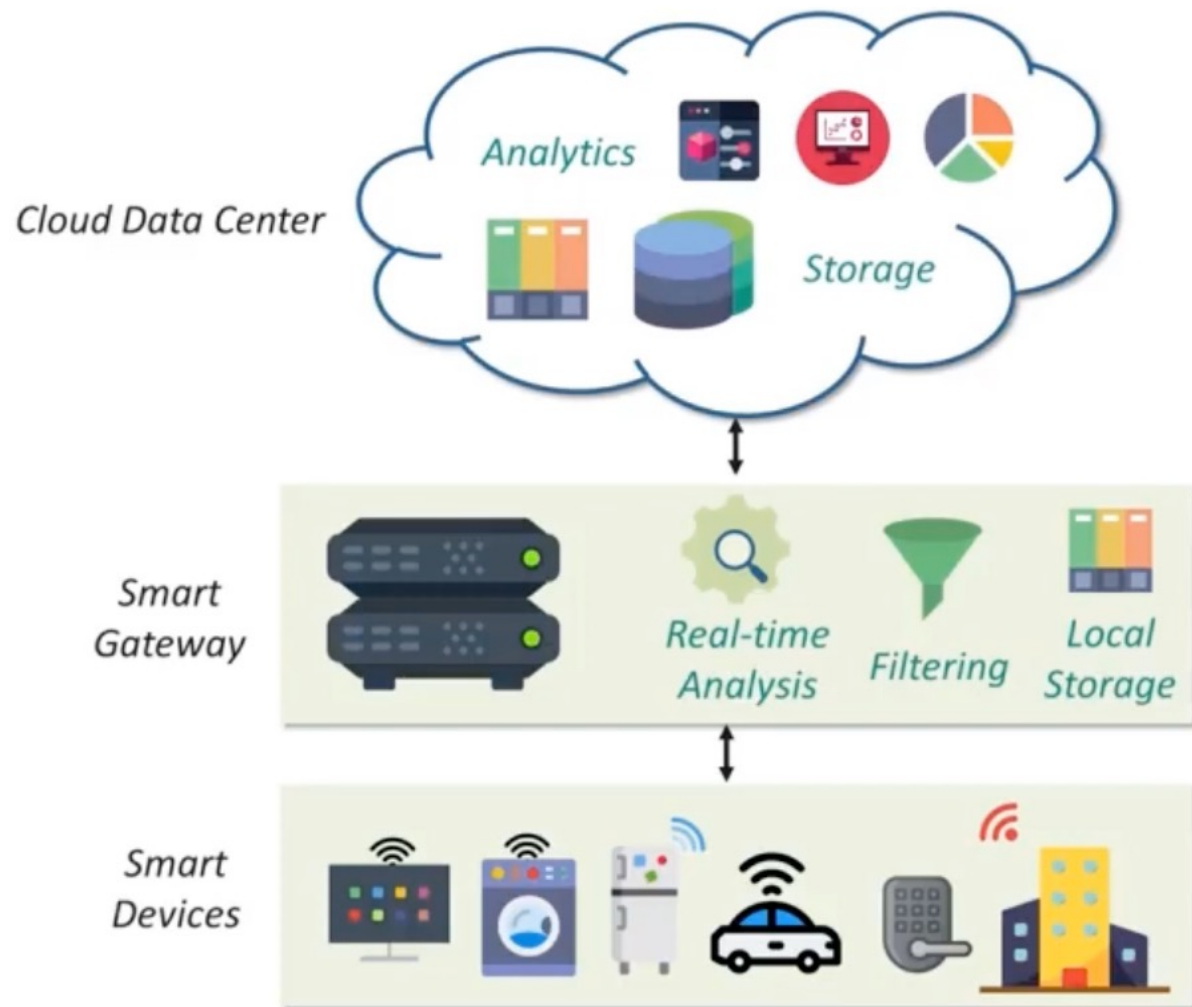
- **Mobility:** Smart devices are mobile & changing network conditions makes communication difficult
- **Reliable & real-time actuation:** Latency sensitive applications need real-time responses.
- **Scalability:** Multiple devices increases the latency



Pre-processing

Features of Fog Computing:

- **Low Latency:** Less time required to access computing or storage resources
- **Distributed Nodes:** Fog nodes are distributed, which provide services to mobile devices
- **Mobility:** Smart devices can communicate to smart gateway present in the proximity.
- **Real-time Response:** Applications with high latency requirements receive real-time response from fog nodes
- **Interaction with Cloud:** The data which needs high processing is sent to cloud



Cloud Computing and Fog Computing

Cloud computing is a concept in which computing performance, storage, software, and other services are provided as a group of virtualized resources over a network, primarily the Internet.

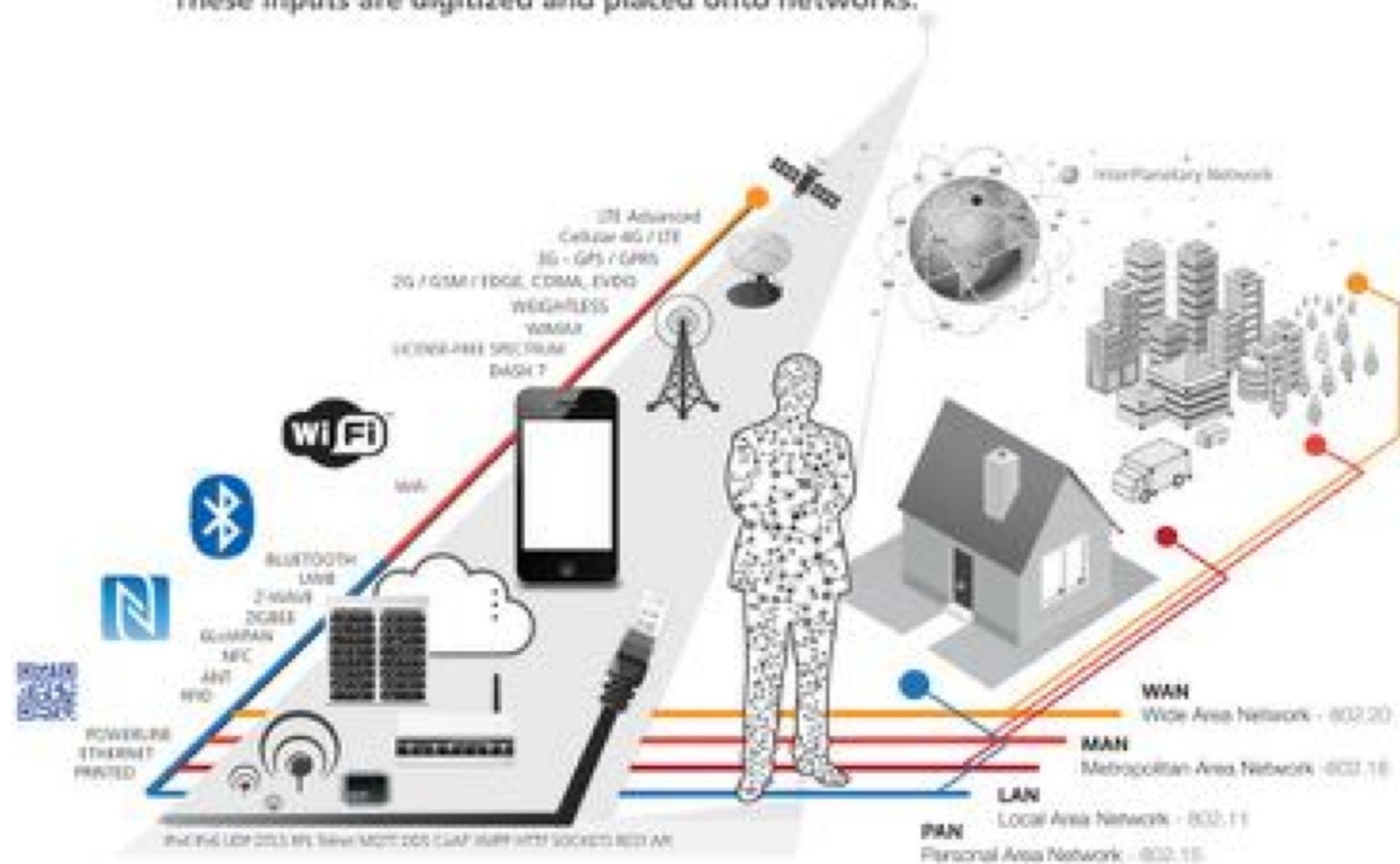
In addition to this, the “Cloud” of resources can be accessed at any time from any connected device and site.

In principle, Cloud computing achieves excellent results in terms of networking resources and storing and accessing data related to or derived from connected things.

- Fog computing, as a highly virtualized platform, provides computing, storage, and networking services between end devices and traditional cloud computing data centers that are typically, but not exclusively, located at the edge of a network.
- Focusing more on the “edge of the network,” however, implies a number of characteristics that make fog computing a nontrivial extension of cloud computing.
- Fog computing is expected, for example, to deal with widely distributed and mobile deployments in which very large numbers of nodes are involved, for example, fast-moving and large groups of vehicles along highways or large-scale sensor networks to monitor the environment).

2 CONNECTIVITY

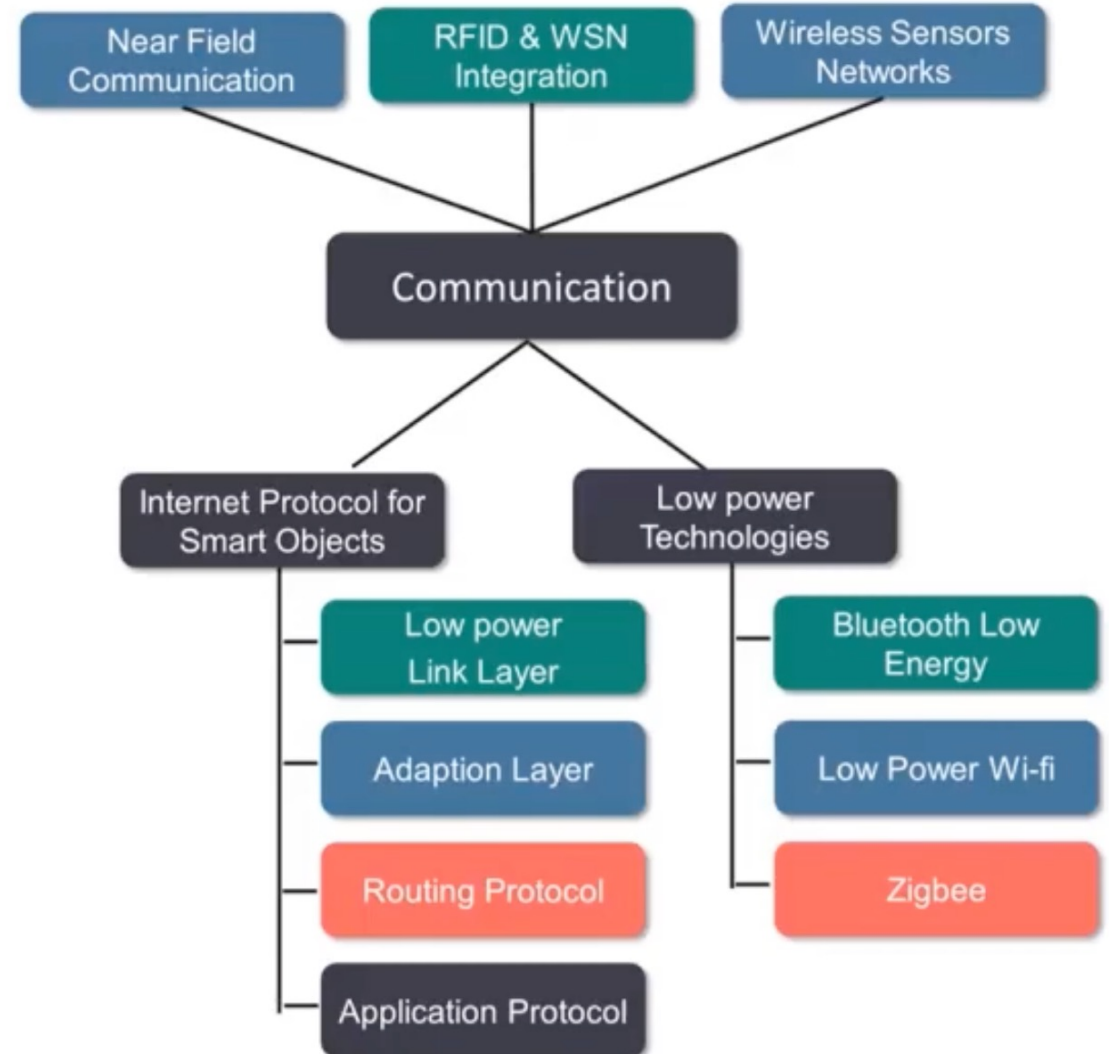
These inputs are digitized and placed onto networks.



Communication

Communication challenges which needs to be addressed:

- *Addressing & Identification*: Each smart device needs to be identified with a unique address in the network
- *Low Power Communication*: Communication between devices needs to be low power consuming
- Routing protocol with low memory requirement & efficient communication protocol
- High speed & Lossless communication



Wireless Body Area Networks (WBANs)



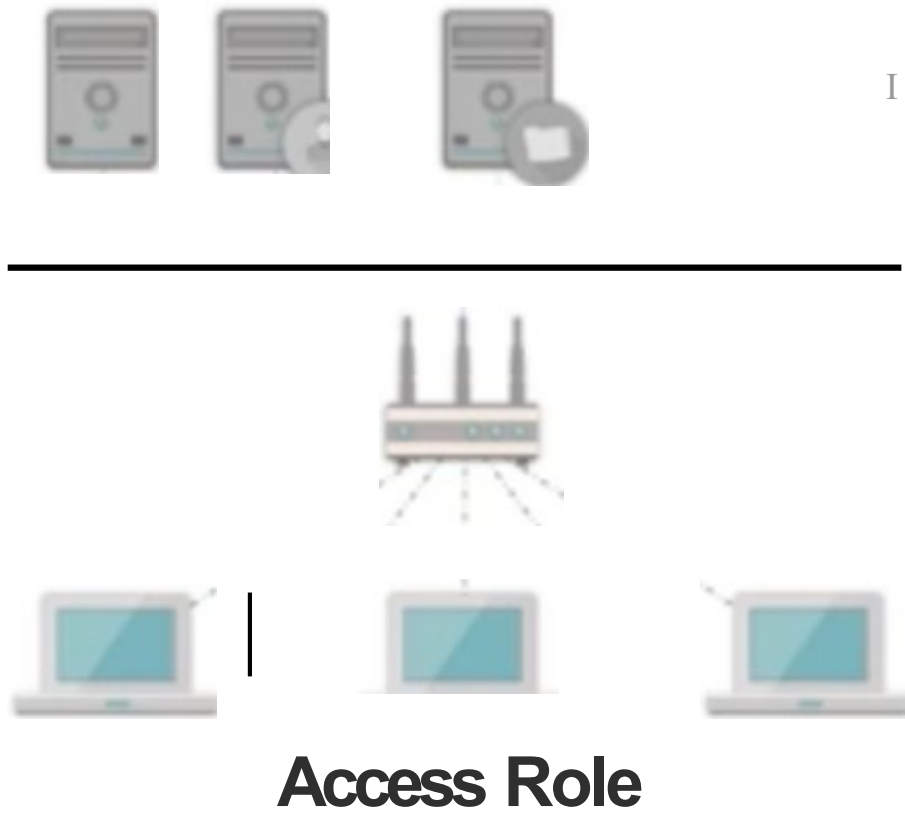
- Also called:
 - Body Area Network (BAN)
 - Medical Body Area Network (MBAN)
 - Body Sensor Network (BSN)
- 10 cm to 1 m range
- Includes:
 - Bluetooth
 - NFC
 - RFID
 - Proprietary

Wireless Personal Area Networks (WPANs)



- 1 m to 10 m range
- Includes:
 - Bluetooth
 - RFID
 - Proprietary

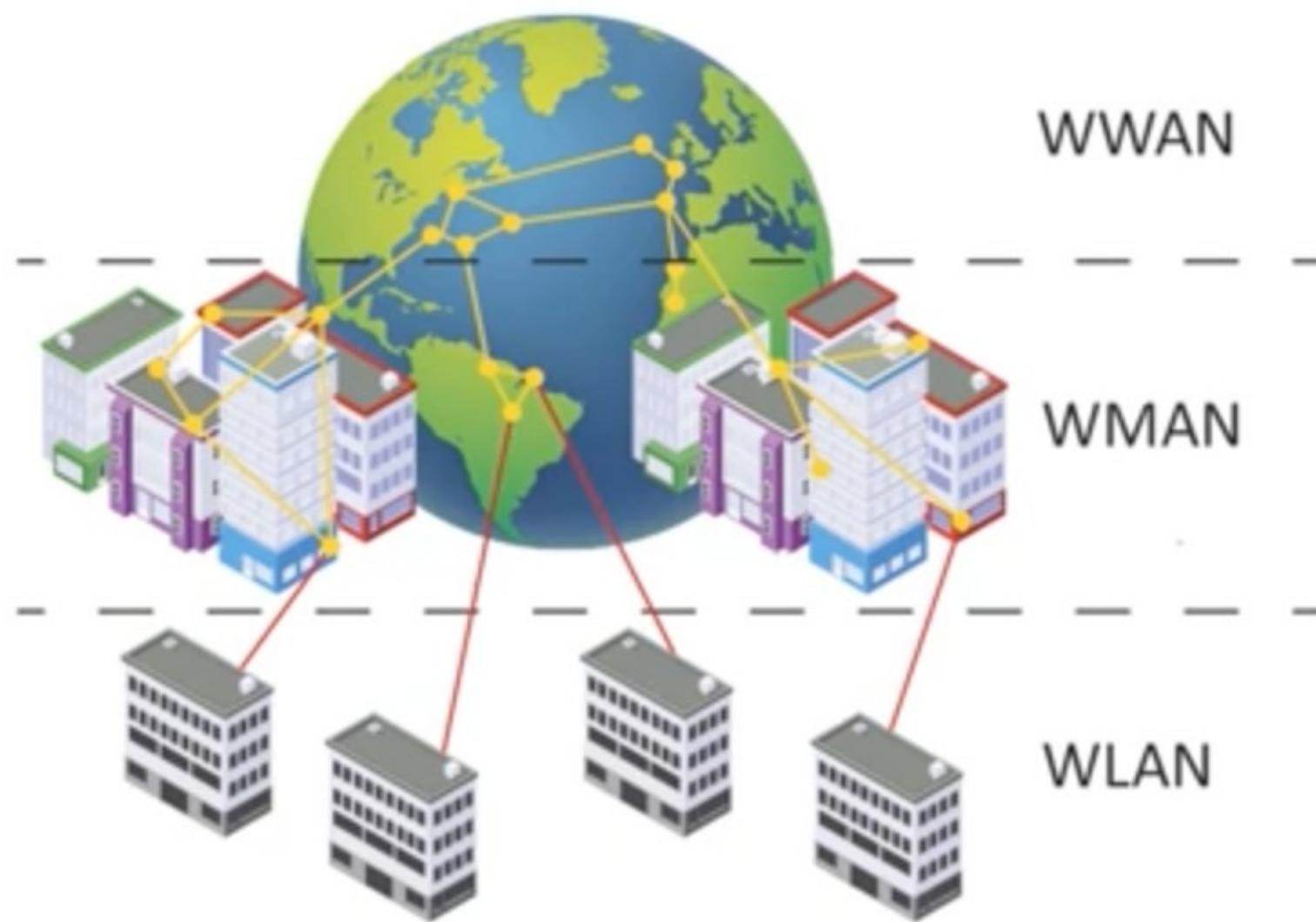
Wireless Local Area Networks (WLANs)



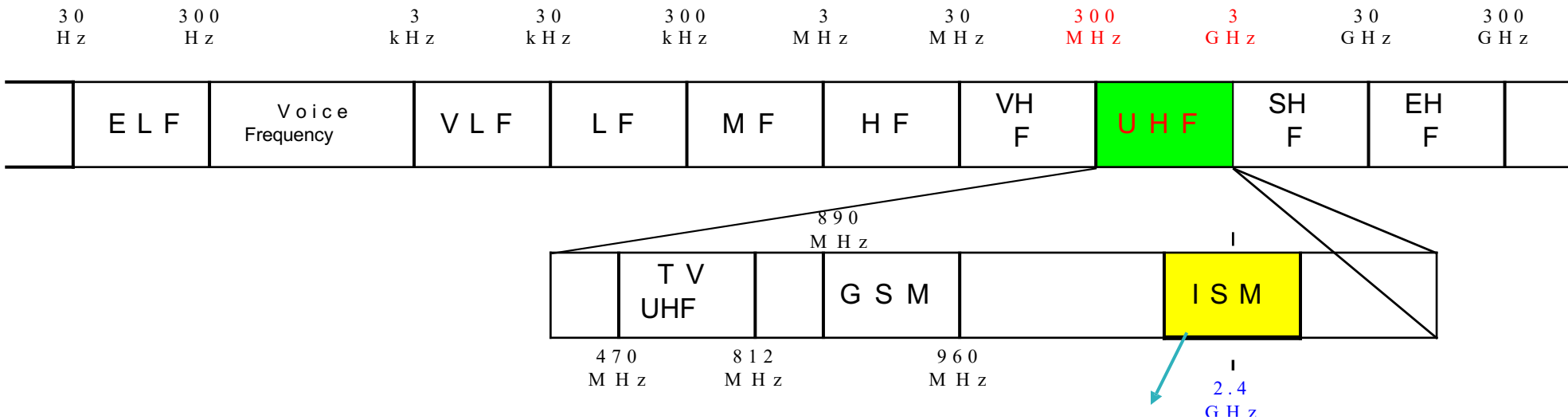
Wireless Metropolitan Area Networks (WMANs)



Wireless Wide Area Networks (WWANs)



Frequency Allocation



Note: The **Industrial, Scientific and Medical (ISM)** radio bands were originally reserved internationally for non-commercial use of RF electromagnetic fields for industrial, scientific and medical purposes.

In recent years they have also been used for license-free error-tolerant communications applications such as Bluetooth and IEEE 802.11b

2–Standard for 5.2 GHz NII band (300 MHz)

–**Unlicensed National Information Infrastructure (U-NII)** band , USA

ENERGY



SAFE and BENEFICIAL
IN APPROPRIATE
DOSAGE *

ALMOST SAFE,
LOW DANGER

DANGER

SAFE and BENEFICIAL
IN APPROPRIATE
DOSAGE *

EXTREMELY HARMFUL



ELF

VLF

LF

RADIOFREQUENCIES

MICROWAVES

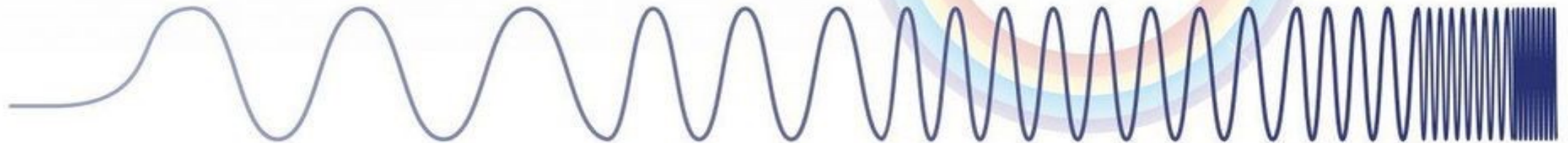
INFRA-RED

VISIBLE

ULTRAVIOLET

X-RAY

GAMMA RAYS



FREQUENCY

50 Hz

1 MHz

500 MHz

1 GHz

10 GHz

30 GHz

600 THz

3 PHz

300 PHz

30 EHz

WAVELENGTH

6000 km

300 m

60 cm

30 cm

3 cm

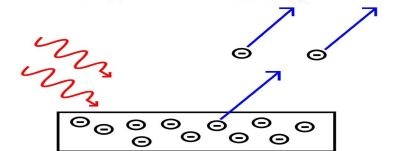
10 mm

500 nm

100 nm

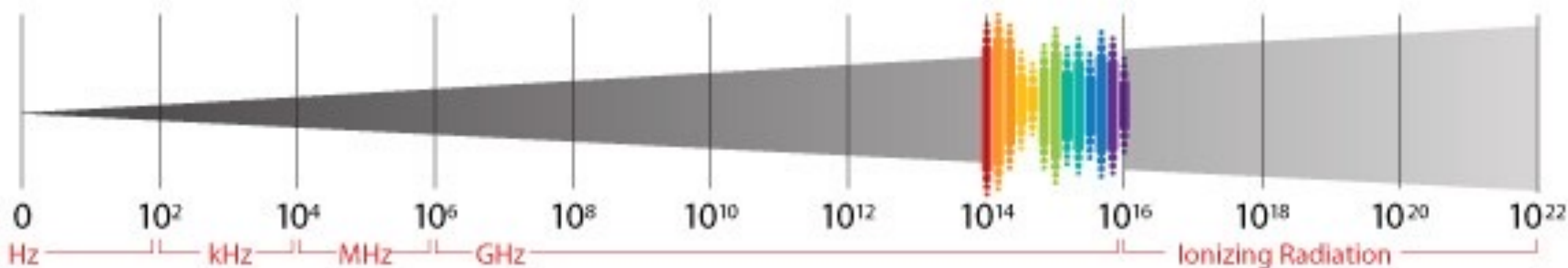
1 nm

10 pm



Electromagnetic Spectrum

Frequency (Hz)



Direct Current

Extremely Low Frequency

Low Frequency

Radiowaves

Microwaves

Infrared Radiation

Visible Light

Ultraviolet Radiation

X-rays

Gamma Rays



Computer
60–100 Hz



Radio
AM 520–1610 kHz
FM 87.5–108 MHz



Cell Phone UMTS
1.9–2.2 GHz



Microwaves
3–30 GHz



Remote Control
5.8 GHz



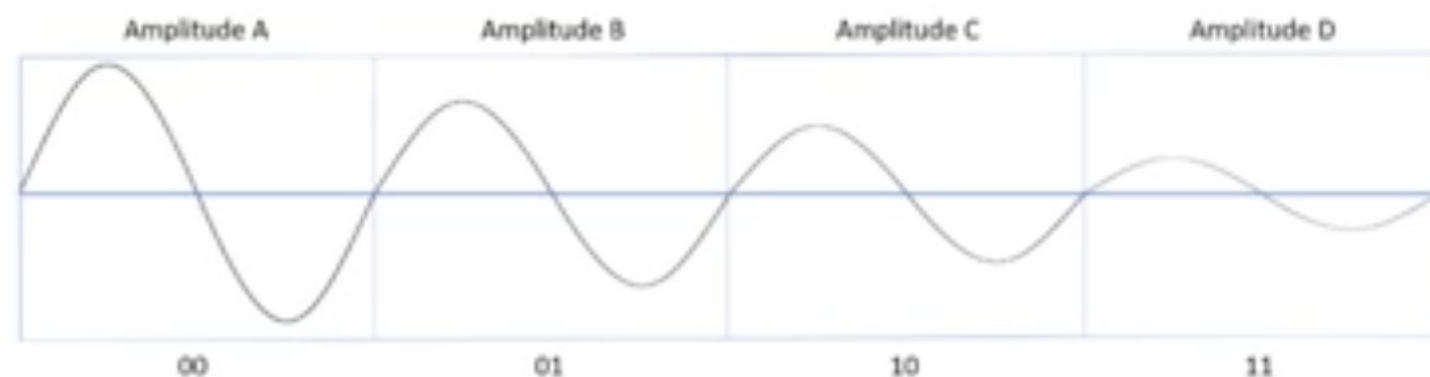
Ultraviolet
UVA and UVB



X-rays
range from
 30×10^{16} Hz
to 30×10^{19} Hz

RF and Speed

- Modulation
- Coding
- Channel Bandwidth
- SNR/SINR
- Spatial Streams

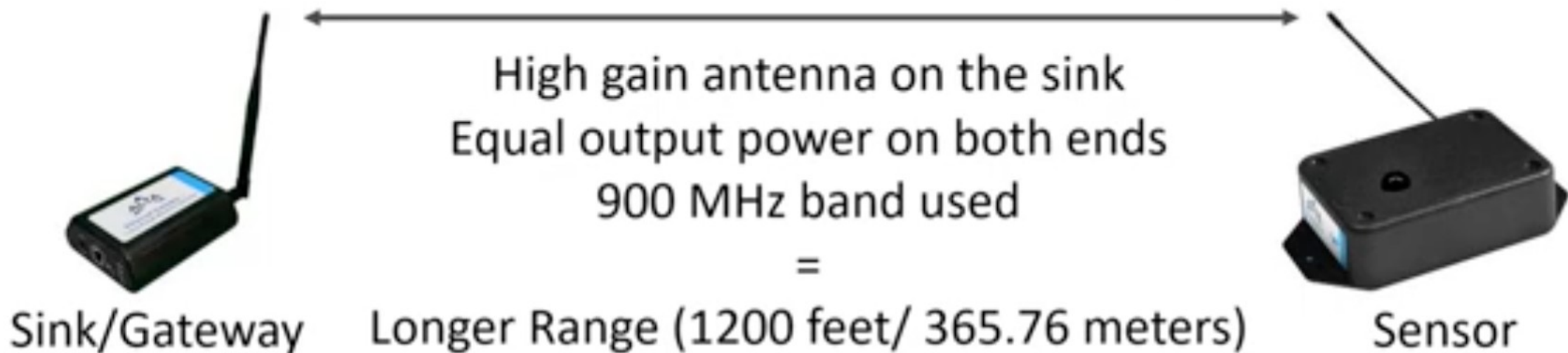
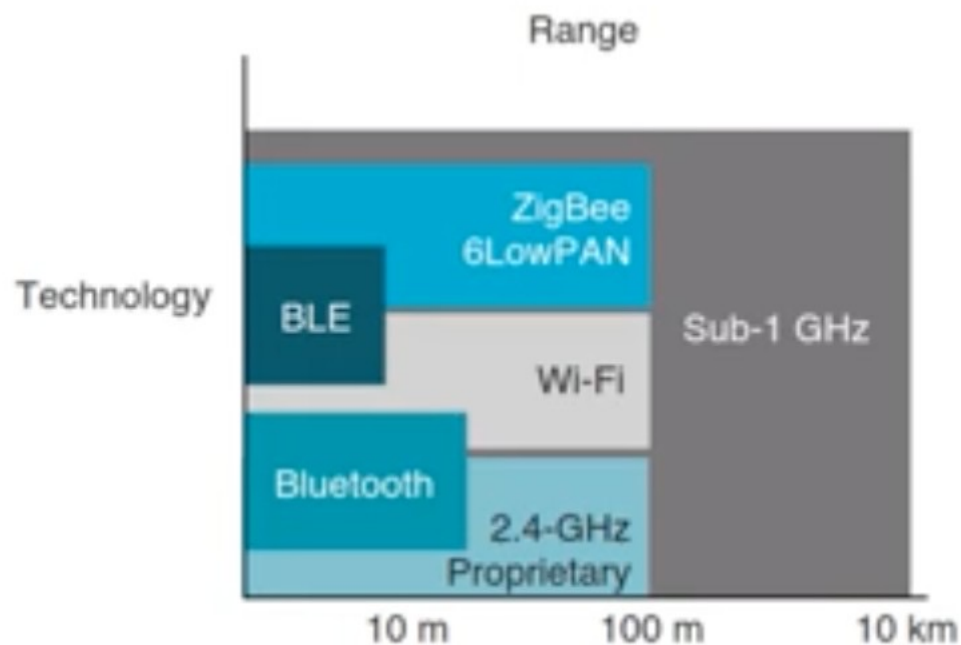


Low-rate wireless can be beneficial in the following situations:

- **Noisy environments:** environments with limited SNR require the use of less complex, and therefore slower, modulation methods.
- **Long-range communications:** longer distances result in weaker signals at the receivers and may require slower modulation methods.
- **Limited frequency bandwidth available:** narrower channels have fewer carriers and require slower data rates even with more complex modulation methods.

RF and Range

- Output power
- Frequency band
- Antennas
- Desired performance



RF and Power

- Low-Power Wireless = Low output power
- Low-Power Consumption = Power management

Low-Power Wireless Solutions

- Bluetooth Low Energy (BLE) (100 meters/500 meters with version 5)
- Near Field Communication (NFC) (10 centimeters)
- ZigBee (100 meters)
- ANT – a proprietary protocol (30 meters)
- Wi-Fi (distance based on output power and antennas)

Power Consumers

- Radio components
- CPU/ASIC
- Local storage
- Wired ports
- Additional interfaces





Wireless Communications Technologies for IoT

1. Cellular phone
2. Wireless LAN, WIFI
3. Wireless MAN, WIMAX
4. Bluetooth
5. Zigbee
6. 6LOWPAN
7. LORA / LORAWAN
8. NB-IOT and LTE-M

Cellular communications

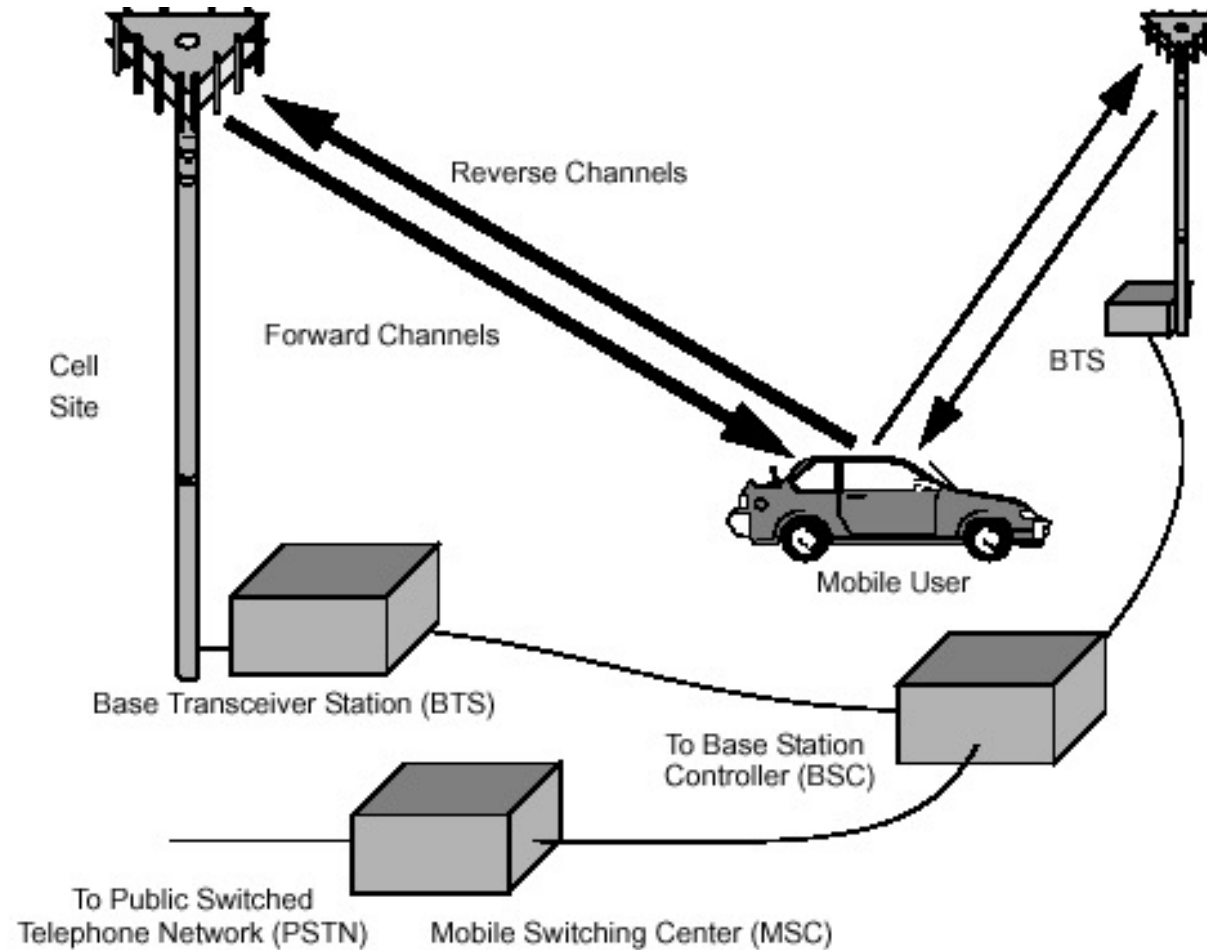


Figure 1-3 There are two main types of forward channels. Control and access channels are used to set up calls and provide security and management functions. Traffic channels are used to carry voice traffic. The reverse channels are also divided into access channels and traffic channels. In some systems, the Base Station Controller (BSC) may be integrated directly into the cell site. In other systems, as shown here, the Base Transceiver Stations (BTSs) are connected to a Base Station Controller.

Cellular Architecture



IoT Device



IoT Gateway (Wi-Fi, Proprietary, etc.)

Gateway Connect Model



Cellular Network

Direct Connect Model



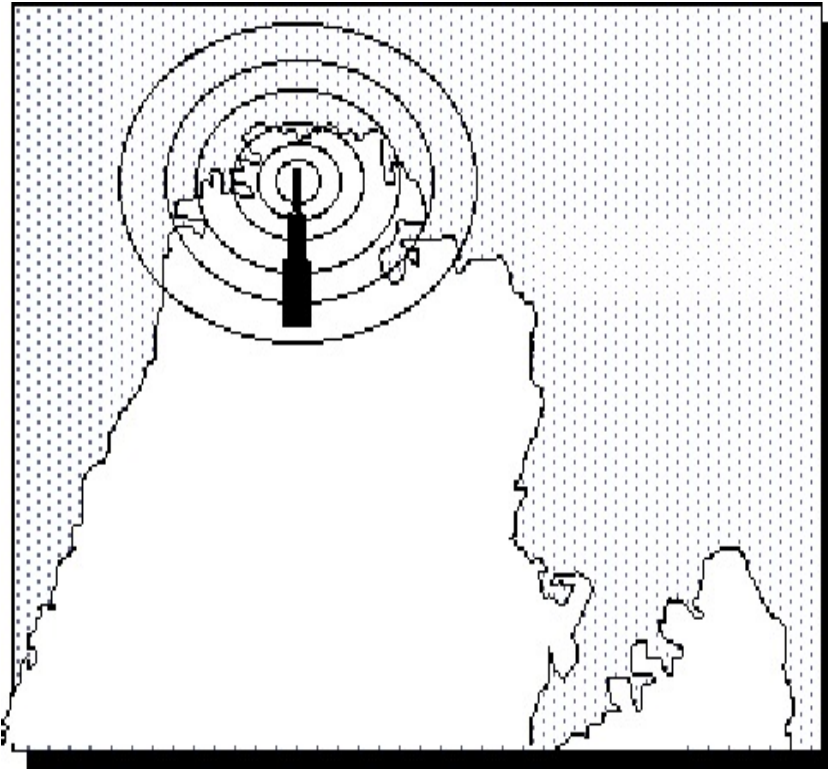
2G/3G/4G:

- There are different generations of mobile communication standards.
 - 2G including GSM and CDMA,
 - Third generation that is, 3G including UMTS and CDMA 2000.
 - Fourth generation that is, 4G including LTE.
- IoT devices based on these standards, can communicate over cellular networks.

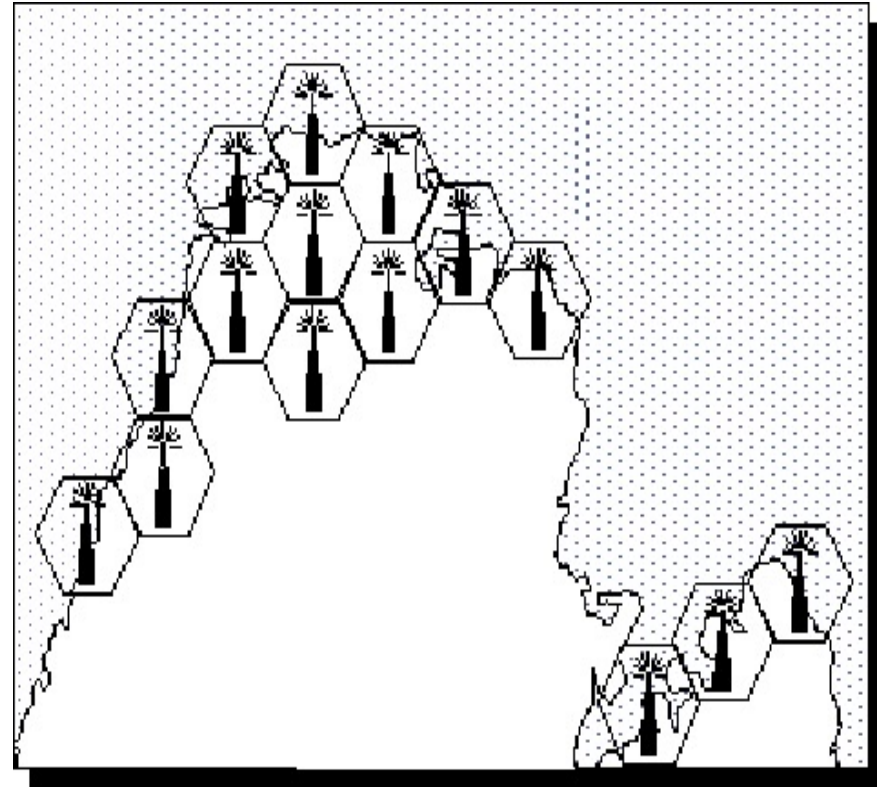


Cellular Telephone Systems

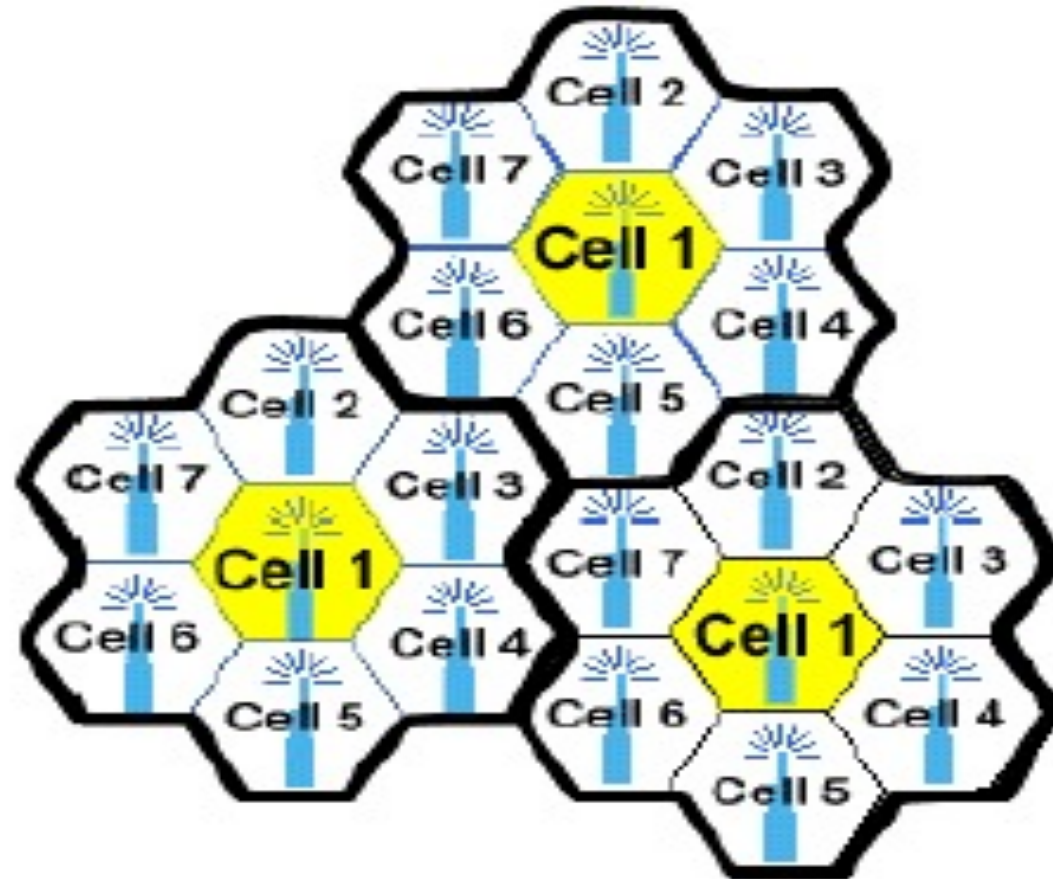
Early Mobile Telephone System Architecture



Mobile Telephone System Using Cellular Architecture



Frequency Reuse



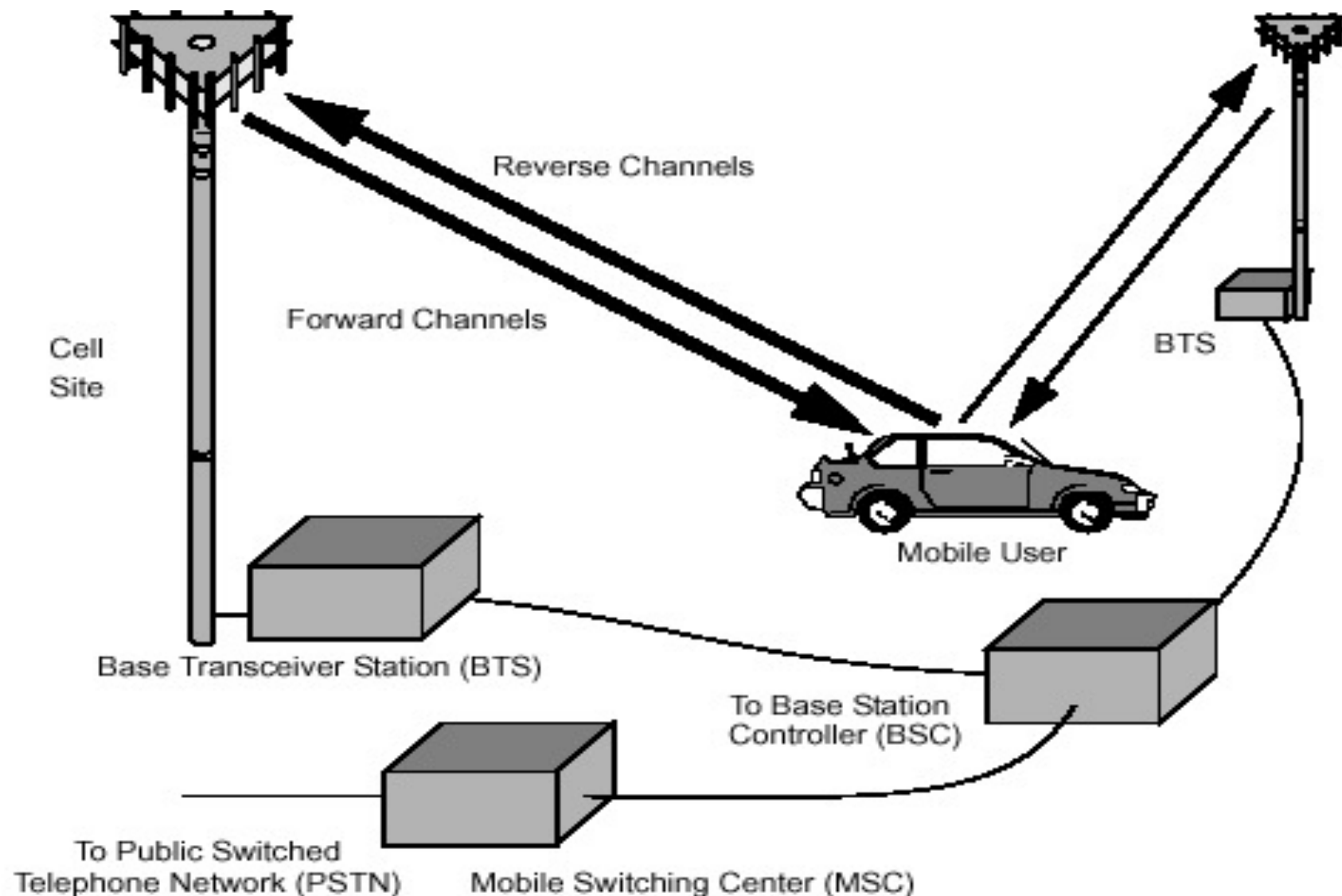
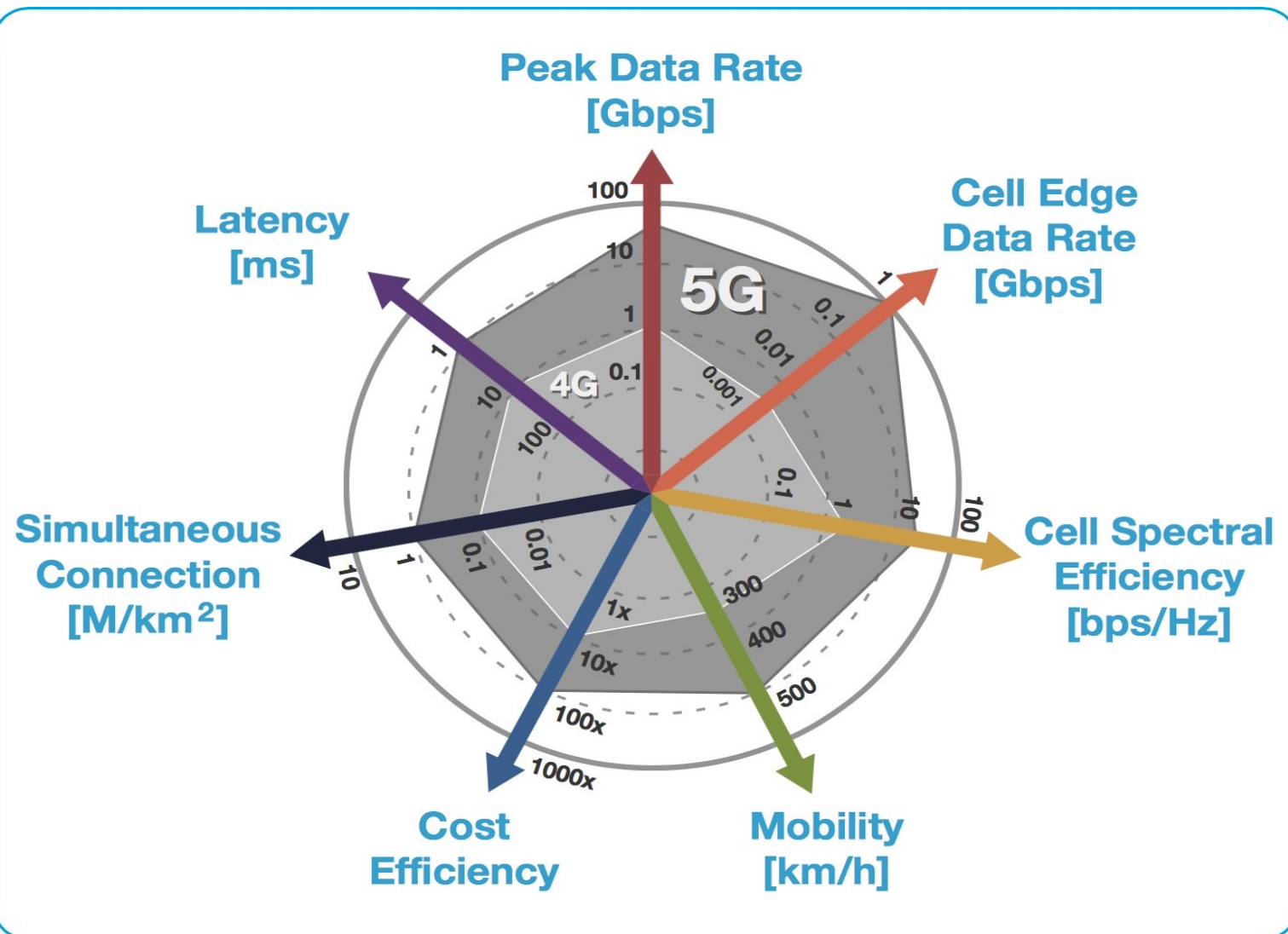


Figure 1-3 There are two main types of forward channels. Control and access channels are used to set up calls and provide security and management functions. Traffic channels are used to carry voice traffic. The reverse channels are also divided into access channels and traffic channels. In some systems, the Base Station Controller (BSC) may be integrated directly into the cell site. In other systems, as shown here, the Base Transceiver Stations (BTSs) are connected to a Base Station Controller.

5G

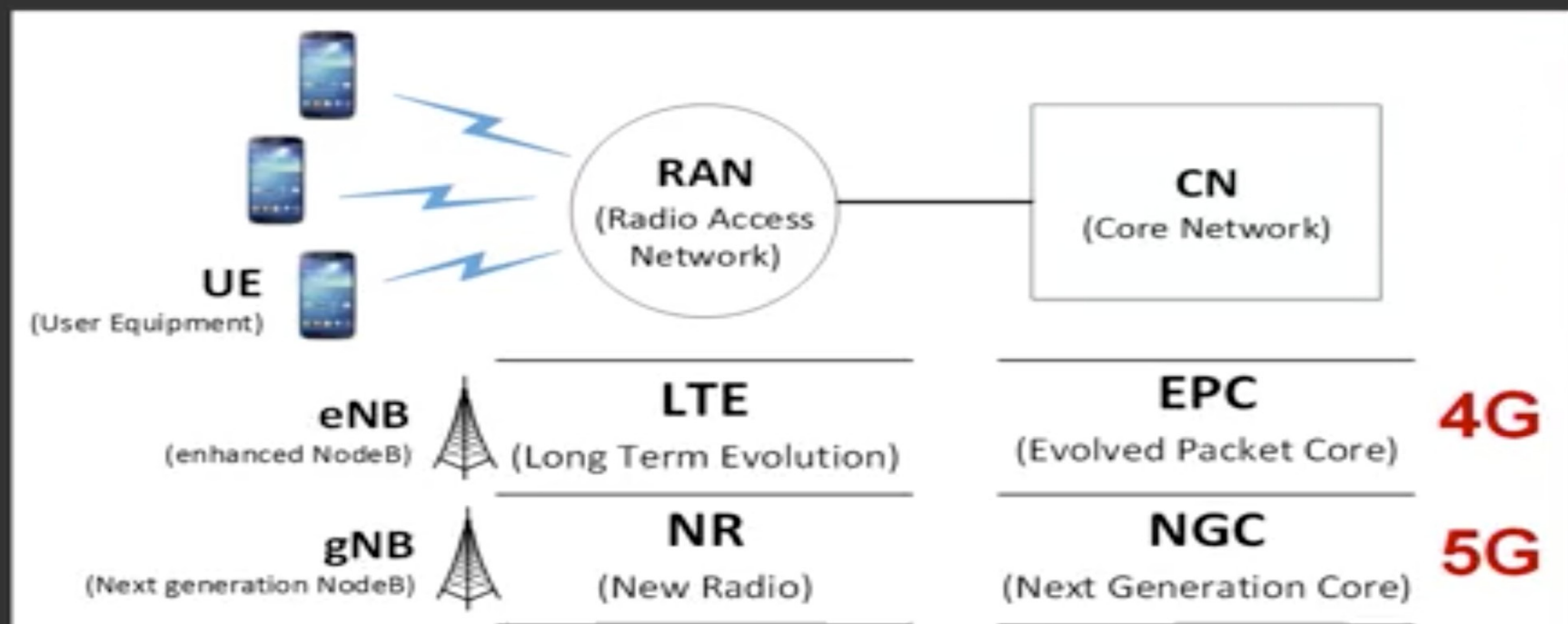


2G : digital voice, 3G : first data services, 4G : mobile broadband
5G : designed to serve not only phones but for connecting everything

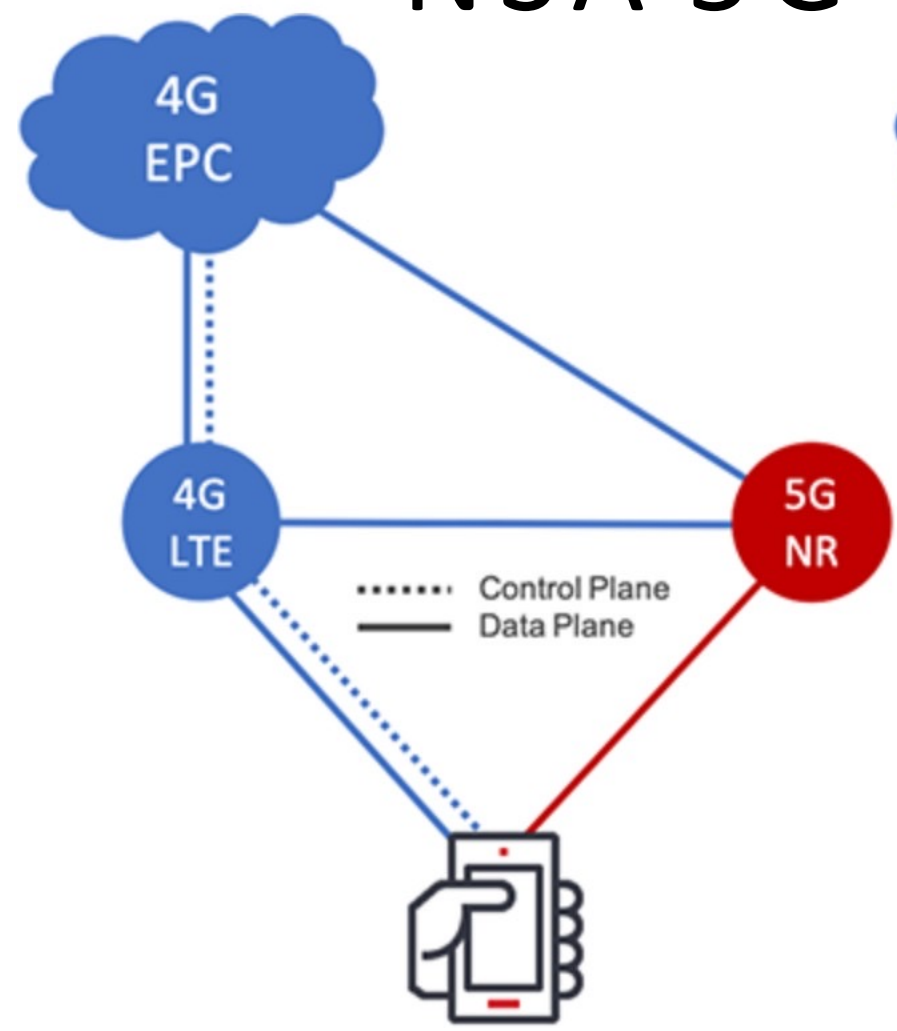
(5G Isn't About the Smartphone @ IEEE Spectrum March 2019)

5G Architecture

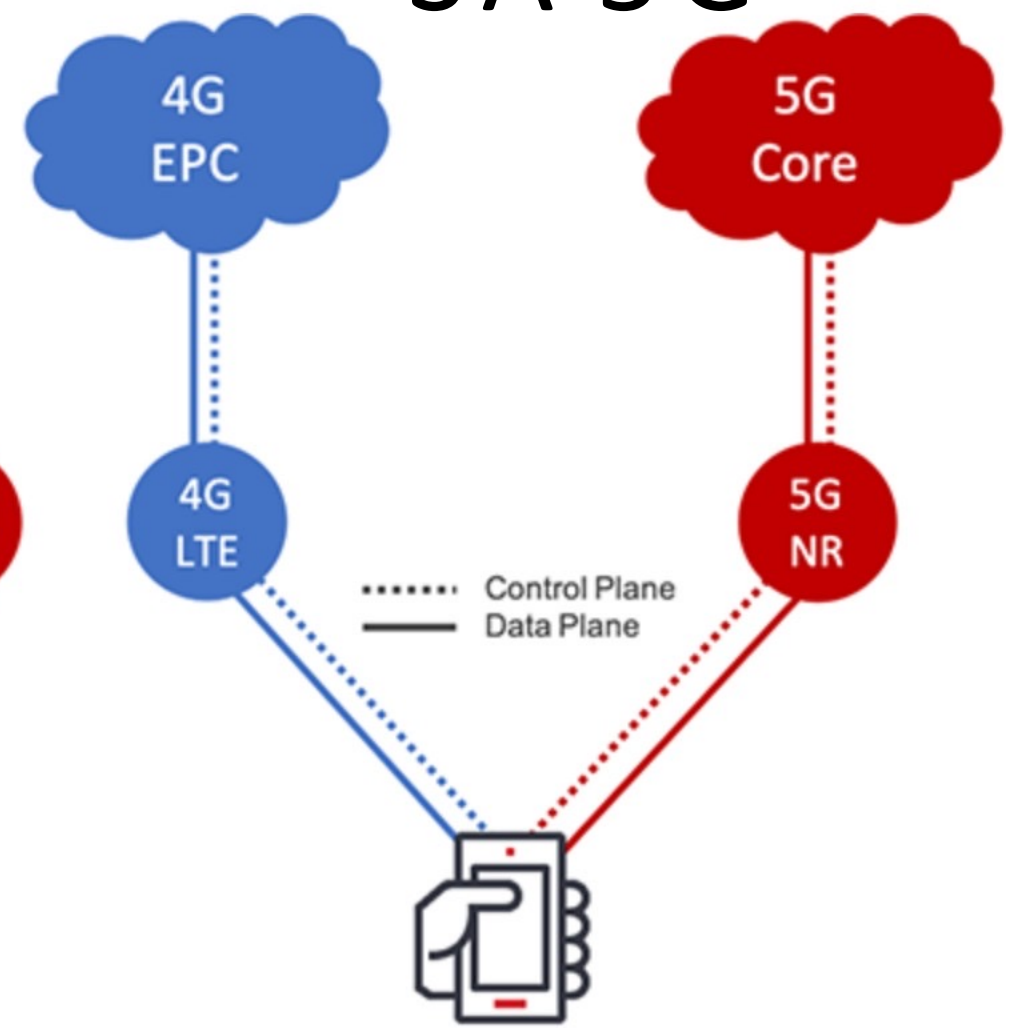
❖ Cellular Network Architecture



NSA 5G



SA 5G

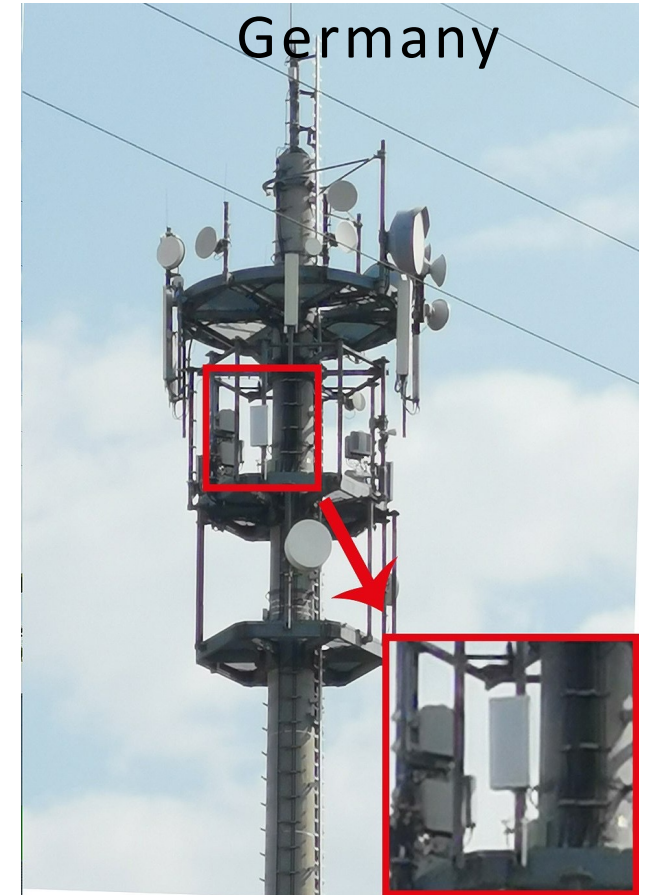




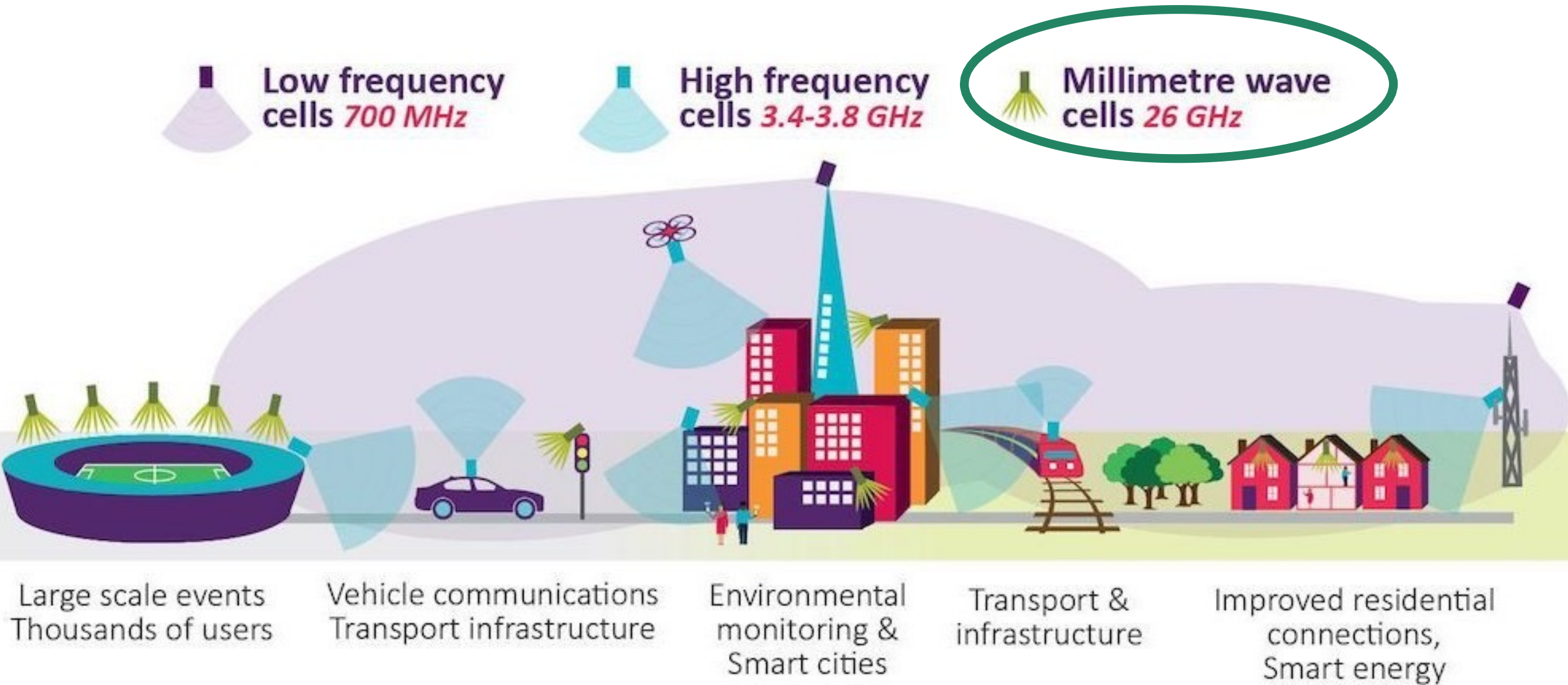
5G 3.5 GHz Cell Site of Deutsche Telekom in Darmstadt, Germany



5G 3.5 GHz Cell Site of Vodafone in Karlsruhe, Germany



5G NR (New Radio) is a new radio access technology (RAT) developed by **3GPP** for the **5G** (fifth generation) mobile network. It was designed to be the global standard for the air interface of **5G** networks. ... **gNB** (i.e. a 5G next generation base station), **NSA Vs. SA options**



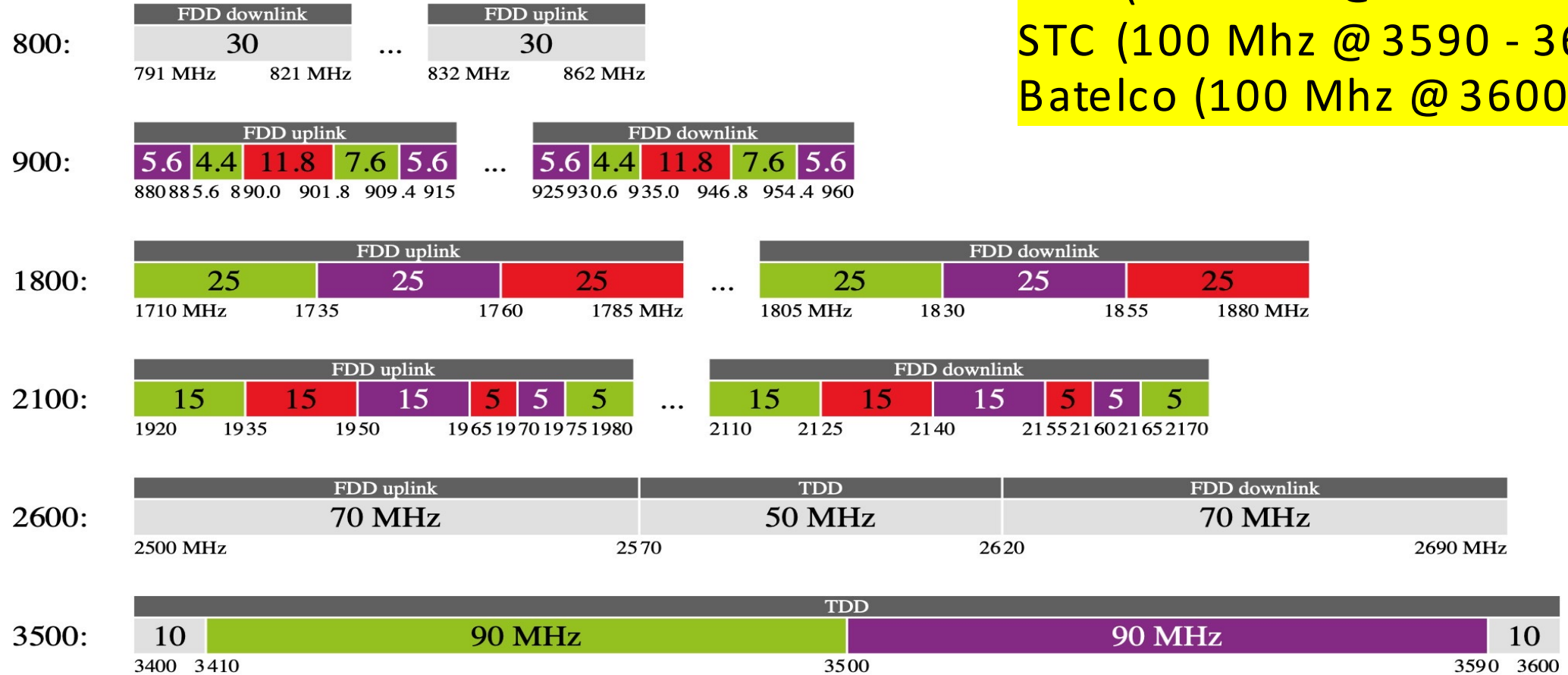
THE millimeter-wave (mmWave) band : is part of the radio frequency (RF) spectrum, comprised of frequencies between 30 GHz and 300 GHz, corresponding to a wavelength range of 10 to 1 mm. The photon energy of mmWaves ranges from 0.1 to 1.2 milli-electron volts (meV). Unlike ultraviolet, X-ray, and gamma radiation, mmWave radiation is non-ionizing, and the main safety concern is heating of the eyes and skin caused by the absorption of mmWave energy in the human body [1][2][3].

5G NR uses two frequency ranges:^[4]

1. Frequency Range 1 (FR1), including **sub-6 GHz** frequency bands
2. Frequency Range 2 (FR2), including frequency bands in the **mmWave** range (**24–100GHz**)

Country or territory	Operator	Band									Notes
		DSS with 4G LTE	n40 2.3 GHz	n41 2.5 GHz	n78 3.5 GHz	n79 4.7 GHz	n257 28 GHz (APAC)	n258 26 GHz (Ei Sort ascending)	n261 28 GHz	Others	
Bahrain	Batelco				90 MHz Jun 2019						[19][20][21]
	stc				90 MHz Jun 2019						[19][22][23]
	Zain				90 MHz Jun 2020						[19][24]
South Korea	LG U+				80 MHz Dec 2018		800 MHz Dec 2018				[1][175][176][177] World's first commercial service
	KT				100 MHz Dec 2018		800 MHz Dec 2018				[1][175][176][177] World's first commercial service
	SK Telecom				100 MHz Dec 2018		800 MHz Dec 2018				[1][175][176][177] World's first commercial service

Zain (100 Mhz @ 3400 - 3410 Band)
 STC (100 Mhz @ 3590 - 3600 Band)
 Batelco (100 Mhz @ 3600 - 3700 Ban



5G vs 4G cells



<https://vividcomm.com/2019/10/04/5g-small-cells/>



 Macro Cell - outdoor
200 [W]

 Micro Cell – outdoor/indoor

 Pico Cell – outdoor/indoor

 Femtocell – indoor

Power



Coverage area	100 meters to 250 meters (indoors)
Power	Typically 250 milliwatts
Number of users	32 to 64 users
Backhaul	Wired, fiber connection
Application	Indoor applications (offices, hospitals, shopping centre and schools)
Cost	Low cost



Coverage area	500 meters to 2.5 kilometers
Power	2 to 5 watts
Number of users	up to 200 simultaneous users
Backhaul	Wired, fiber connection and microwave links
Application	Outdoor applications
Cost	Medium cost



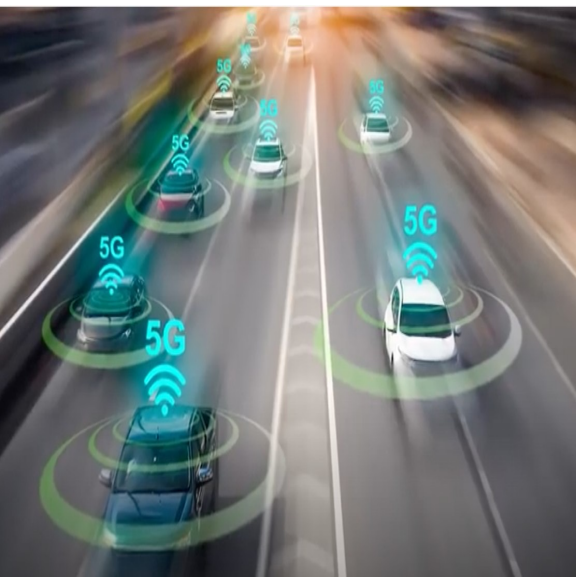
Coverage area	10 meters to 50 meters (indoors)
Power	Typically 100 milliwatts
Number of users	8 to 16 users
Backhaul	Wired, fiber connection
Application	Indoor (primarily for indoor application, can be used for outdoor applications)
Cost	Low cost

4G vs 5G

Performance Metrics	4G	5G
Peak data rate (Gbps)	1	20
User experienced data rate (Mbps)	10	100
Connection density (devices/km ²)	10 ⁵	10 ⁶
Mobility support (kmph)	350	500
Area traffic capacity (Mbit/s/m ²)	0.1	10
Latency (ms)	10	1
Reliability (%)	99	99.99
Positioning accuracy (m)	1	0.01
Spectral efficiency (bps/Hz)	3	10
Network energy efficiency (J/bit) ¹	1	0.01

	3G	3G	4G	5G	
TECH	UMTS	HSPA	LTE/LTE A.	5G NR	URLLC
Latency (ms)	200-400 ms	80-150 ms	15-80 ms	2-5 ms	1-2 ms

4G vs 5G



Performance Metrics	4G	5G
Peak data rate (Gbps)	1	20
User experienced data rate (Mbps)	10	100
Connection density (devices/km ²)	10 ⁵	10 ⁶ (IOT)
Mobility support (kmph)	350	500
Area traffic capacity (Mbit/s/m ²)	0.1	10
Latency (ms)	10	1
Reliability (%)	99	99.99
Positioning accuracy (m)	1	0.01
Spectral efficiency (bps/Hz)	3	10
Network energy efficiency (J/bit) ¹	1	0.01

[IEEE Communications Surveys & Tutorials](#) (Volume: 20 , [12](#) , 2018)



IoT Platforms:

AWS vs Azure vs Google vs IBM vs Cisco

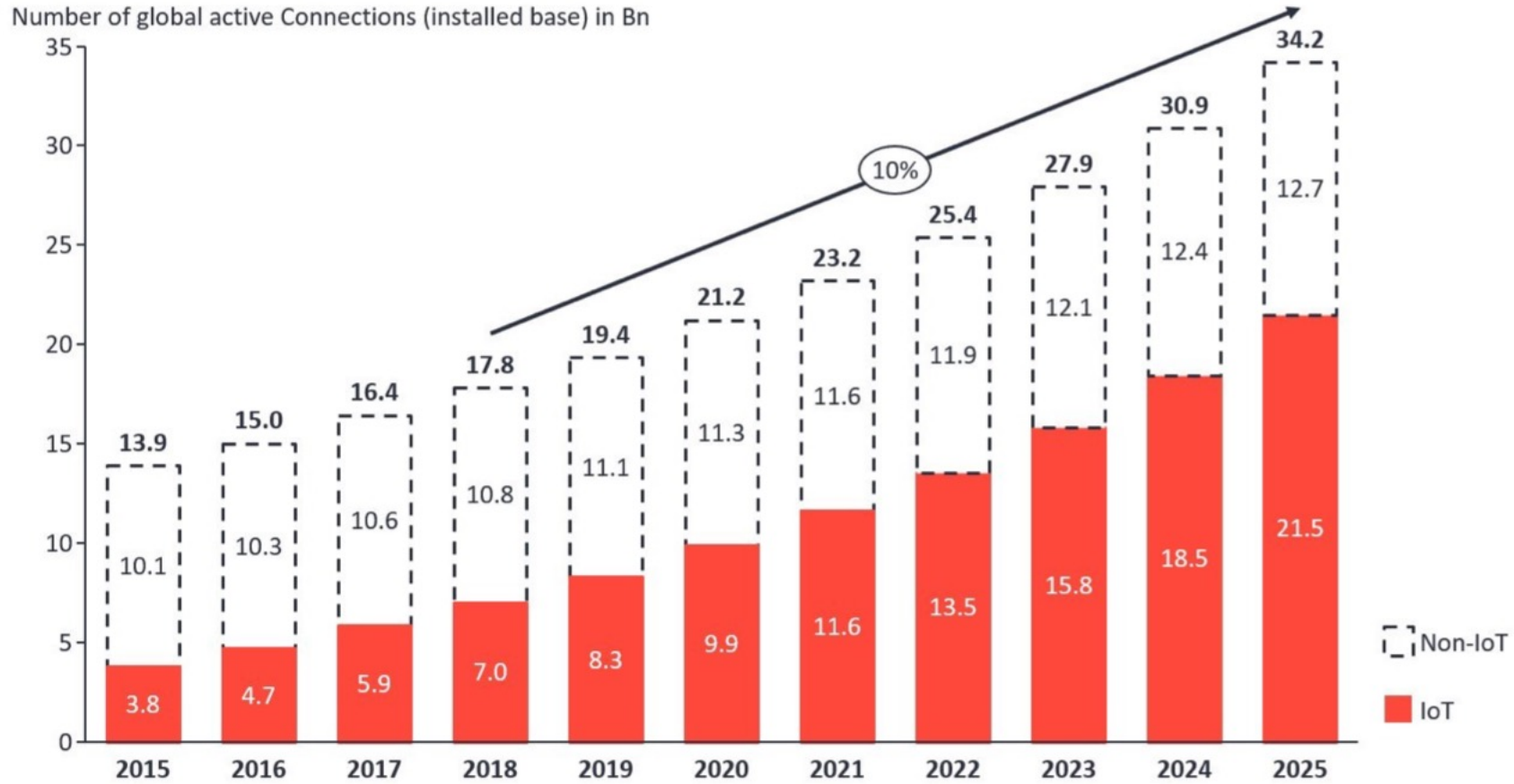
Before you finish reading this Lecture, hundreds of new devices will be connected to the web at a breathtaking pace of 127 additions per minute.

For the most part, they belong to the Internet of Things (IoT), or gadgets capable of communicating and sharing data without human interaction.

The technology will shift into an even higher gear with the arrival of fifth-generation or 5G networks supporting a million gadgets per square kilometer — ten times as many as in the 4G era.

The number of active IoT connections is expected to double by 2025, surging from today's 9.9 billion to 21.5 billion.

Total number of active device connections worldwide

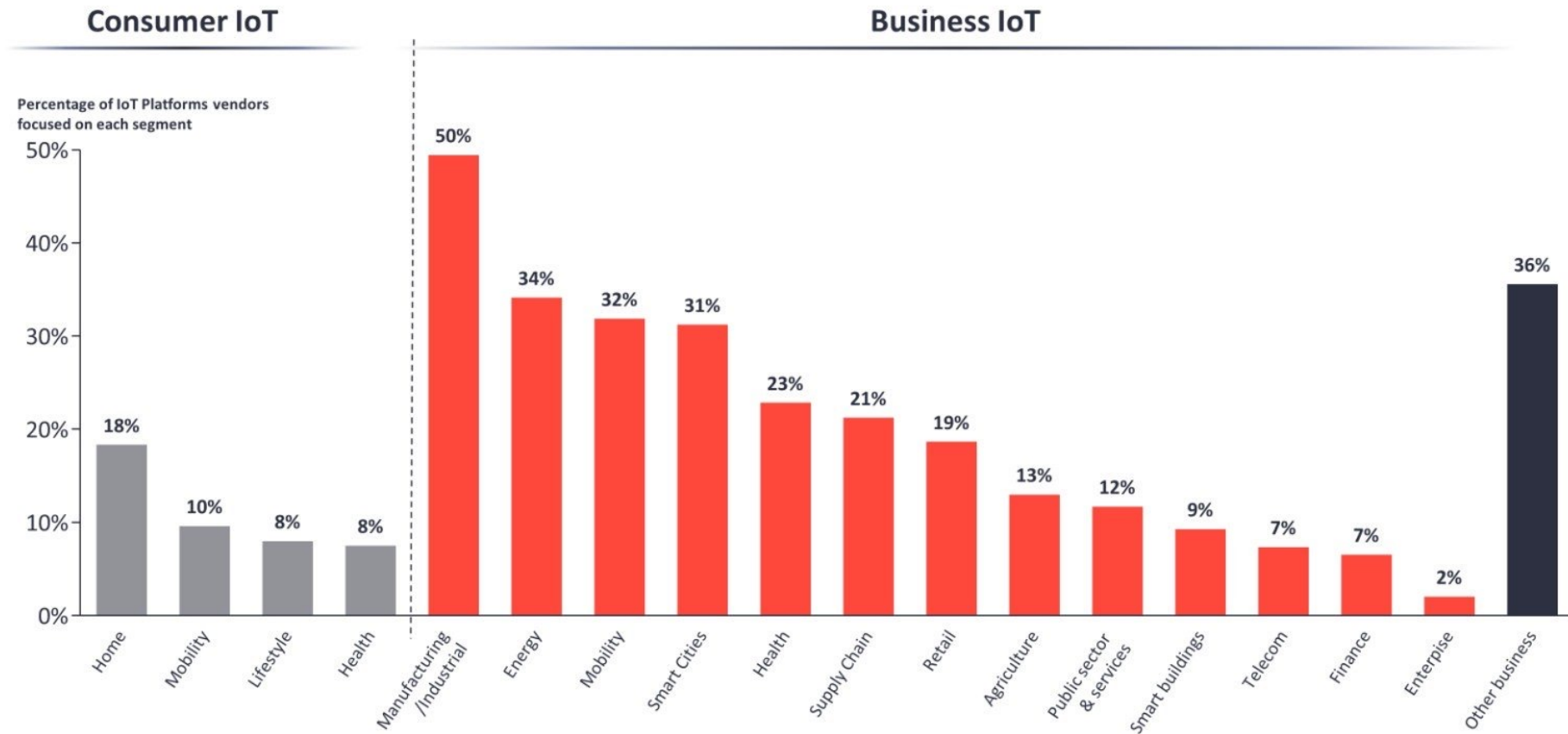


The growth in connected devices over the 2015-2025 decade. Source: [IoT Analytics](#)

IoT platform landscape and key players

By the end of 2019, the total number of known IoT platforms reached 620, with half of them focusing on manufacturing and industrial use (IIoT). Other popular activity areas are energy, mobility, smart cities, and healthcare.

Number of Identified IoT Platforms – By industry (Dec 2019)








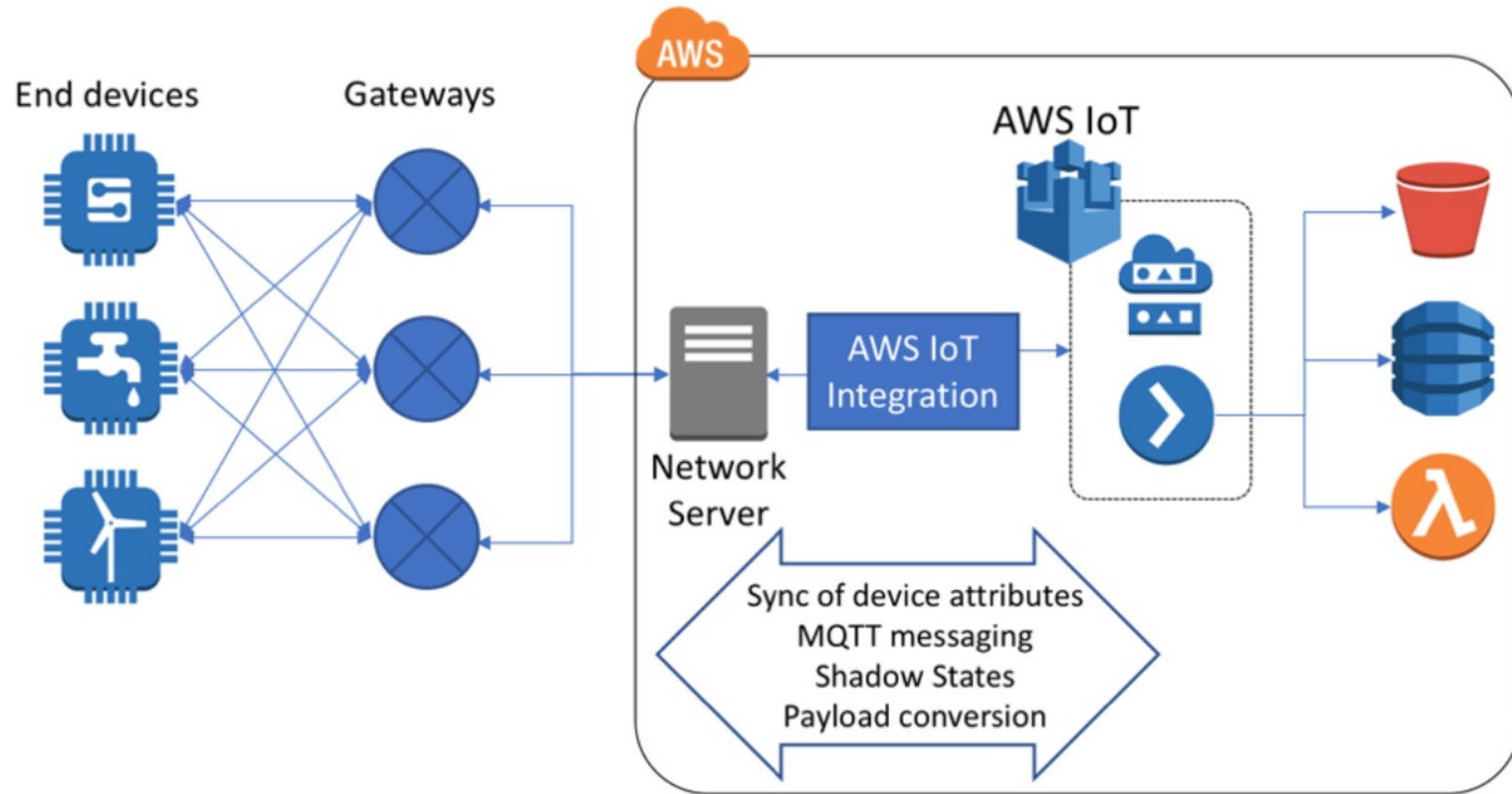
Fragmented and unconsolidated, the IoT platform market nonetheless has several major players enjoying the largest market share. The list of the top five, fully-fledged solutions in alphabetical order is as follows:

- Amazon Web Service (AWS) [IoT platform](https://aws.amazon.com/iot/), (<https://aws.amazon.com/iot/>)
- Cisco [IoT](https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html), (<https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html>)
- Google [Cloud IoT](https://cloud.google.com/solutions/iot), (<https://cloud.google.com/solutions/iot>)
- IBM [Watson IoT platform](https://www.ibm.com/cloud/watson-iot-platform), (<https://www.ibm.com/cloud/watson-iot-platform>)
- Microsoft [Azure IoT](https://azure.microsoft.com). (<https://azure.microsoft.com>)

All five options have a core solution with basic functionality and a set of additional modules you can add when necessary. Below, we'll explore building blocks of key platforms in more detail.

Key IoT middleware at a glance

	Communication protocols	Key offering and its main functions	Edge computing solutions	Top-3 use cases
	HTTP MQTT WebSockets	AWS IoT Core: <ul style="list-style-type: none"> ✓ Connectivity ✓ Authentication ✓ Rules engine ✓ Development environment 	FreeRTOS edge operating system IoT GreenGrass edge computing platform	<ul style="list-style-type: none"> ✓ Smart city ✓ Connected home ✓ Agriculture
	MQTT	Cisco IoT Control Center <ul style="list-style-type: none"> ✓ Mobile connectivity ✓ eSIM as a service ✓ Machine learning to improve security 	Cisco iOX edge development platform Cisco Edge Intelligence	<ul style="list-style-type: none"> ✓ Connected vehicles ✓ Manufacturing ✓ Smart city
	HTTP MQTT	Google Cloud IoT Core <ul style="list-style-type: none"> ✓ Connectivity ✓ Device management 	Edge TPU chip enabling deployment AI at the edge	<ul style="list-style-type: none"> ✓ Energy ✓ Smart parking ✓ Transportation and logistics
	HTTP MQTT	IBM Watson IoT Platform <ul style="list-style-type: none"> ✓ Connectivity ✓ Device management ✓ Real-time analytics ✓ Blockchain 	IBM Edge Application Manager platform	<ul style="list-style-type: none"> ✓ Manufacturing ✓ Agriculture ✓ Smart buildings
	HTTP MQTT AMQP over WebSockets	Azure IoT Hub <ul style="list-style-type: none"> ✓ Connectivity ✓ Authentication ✓ Device monitoring ✓ Device management ✓ IoT Edge 	IoT Edge as an integral part of IoT Hub	<ul style="list-style-type: none"> ✓ Healthcare ✓ Retail ✓ Manufacturing

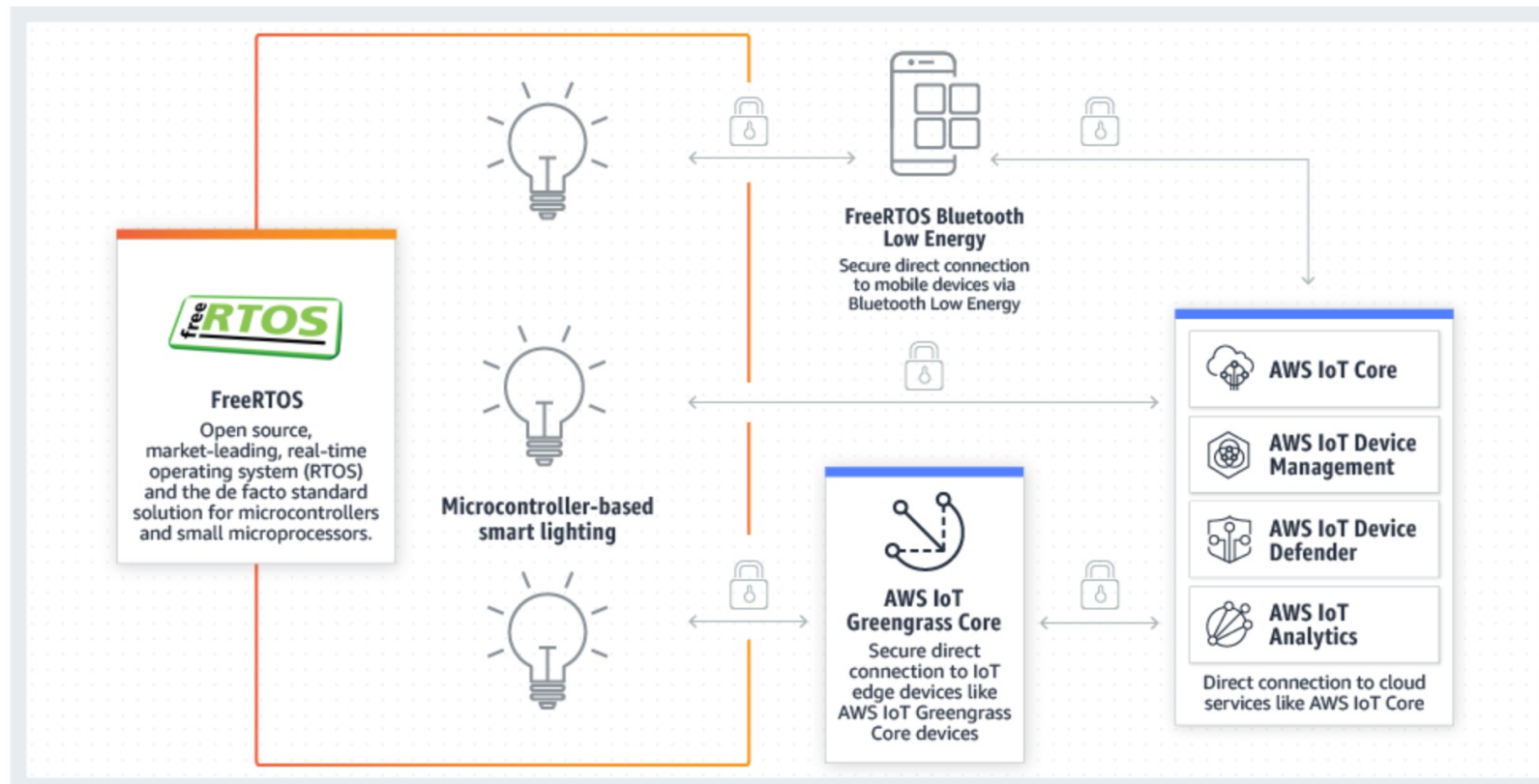


AWS IoT infrastructure. Source: [AWS](#)

How it works

FreeRTOS provides everything you need to easily program connected microcontroller-based devices and collect data from them for IoT applications. You can get started by choosing a FreeRTOS-qualified microcontroller from the [AWS Partner Device Catalog](#). Then, you can use the [AWS console](#) or [GitHub](#) to select and download relevant FreeRTOS libraries or pre-validated IoT reference integrations. Visit our getting started page to learn more about all the options.

You can securely connect FreeRTOS devices to cloud services like AWS IoT Core, to a local edge device, or to a mobile device via Bluetooth Low Energy, and update them remotely using the OTA update feature available with AWS IoT Device Management. An integration with AWS IoT Device Defender makes it easy to report on device-side metrics to detect anomalies when these metrics deviate from expected behavior.



Top 5 Open Source Tools for IoT Analytics



Countly

<https://count.ly>

Popularly known as one of the best open source tools for IoT analytics, Countly makes a compelling market presence through its Web analytics, mobile analytics and marketing platform capabilities. Developed on Node.js, Countly's open source SDKs are compatible with a range of modern-day devices – Web based, mobile tech, smart TVs, smart watches and other IoT smart devices.

Billions of data points from across several devices are processed on the cloud to generate customisable reports. Countly provides real-time data dashboards with a maximum time latency of up to just ten seconds, which is on par with various costly enterprise IoT analytics options available in the market.

In Countly, Web analytics is provided from a granular level. User profiles, attribution analytics, campaign tracking, session frequency tracking, geolocation (city/country) tracking, crash reports are a few of the many detailed insights provided by it. The tool also gives users the option to create funnel visualisation and Heat maps.

ThingsBoard

<https://thingsboard.io>

This open source IoT platform for collecting, processing, analysing and visualising telemetry sensor data is scalable, fault-tolerant and geared for high-performance computing. The toolkit supports both on-premise and cloud deployments.

The toolkit's core service, the ThingsBoard node, written in Java, is responsible for transferring data using REST API calls. Fully customisable, ThingsBoard clusters offer possibilities to create a range of technical microservices — HTTP/MQTT/CoAP transport microservices, WebUI microservices and JavaScript executor microservices. Rule based data processing algorithms can be applied to normalise, validate or transform input data sets. Users can also customise the Rule Engine toolset from the ThingsBoard dashboard to drag/drop Rule Nodes or define Root Rule Chain.

ThingsBoard is best known for its real-time IoT dashboard. The toolkit offers more than thirty customisable widgets to create rich visualisations, perform deep analytics and provide compelling IoT use cases.

ThingSpeak

<https://thingspeak.com>

The data aggregation and analytics IoT toolkit, ThingSpeak, offers non-commercial open source solutions that can visualise IoT device data using MATLAB widgets. ThingSpeak's reputation can be attributed to its seamless integration with the MathWorks product suite.

This robust IoT analytics tool supports RaspberryPi, Arduino and Nodemcu devices. IoT sensor data transferred to the ThingSpeak cloud using restful APIs and HTTP protocols can be analysed and visualised for more in-depth insights using MATLAB software.

There are also options to retrieve data in JSON, XML and CSV formats for manual data analysis and reporting. There are options for users to share data with their teams using private and public channels. ThingSpeak also has a paid commercial toolkit, but its open source and free-to-use solutions that work alongside MATLAB computational algorithms are more than well-suited for performing the fundamental IoT data analysis and visualisations.

Apache StreamPipes (<https://streampipes.apache.org>)

This industrial analytics toolkit is known to help both non-technical and technical users to collect, analyse and study IoT data sets. StreamPipes uses machine learning algorithms to perform advanced analytics, pattern detection, predictive analysis, anomaly detection and temporal analysis. It is well-reputed with non-technical users thanks to the intuitive, easy to use Web interface and graphical editor.

StreamPipes Connect, the in-built channelisation framework, can collect data inputs both from IoT device archived and real-time data sets. StreamPipes also comes with built-in semantics to provide intelligent insights and recommendations for data stream elements and/or transformational modules. The toolkit is compatible with HTTP/REST, MQTT, Kafka, OPCUA and ROS protocols. Enterprise key process indicators (KPIs) and production reports can be visualised in real-time using Web based cockpits.

There are additional options for software developers to use wrappers like Apache Flink and Apache Spark to customise SDKs and Maven archetypes to create new data processing elements. One of the unique features of StreamPipes is its ability to aggregate geographically distributed data pipelines in real-time, thereby creating possibilities to perform edge computing on IoT data. Various data harmonisation algorithms like filters, aggregation and unit converters, help developers clean and enrich device sensor data, periodically.

WSO2 IoT Server (<https://wso2.com/iot/>)

A server for the IoT platform released under Apache 2.0 license, this toolkit is trusted to offer versatile solutions with edge computing. WSO2 IoT Server creators pride themselves on its seamless integration, easy-to-deploy drag/drop widgets and platform scalability. The platform can manage up to a million IoT devices and provide deep data analytics of all the data aggregated from them.

WSO2 uses WSO2 Data Analytics Server (WSO2 DAS) to perform real-time analysis, batch analysis, interactive analysis and predictive analytics. WSO2 Complex Event Processor (WSO2 CEP) is used to handle millions of data aggregations per second. This makes the analytics platform well-suited to processing enormous volumes of IoT data.

WSO2 also provides analytics extension event adapters for HBase, Rabbitmq and Twitter, in addition to the native built-in event adapters available on its analytics platform.

Previously, the processes of collecting, storing and analysing an enormous volume of data sets was considered a complex and expensive task. But, today, with IoT standardisation, cloud computing, machine learning and edge computing, IoT analytics is taking huge progressive leaps in the industry. Our commercial world may not be fully adapted yet to leverage the power of IoT analytics, but we are definitely getting there.

Industries such as retail, pharma, healthcare, manufacturing and even smart city projects are increasingly gaining momentum in terms of artificial intelligence, machine learning and data analytics. Fortune 500 companies are already deploying IoT architecture in order to have a better understanding of their business processes and customer preferences. IoT data analytics is transforming enterprises and businesses already. Therefore, the sooner we adapt to achieving new possibilities with IoT, the better our stakes will be to make early gains from them.

What would be a better way to go SMART with IoT than by trying it for free? Try your hands on these top five open source IoT analytics tools and upgrade yourself for the future of work.