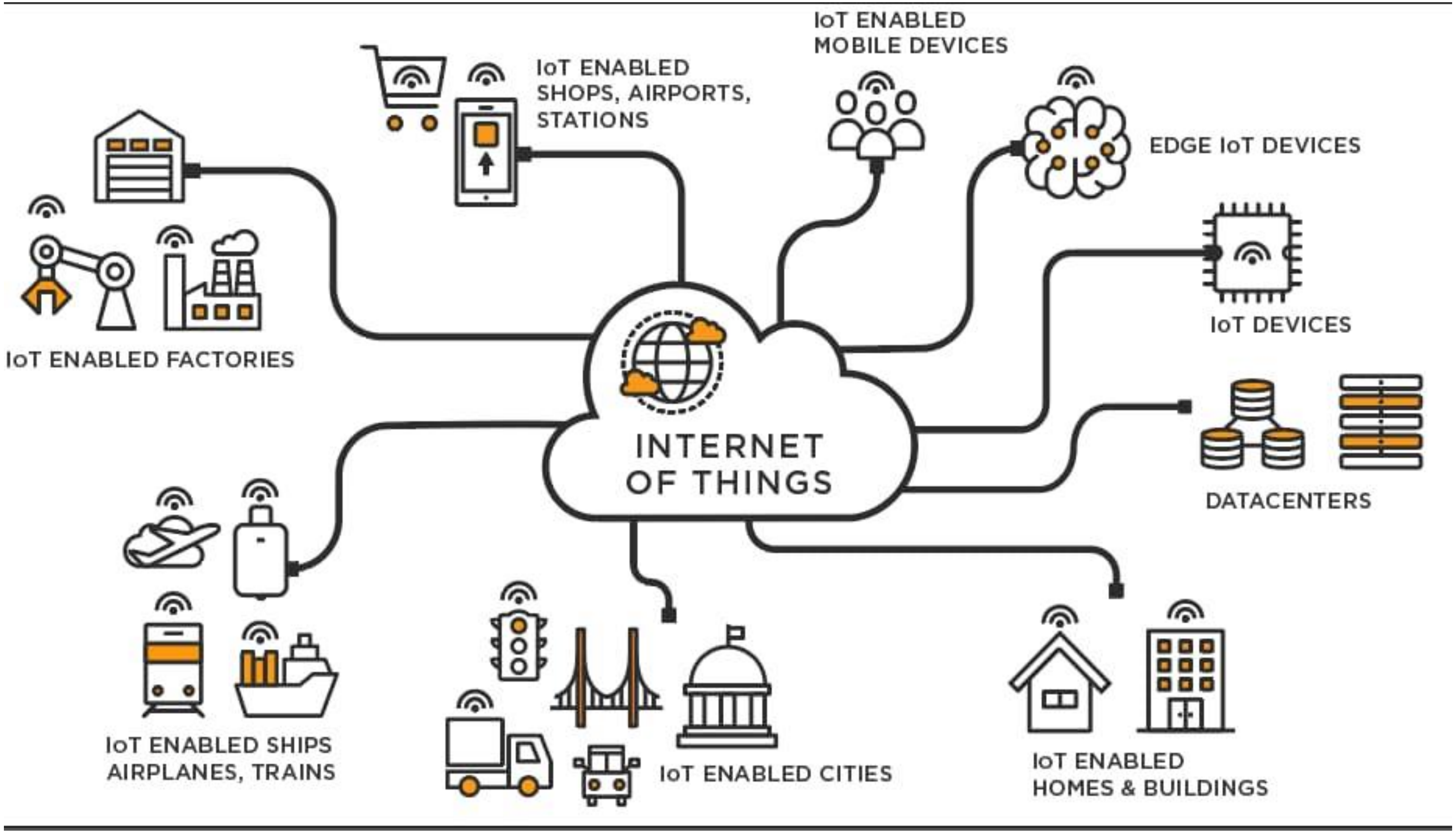
What is Internet of Things(IoT)?

The Internet of Things means“ **taking all the things in the world and connecting them to the internet**”.


IoT ENABLED MOBILE DEVICES
IoT ENABLED SHOPS, AIRPORTS, STATIONS
EDGE IoT DEVICES
IoT DEVICES
IoT ENABLED FACTORIES
INTERNET OF THINGS
DATACENTERS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

The most important applications of the Internet of Things (IoT)

✓ Nowadays, many companies from different sectors are adopting this technology to simplify, improve, automate and control different processes.

1. **Wearables:** Virtual glasses, fitness bands to monitor for example calorie expenditure and heart beats, or GPS tracking belts
2. **Health:** The use of wearables or sensors connected to patients, allows doctors to monitor a patient's condition outside the hospital and in real-time.
3. **Traffic monitoring:** The Internet of things can be very useful in the management of vehicular traffic in large cities, contributing to the concept of smart cities.
4. **Fleet management:** The installation of sensors in fleet vehicles helps to establish an effective interconnectivity between the vehicles and their managers as well as between the vehicles and their drivers. Both driver and manager/ owner can know all kinds of details about the status, operation and needs of the vehicle.
5. **Agriculture:** the Internet of Things offers farmers the possibility to access detailed knowledge and valuable information of their soil condition.

The most important applications of the Internet of Things (IoT)

6. **Hospitality:** The application of the IoT to the hotel industry brings with it interesting improvements in the quality of the service. With the implementation of electronic keys, which are sent directly to the mobile devices of each guest, it is possible to automate various interactions**.**
7. **Smart grid and energy saving:** The progressive use of intelligent energy meters, or meters equipped with sensors, and the installation of sensors in different strategic points that go from the production plants to the different distribution points, allows better monitoring and control of the electrical network.
8. **Water supply:** A sensor, either incorporated or adjusted externally to water meters, connected to the Internet and accompanied by the necessary *software* , helps to collect, process and analyze data, which allows understanding the behavior of consumers, detecting faults in the supply service, report results and offer courses of action to the company that provides the service.
9. **Home Automation**

10. **Smart City**

IoT Vision

- Vision of IoT—things becoming intelligent, smart and behaving alive.

- Internet of Things is a vision where things (wearable watches, alarm clocks, home devices, surrounding objects) become ‘smart’ and function like living entities by sensing, computing and communicating through embedded devices which interact with remote objects (servers, clouds, applications, services and processes) or persons through the Internet or Near-Field Communication (NFC) etc.

What is IOT?

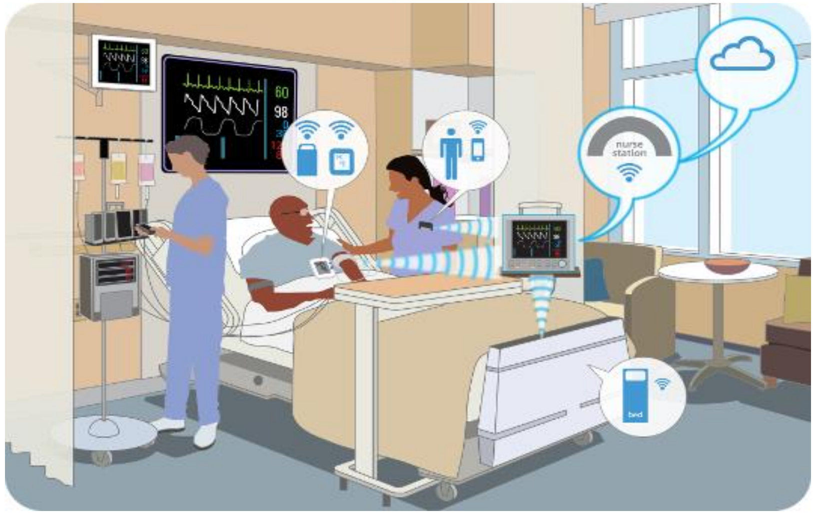
- The Internet of Things (IOT) is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data.

- IOT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.

Where is IOT?

Wearable Tech

Healthcare



Smart Appliances

The Smart *Internet of Things* School

Personalized learning with adaptive eTextbooks

Digital classroom white boards and display

iBeacons

Complete coverage with high performance Wi-Fi

Video recorders for lecture capture

Wearables for athletics and attendance tracking

International Collaboration and social exchange

Online testing

Sensors on trash receptacles

Supplies and inventory tracking by sensor with auto-reorder

Robot cleaning

Augmented and virtual reality

Makerspaces with 3D printers and laser trimmers

Student devices & eTextbooks

- Notebooks
- Tablets
- Smartphones

Internet of Things-based HVAC

Monitor and display of air quality throughout school

File and program storage, local or cloud-based

- Demographics, academics, behavior, interests
- LMS, CMS, SIS
- Educational programs and applications
- Video files: lectures and recorded lab experiments

Robotics for STEM and remote presence

Surveillance security cameras

Wi-Fi sensors and locks

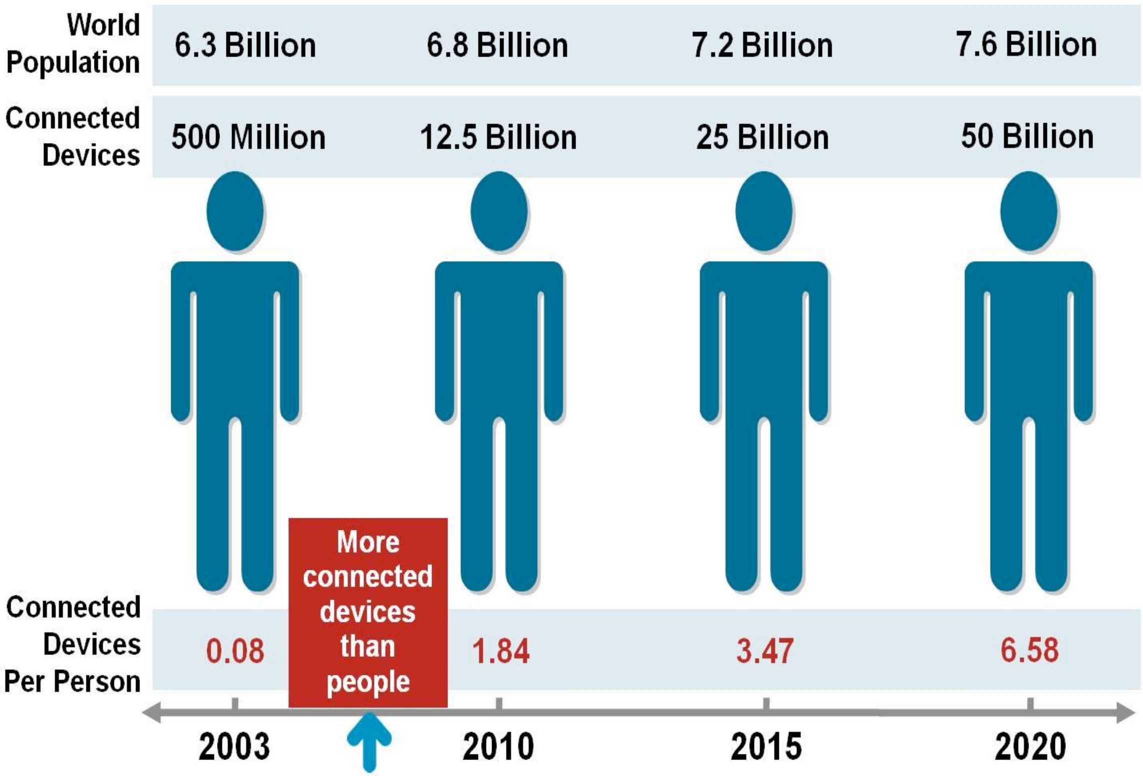
- Entrances and exits
- Classroom doors

Sensors track buses and verify student passengers

Network application analytics to monitor devices and network behavior

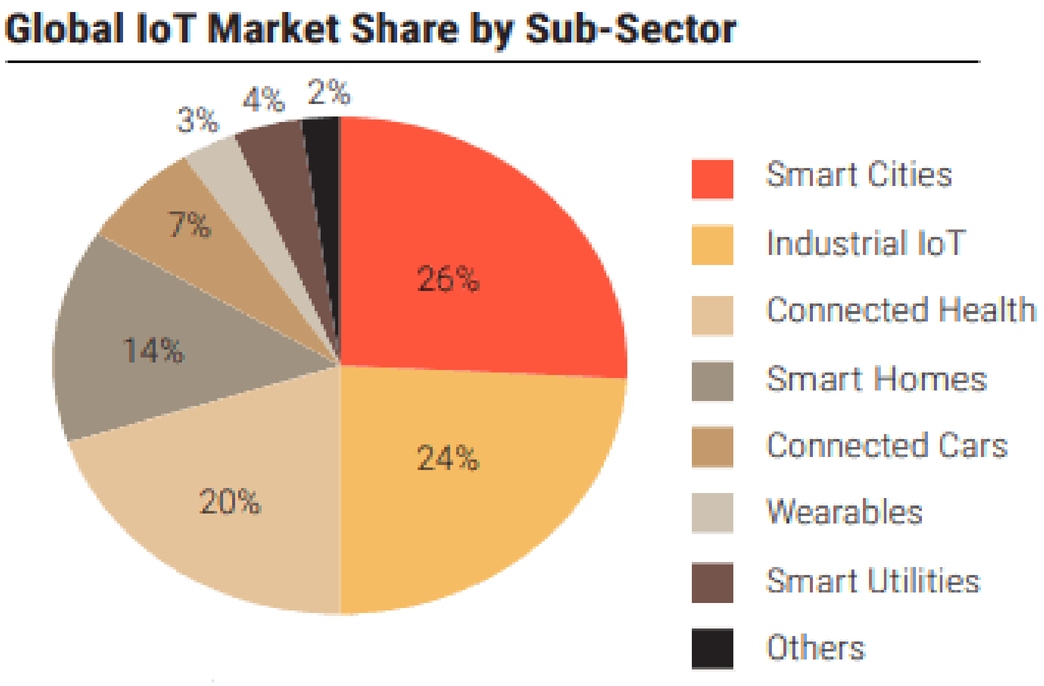
Sensors in parking lot and driveways

Current Status & Future Prospect of IOT



	2003	2010	2015	2020
World Population	6.3 Billion	6.8 Billion	7.2 Billion	7.6 Billion
Connected Devices	500 Million	12.5 Billion	25 Billion	50 Billion
Connected Devices Per Person	0.08	1.84	3.47	6.58

More connected devices than people



Global IoT Market Share by Sub-Sector

IOT Application Scenario - Shopping

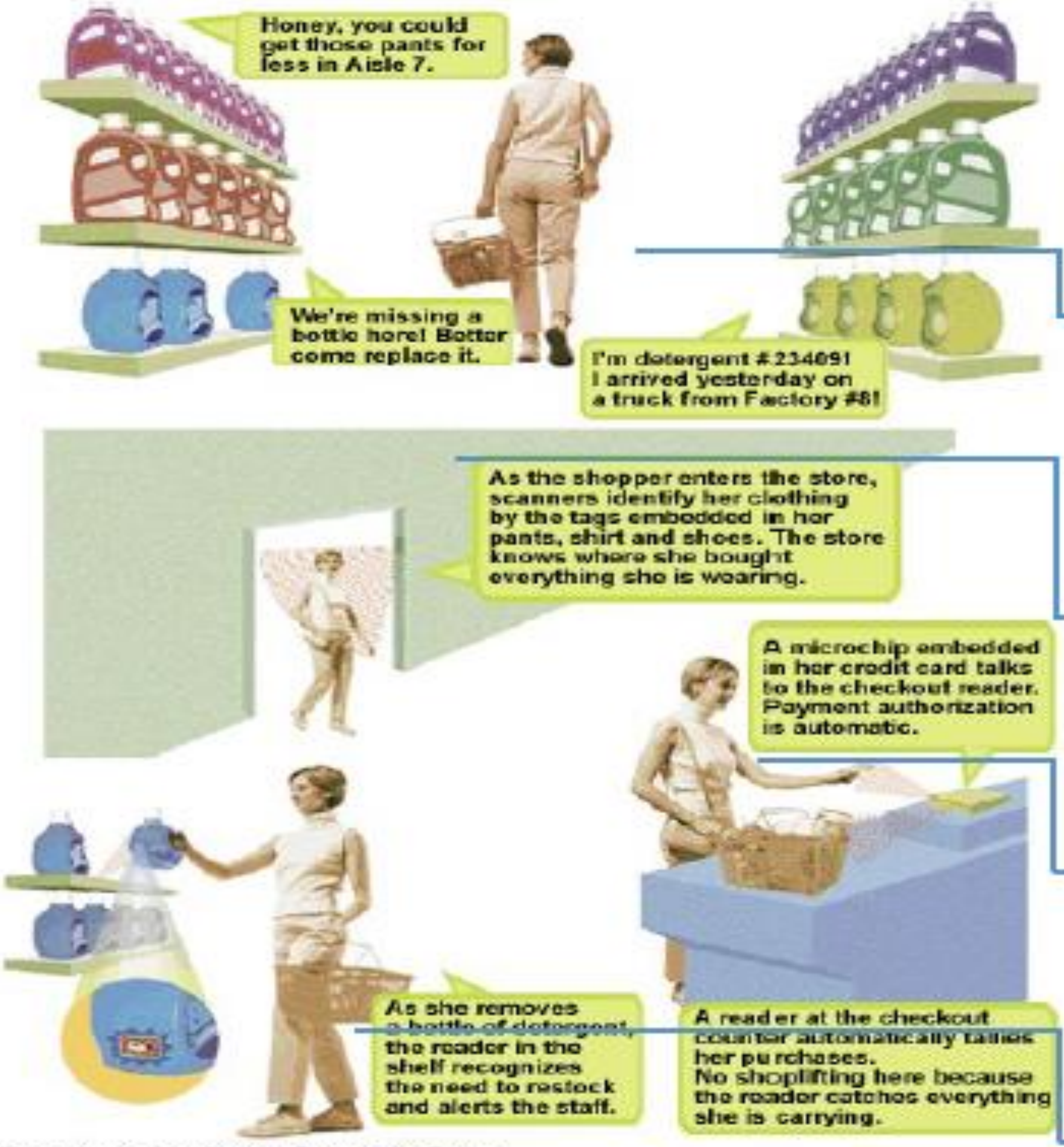

Honey, you could get those pants for less in Aisle 7.
We're missing a bottle here! Better come replace it.
I'm detergent #234091 I arrived yesterday on a truck from Factory #8!
As the shopper enters the store, scanners identify her clothing by the tags embedded in her pants, shirt and shoes. The store knows where she bought everything sho is wearing.
A microchip embedded in her credit card talks to the checkout reader. Payment authorization is automatic.
As she removes a bottle of detergent, the reader in the shelf recognizes the need to restock and alerts the staff.
A reader at the checkout counter automatically tallies her purchases. No shoplifting here because the reader catches everything she is carrying.

Illustration by Lisa Knouse Braiman for Forbes

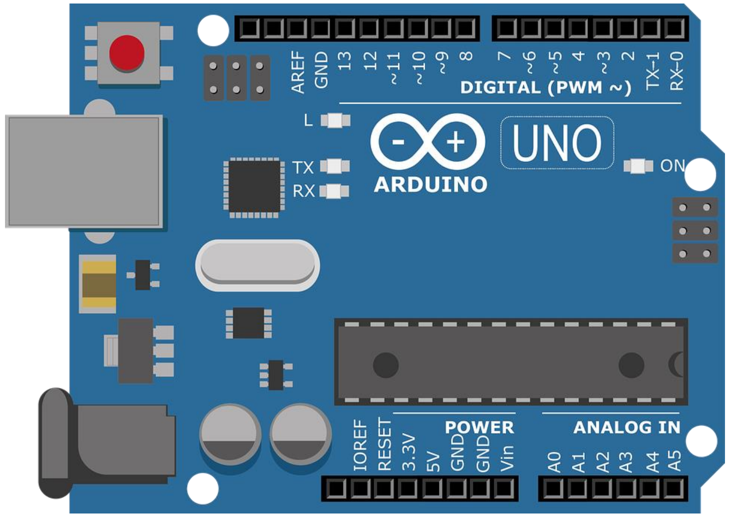
(2) When shopping in the market, the goods will introduce themselves.

(1) When entering the doors, scanners will identify the tags on her clothing.

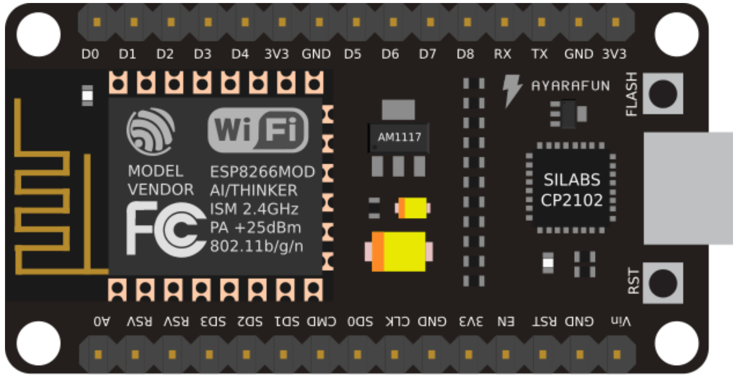
(4) When paying for the goods, the microchip of the credit card will communicate with checkout reader.

(3) When moving the goods, the reader will tell the staff to put a new one.

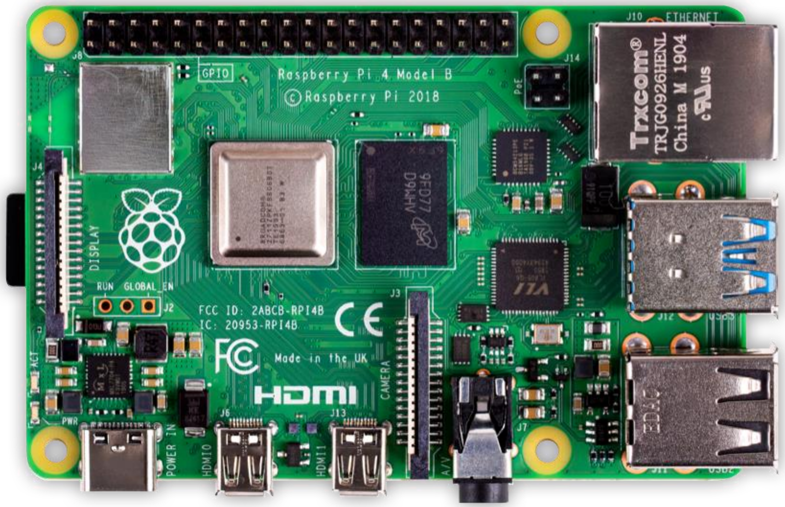
Different Hardware for IoT



ARDUINO



NODE MCU



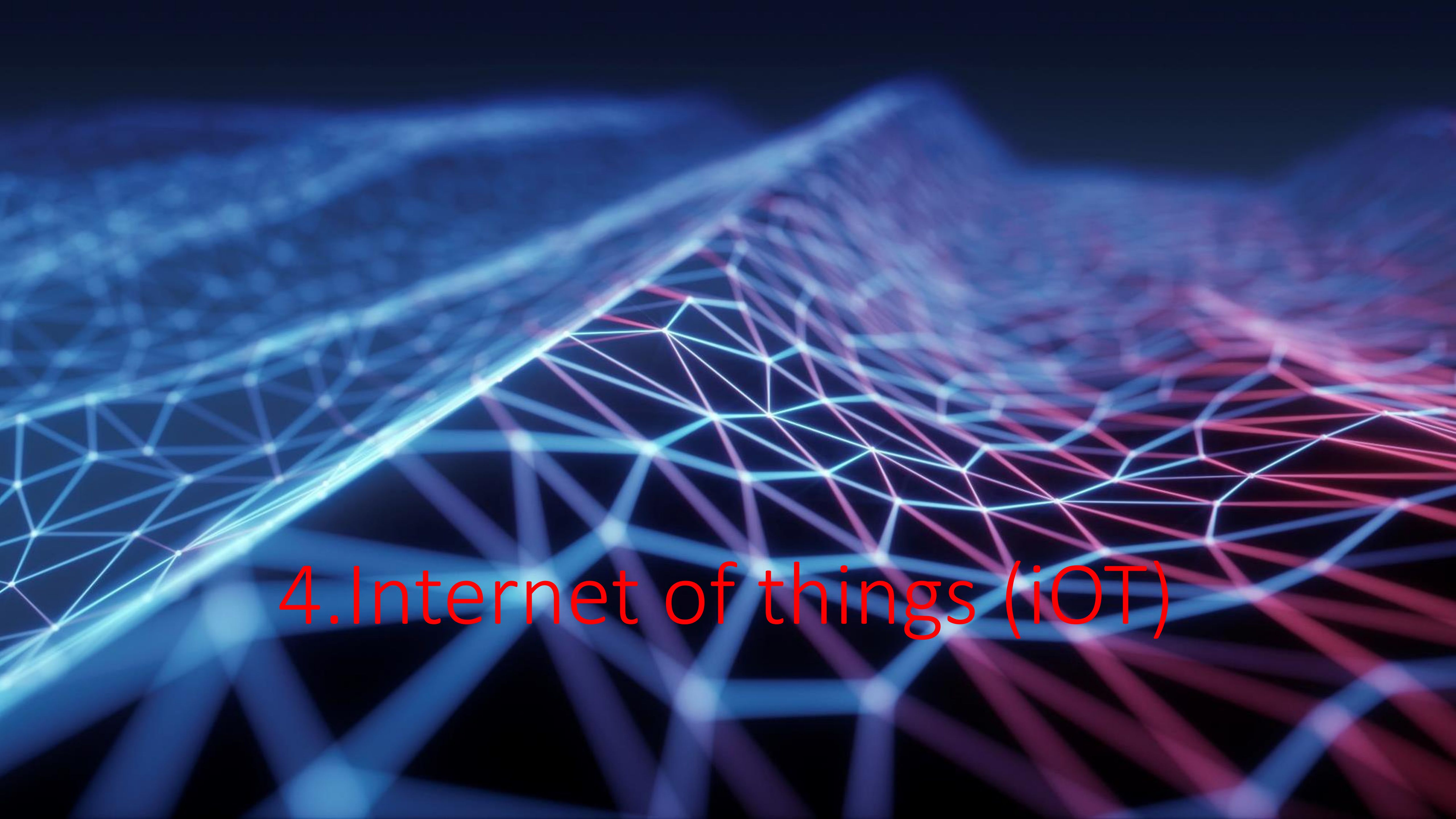
RASPBERRY PI

Comparison

	ESP8266 (Node MCU)	Arduino	Raspberry Pi
Cost	~ INR 300	~ INR 400	~INR 2500
Wifi	Built-in	ESP8266 Module ~ INR 150	USB Dongle / INBUILT / Ethernet
Programming	C++/Lua	C++	Python/Java/C++
Storage	Built-In	Built-In	SD-Card
I/O	10 GPIO/ 1 ADC	Arduino Uno: 13 GPIO/ 6 ADC	17 GPIO

Comparison

	ESP8266 (Node MCU)	Arduino	Raspberry Pi
Operating Voltage	3.3v	5v	5v
Clock Speed	26 MHz – 52 MHz	16 MHz	1.2GHz
Flash Memory	Upto 128 MB	32 KB	-



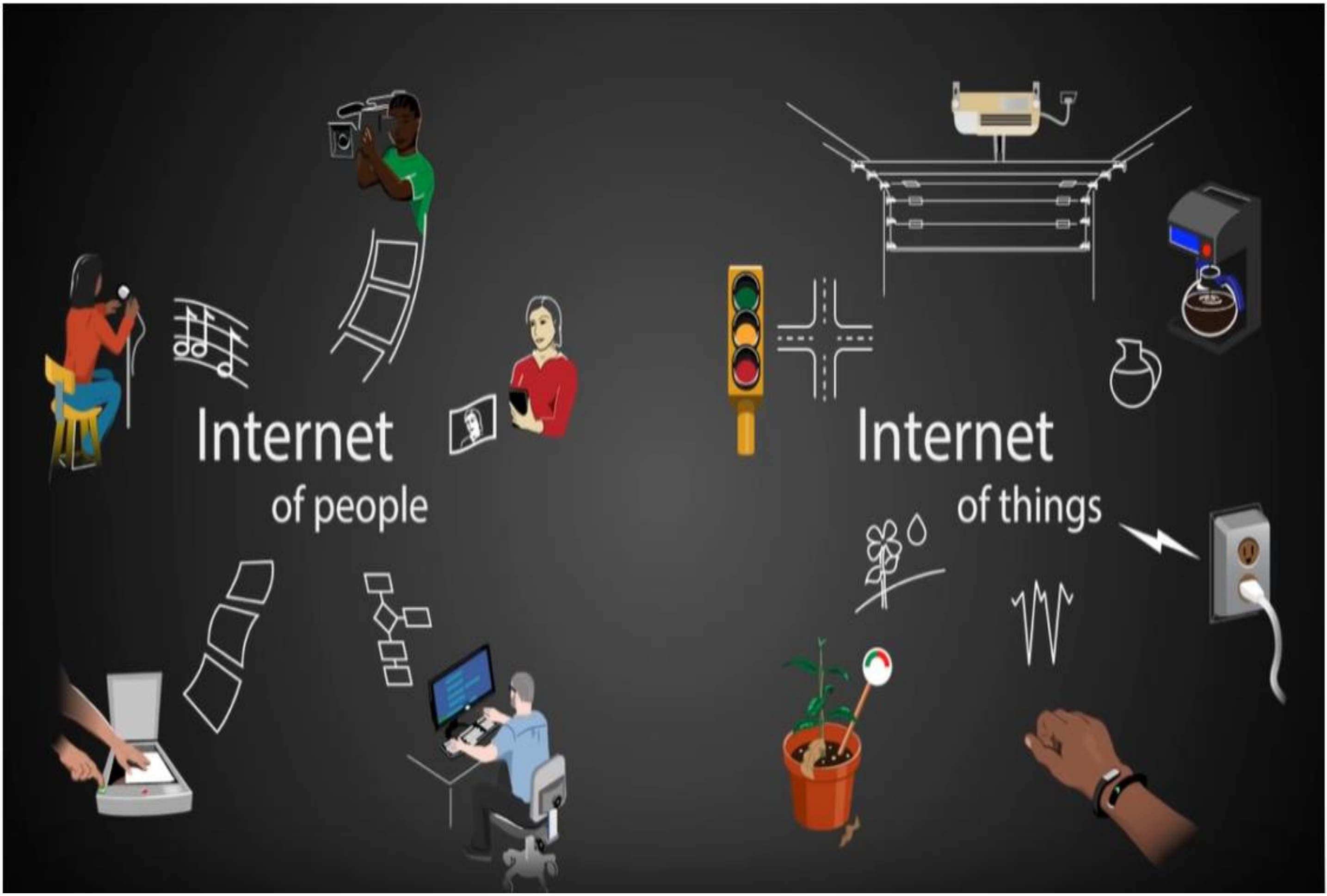
4.Internet of things (iOT)

What is internet of things (ioT)?

New and vast upcoming technology.

Network of physical objects or **"things“.** Embedded with **electronics, software, sensors, and network connectivity** which enables the system to **collect**, **process** data and hence **perform certain functions as per the requirement**.

In layman's terms, IoT enables the two or more devices connected over a network to talk to each other by the means of sharing data.



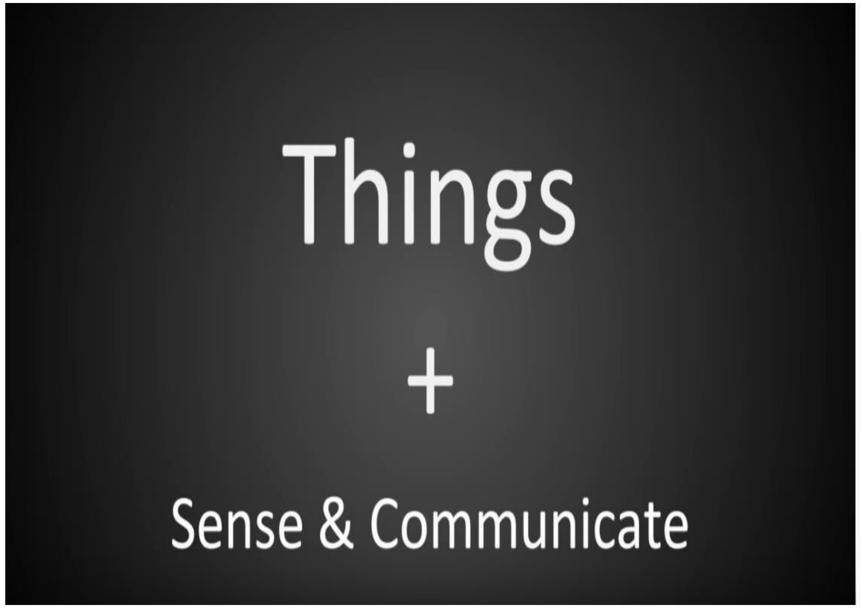
How does it work?

The working of an IoT is fairly simple to understand. There are at least two devices connected over the internet. One or both the devices may collect data and exchange between themselves or show it on an online platform using the firebase or storing it on cloud system.

Example: You connect a gas sensor to internet. You program the sensor such that it collects the data every minute and sends it to a cloud storage or firebase.

Now this data can be accessed by anyone who is allowed to view it on any device from anywhere in the world.

Like in Delhi, you find large LCDs screens at places and which show the pollution level of the area. That uses a similar system. The screens are programmed in such a way that they automatically collect the data from the servers and display them.

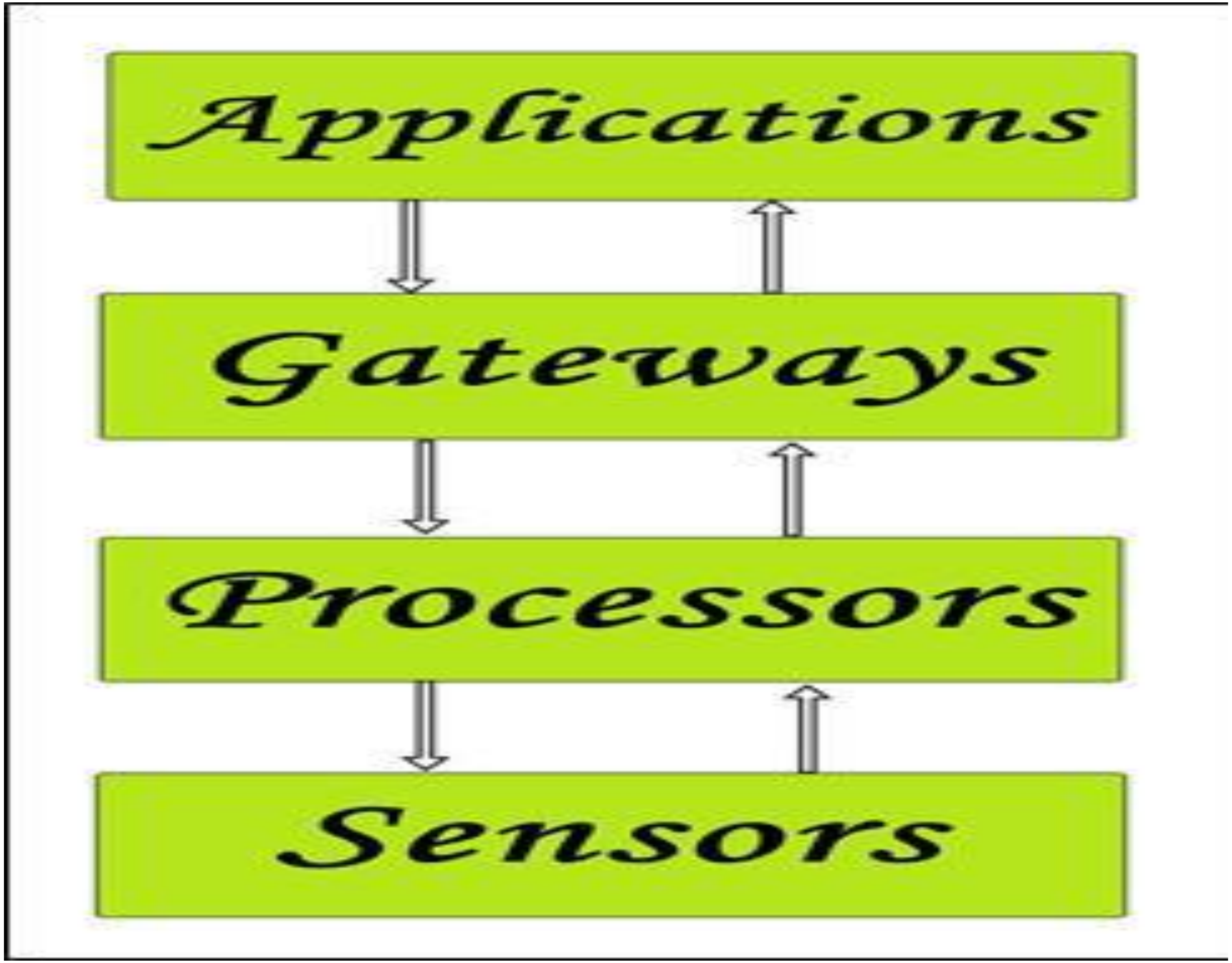


Things

+

Sense & Communicate

Building Blocks



Sensors

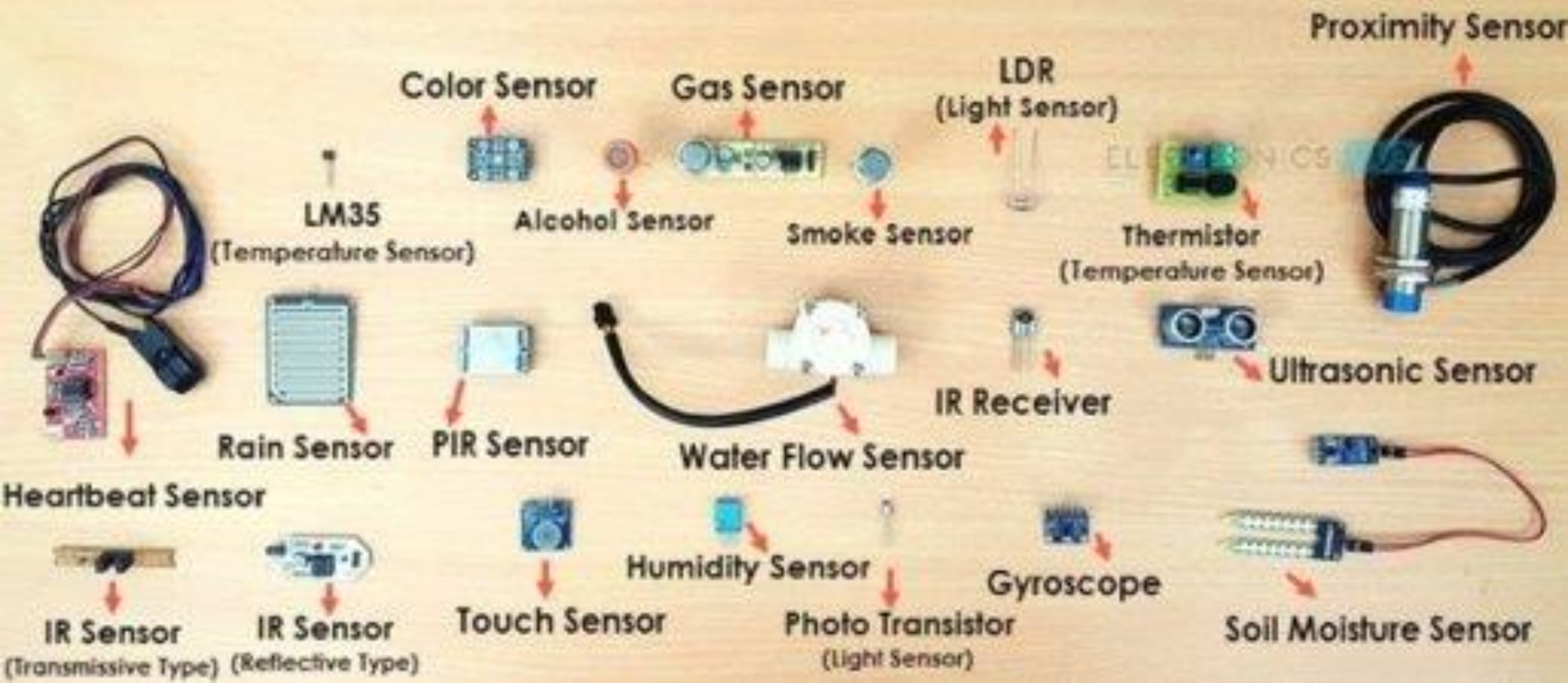
Sensors are the small electronic devices which are used to **collect data** from its surroundings.

Main purpose - collect data from its surrounding (sensors) or give out data to its surrounding (actuators).

These also have to be **uniquely identifiable devices** with a unique IP address so that they can be easily identifiable over a large network.

These devices **have to be always active** to send the real time data updates to the servers.

DIFFERENT TYPES OF SENSORS



Processors

“Brain” of the IoT system.

Main function - process the data captured by the sensors to extract the valuable data from the enormous amount of raw data collected.

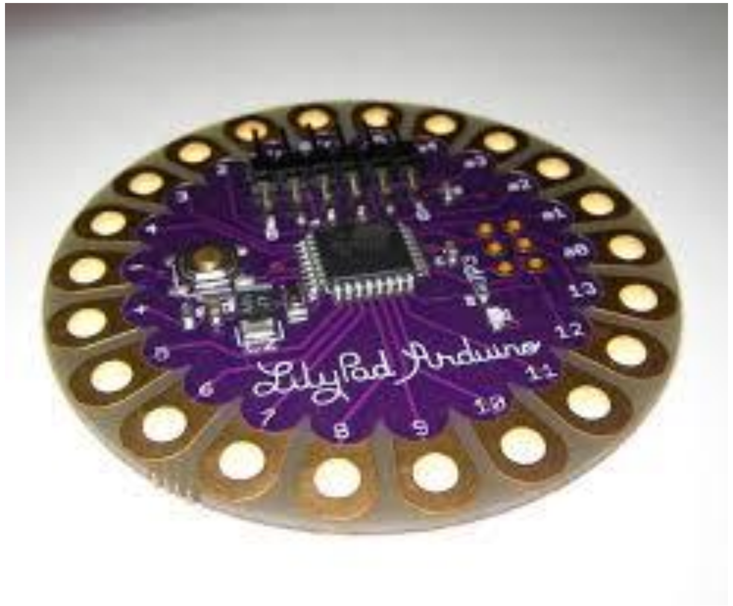
Gives **intelligence to the data.**

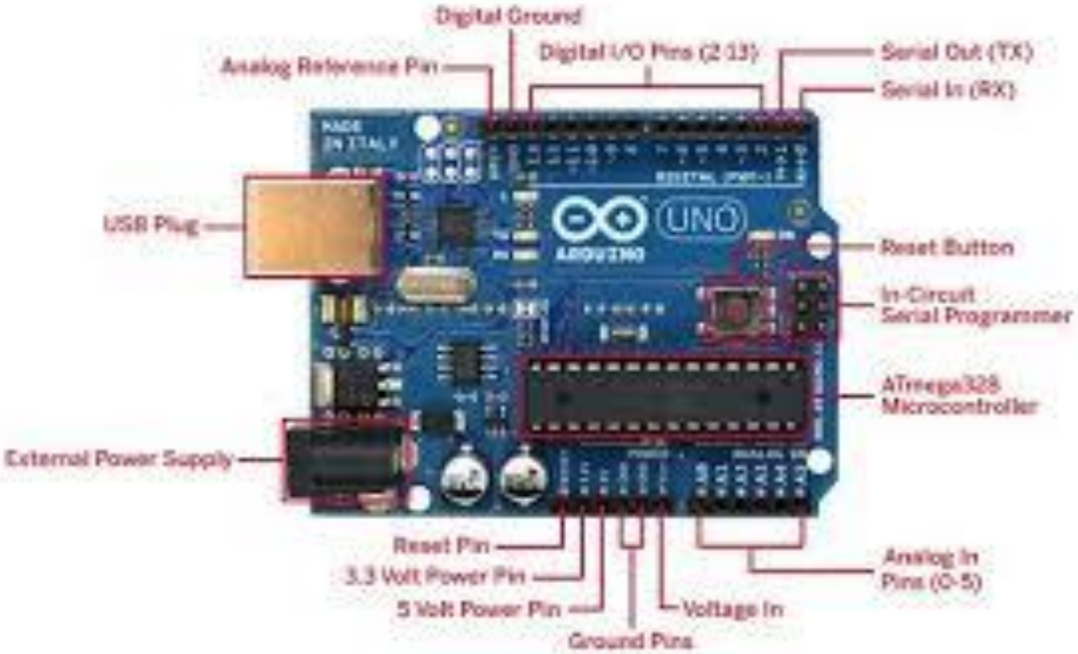
Processors mostly work on **real-time** basis and can be easily controlled by applications.

Responsible for securing the data – that is performing **encryption and decryption of data**.

Embedded hardware devices, microcontroller etc are the ones that process the data because they have processors attached to it.

MEGA
ARDUINO


LilyPad Arduino


Digital Ground
Analog Reference Pin
Digital I/O Pins (2-13)
Serial Out (TX)
Serial In (RX)
USB Plug
Reset Button
In-Circuit Serial Programmer
ATmega328 Microcontroller
External Power Supply
Reset Pin
3.3 Volt Power Pin
5 Volt Power Pin
Ground Pins
Voltage In
Analog In Pins (0-5)
UNO
ARDUINO

RAW GND RST VCC A3 A2 A1 A0 15 14 16 10
J1 TXO RXI GND GND 2 3 4 5 6 7 8 9
Pro Micro

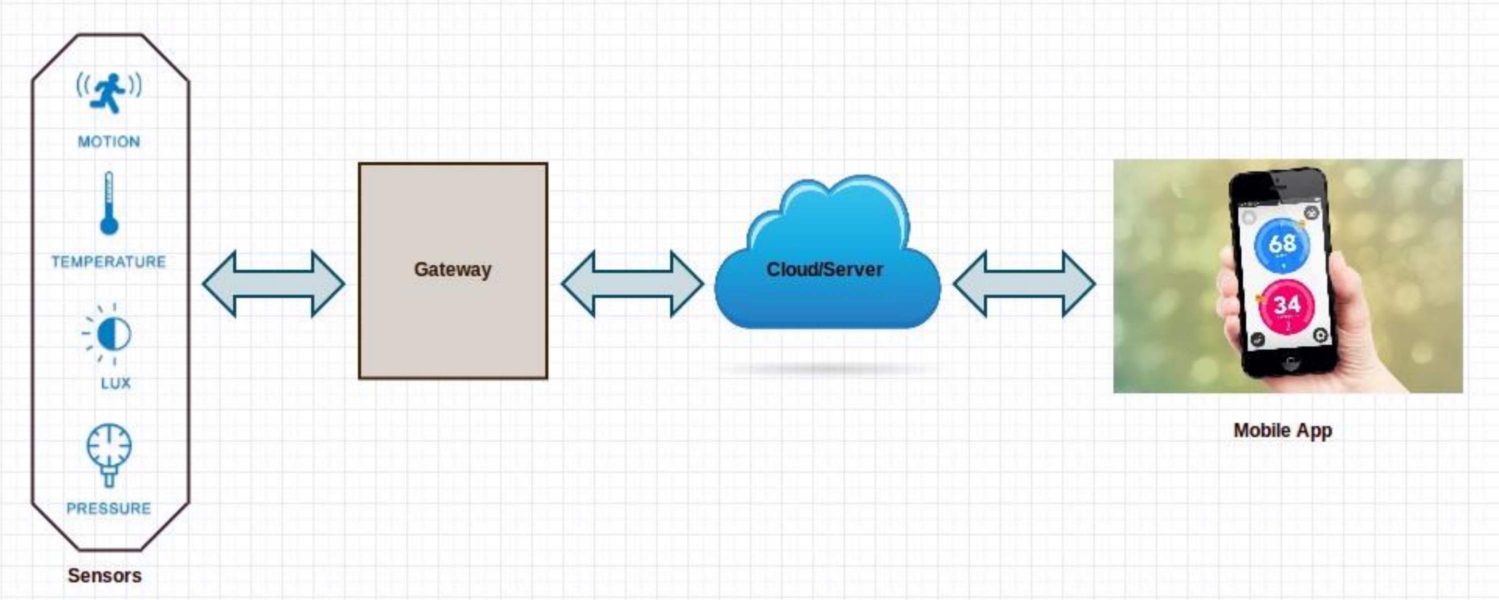
Gateways

Responsible for **routing** the processed data and send it to proper locations for its (data) proper utilization.

Helps in **to and fro communication** of the data.

Provides **network connectivity** to the data.

LAN, WAN, PAN etc are examples of network gateways.

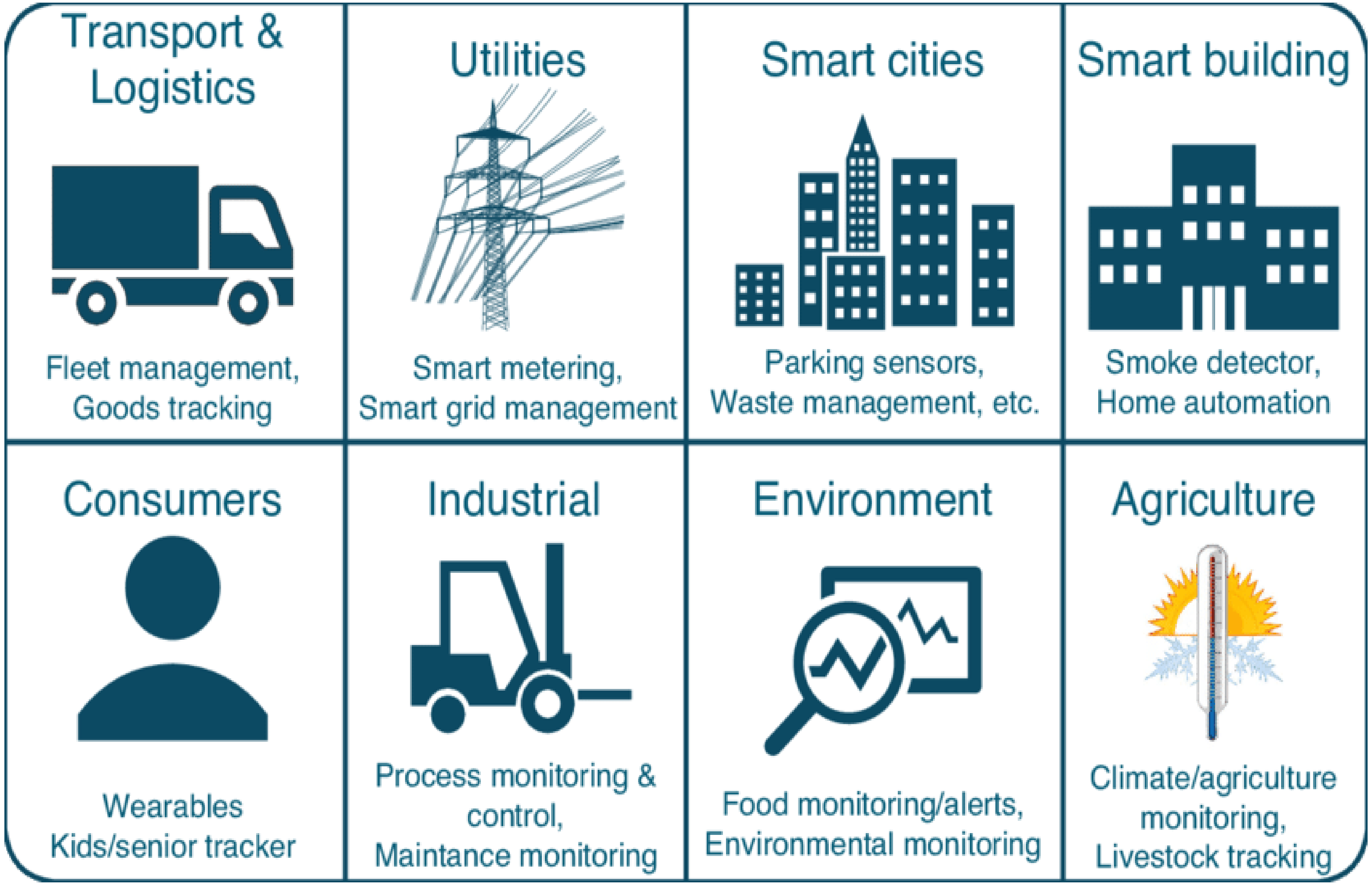


Applications

Form **another end** of an IoT system.

Essential for **proper utilization** of all the data collected.

Examples: home automation apps, security systems, industrial control hub etc.



Transport & Logistics
Fleet management, Goods tracking

Utilities
Smart metering, Smart grid management

Smart cities
Parking sensors, Waste management, etc.

Smart building
Smoke detector, Home automation

Consumers
Wearables
Kids/senior tracker

Industrial
Process monitoring & control,
Maintance monitoring

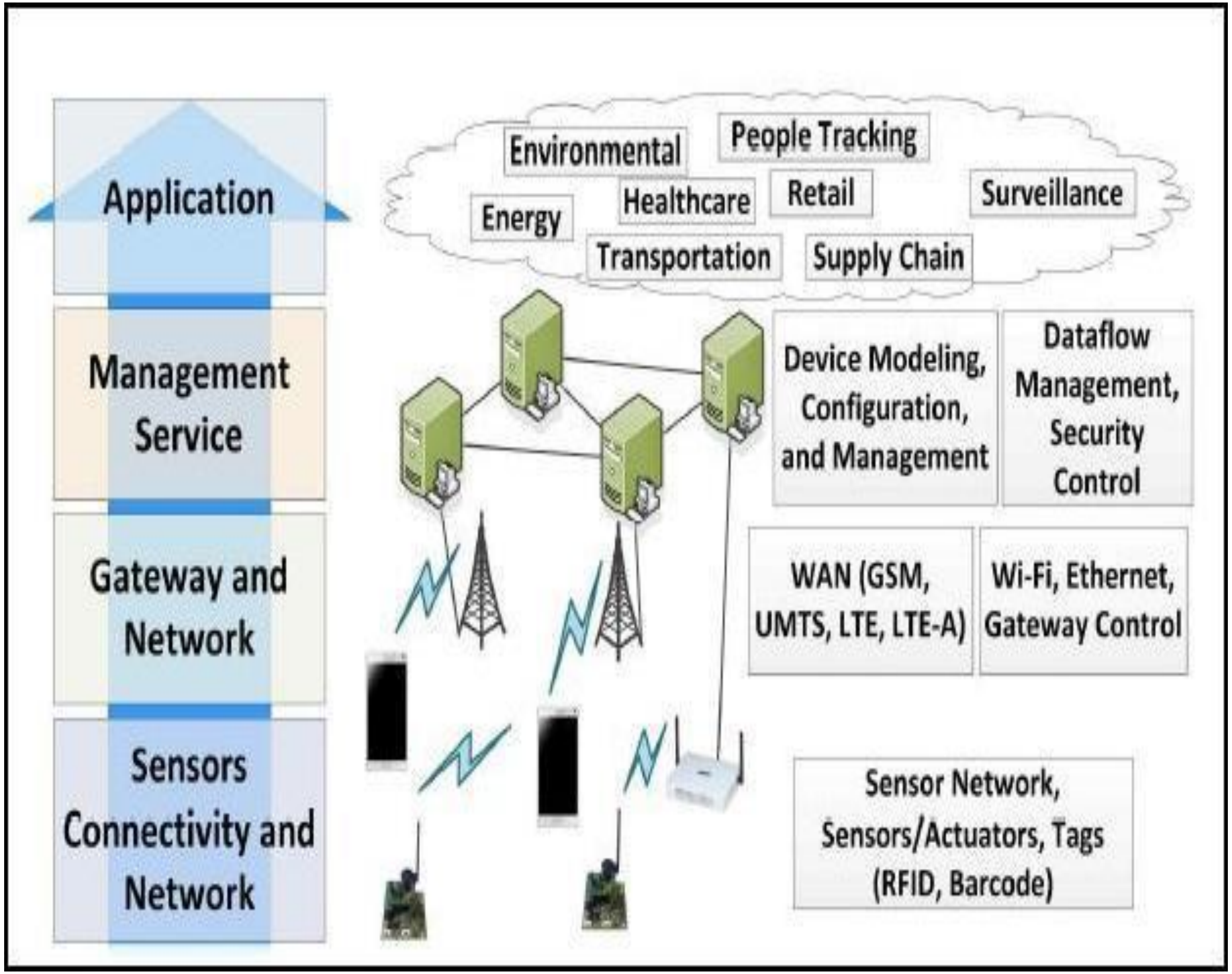
Environment
Food monitoring/alerts, Environmental monitoring

Agriculture
Climate/agriculture monitoring,
Livestock tracking

IOT architecture

Major layers:

- Sensors Connectivity and Network
- Gateway and Network
- Management Service
- Application


Application
Management Service
Gateway and Network
Sensors Connectivity and Network
Environmental
People Tracking
Energy
Healthcare
Retail
Surveillance
Transportation
Supply Chain
Device Modeling, Configuration, and Management
Dataflow Management, Security Control
WAN (GSM, UMTS, LTE, LTE-A)
Wi-Fi, Ethernet, Gateway Control
Sensor Network, Sensors/Actuators, Tags (RFID, Barcode)

Sensor, Connectivity and network layer

Consists of **RFID tags, sensors** - form the essential "**things**" of an IoT system.

Sensors, RFID tags - wireless devices , form the **Wireless Sensor Networks (WSN).**

Sensors are **active** in nature which means that **real-time** information is to be collected and processed.

This layer also has the **network connectivity** (like **WAN, PAN** etc.) which is responsible for **communicating the raw data to the next layer** which is the Gateway and Network Layer.

Gateway and Network Layer

Gateways - responsible for **routing** the data coming from the Sensor, Connectivity and Network layer and **pass it to the next layer** which is the Management Service Layer.

This layer **requires** having a **large storage capacity** for storing the enormous amount of data collected by the sensors, RFID tags etc. Also, this layer needs to have a consistently **trusted performance** in terms of public, private and hybrid networks.

Management Service Layer

Used for **managing the IoT services**.

Responsible for:

Securing Analysis of IoT devices,
Analysis of Information
Device Management.

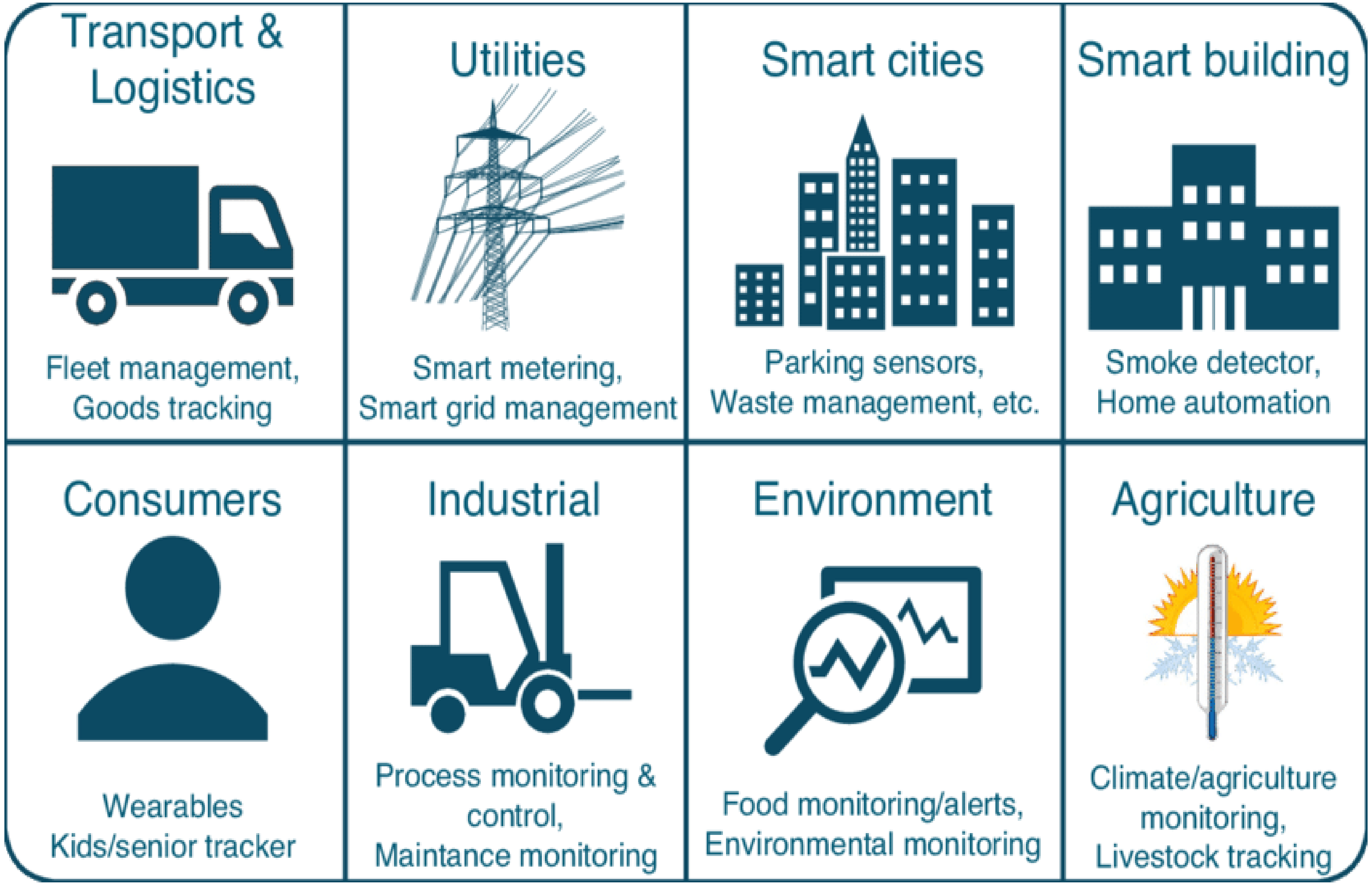
Performs Data management - extract the necessary information from the enormous amount of raw data collected by the sensor devices to yield a valuable result of all the data collected.

Application Layer

Topmost layer.

Responsible for effective utilization of the data collected.

IoT applications include Home Automation, E-health, E-Government etc.



Transport & Logistics
Fleet management, Goods tracking

Utilities
Smart metering, Smart grid management

Smart cities
Parking sensors, Waste management, etc.

Smart building
Smoke detector, Home automation

Consumers
Wearables
Kids/senior tracker

Industrial
Process monitoring & control,
Maintance monitoring

Environment
Food monitoring/alerts,
Environmental monitoring

Agriculture
Climate/agriculture monitoring,
Livestock tracking

DEFINITION OF IoT

- The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. –which,through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals.”
- (Atzori et al., 2010):

- In the SG 20 recommendation document Y.2060 (ITU-T, 2012), the following definition is given:
- “*Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperableinformation and communication technologies.*
- *NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications ,whilst ensuring that security and privacy requirements are fulfilled.*
- *NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technologicaland societal implications.*”

- The definition published on the IERC website* states that the IoT is
- “*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual ‘things’ have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated intothe information network.*”
- In one of the SWG 5 reports published in 2015, the adopted definition for IoT is given in the following terms (ISO/IEC JTC1, 2015):
- “*An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.*”

- In the Request for Comments (RFC) 7452,* which talks about the architectures for networks of smart objects, IoT is defined as follows:
- “*The term ‘Internet of Things’ (IoT) denotes a trend where a large number of embedded devices employ communication services offered by Internet protocols.*
- *Many of these devices, often called ‘smart objects,’ are not directly operated by humans but exist as components in buildings or vehicles, or are spread out in the environment.*”

- The IEEE IoT initiative published a document (IEEE, 2015) with an overview of the IoT applications and a proposal of a definition in order to start a discussion and to give its community members an opportunity to contribute to the definition of the IoT.† The document presents two definitions, one for the small-scale scenarios:
- “*An IoT is a network that connects uniquely identifiable ‘Things’ to the Internet.*
- *The ‘Things’ have sensing/actuation and potential programmability capabilities.*
- *Through the exploitation of unique identification and sensing, information about the ‘Thing’ can be collected and the state of the ‘Thing’ can be changed from anywhere, anytime, by anything*

PROPOSED ARCHITECTURES AND REFERENCE MODELS

- With the intention of making interoperability between different IoT systems possible, several attempts have been made in recent years to create reference layered models for IoT
- Several standards development organizations(SDOs) are also engaged in this process, as will be described below.

- M2M specifications focus on the creation of a framework to support applications and services, such as smart grid, connected car, home automation, public safety, and health.
- During a workshop organized by the European Telecommunications Standards Institute (ETSI), which took place in November 2016, the European Commission highlighted the need for an open common RA for IoT, enabling the integration of different services, for the specific case of smart cities application.
- In fact, this is of critical importance not only to smart cities but also to all areas of application of IoT technologies.
- In addition to oneM2M standardization activities, ETSI has also created a working group on sustainable digital multiservice cities, specifically for the case of smart cities projects

- The IEEE has produced more than 80 standards* that relate to several areas of IoT systems and has around 60 ongoing projects to develop new standards also related to the IoT.
- The GSM Association (GSMA)* has gathered nearly 800 mobile operators and 300 companies worldwide to address four areas of the mobile industry: “
- The GSMA Connected Living Programme (LP) is working with mobile operators to fasten the delivery of IoT solutions that exploit connectivity in innovative ways

- For 2017, the GSMA Connected LP focuses on four new goals:
- (1) Mobile IoT, which mainly addresses increasing the market awareness and support for licensed spectrum LPWA solutions;
- (2) completing the technical specification of the Consumer Remote SIM Provisioning;
- (3) positioning operators as key partners within the IoT big data market through the delivery of data sets and APIs; and
- (4) supporting operators in the provision of services that enable smart cities (GSMA, 2016).

- ITU also created the Internet of Things Global Standards Initiative (IoT-GSI),[‡] which worked in detailing the requirements for developing the standards that are necessary to enable the deployment of IoT on a global scale, taking into account the work done in other SDOs.
- Both Industrial Internet Reference Architecture (IIRA)[¶] and Reference Architecture Model for Industrie 4.0 (RAMI 4.0) were developed, focusing on taking advantage of IoT technology to increase the efficiency of the industrial processes, either improving manufacturing itself or making the supply chain from the suppliers to the customers more effective.

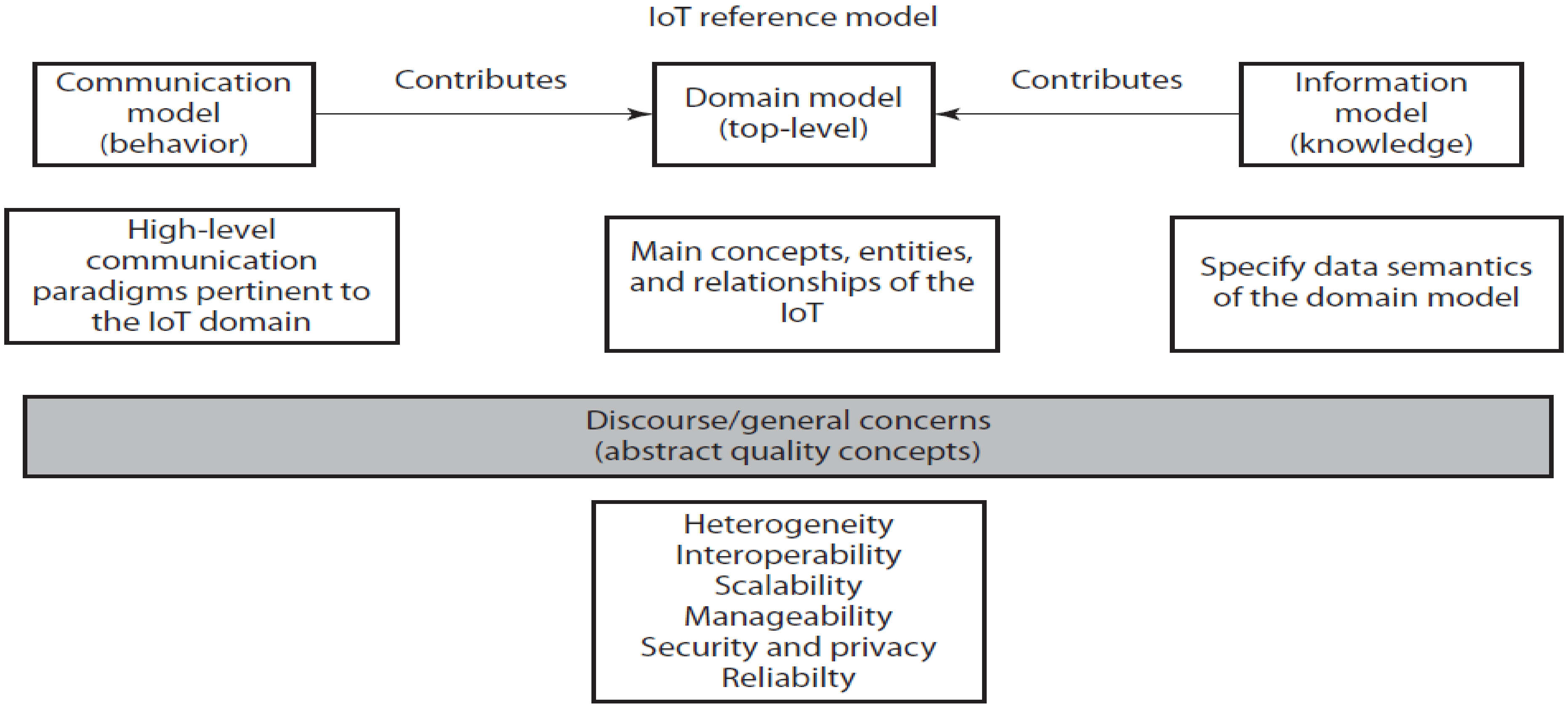
- Sensor Network Reference Architecture (SNRA),** in turn, provides a general overview of the characteristics of a sensor network and the organization of the entities that comprise such a network.
- It also describes the general requirements that are identified for sensor networks, which relate to IoT systems since sensor networks are used by IoT systems as a tool for collecting data

IoT-A

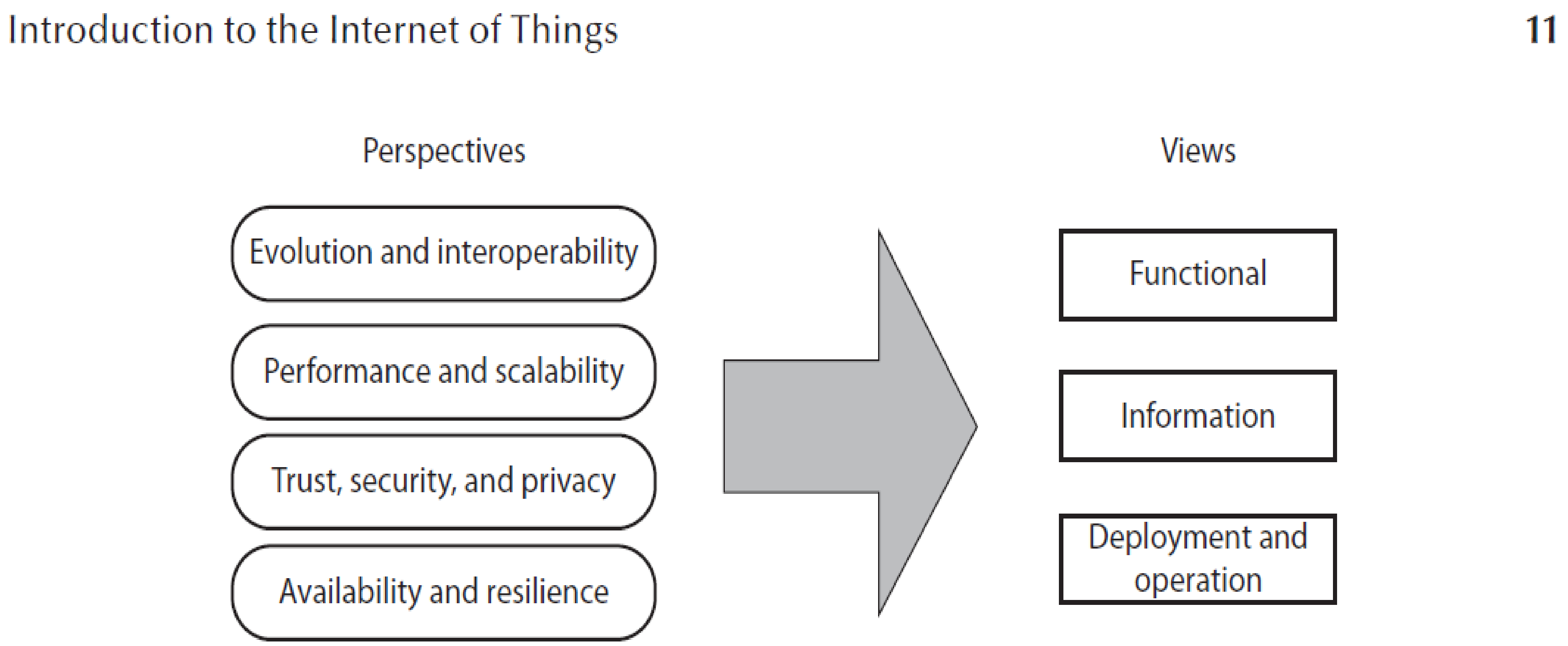
- In the following sections, some of the more relevant RAs are briefly described.
- As they are still being developed, there might be new updates in this field. Currently, the IoT-A project is no longer active.
- However, IoT-A is described here since it is being used as a basis for developing other architectures, such as the IoT RA or Reference IoT Layered Architecture (RILA)

- The IoT-A ARM was created in order to achieve interoperability between different IoT systems
- The IoT ARM is defined to be abstract so that it can be used as a reference for generating concrete system architectures.
- It consists of an RM and an RA. The RM, presented in Figure below, provides a common understanding of the IoT domain by modeling its concepts and their relationships.
- Similar to the Open Systems Interconnection (OSI) model, the IoT RM by itself does not specify the technical particularities of an IoT system.

RM proposed by IoT-A. (Adapted from Bassi, A., et al., *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*, Springer, Berlin, 2013, 163–211.)


IoT reference model
Communication model (behavior)
Contributes
Domain model (top-level)
Contributes
Information model (knowledge)
High-level communication paradigms pertinent to the IoT domain
Main concepts, entities, and relationships of the IoT
Specify data semantics of the domain model
Discourse/general concerns (abstract quality concepts)
Heterogeneity
Interoperability
Scalability
Manageability
Security and privacy
Reliabilty

Perspectives and views of IoT-A. (Adapted from Bassi, A., et al., *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*, Springer, Berlin, 2013, 163–211.)



Introduction to the Internet of Things 11

Perspectives
Evolution and interoperability
Performance and scalability
Trust, security, and privacy
Availability and resilience
Views
Functional
Information
Deployment and operation

- The *domain model* considers a top-level description of the concepts and entities (physical entities, devices, resources, and services) that represent particular aspects of the IoT domain, and defines their relations.
- Therefore, the domain model can also be used as a taxonomy of the IoT.
- The *information model* specifies the data semantics of the domain model; that is, it refers to the knowledge and behavior of the entities considered in the domain model,
- since they are responsible for either keeping track of certain information or performing specific tasks (it describes which type of information the entities are responsible for).

- The *communication model*, in turn, addresses the main communication paradigms necessary for connecting entities, ensuring interoperability between heterogeneous networks.
- The proposed communication model is structured in a seven-layer stack and describes how communication has to be managed, by each layer, in order to achieve the interoperability features required in the IoT.
- It also describes the actors (communicating elements) and the channel model for communication in IoT.

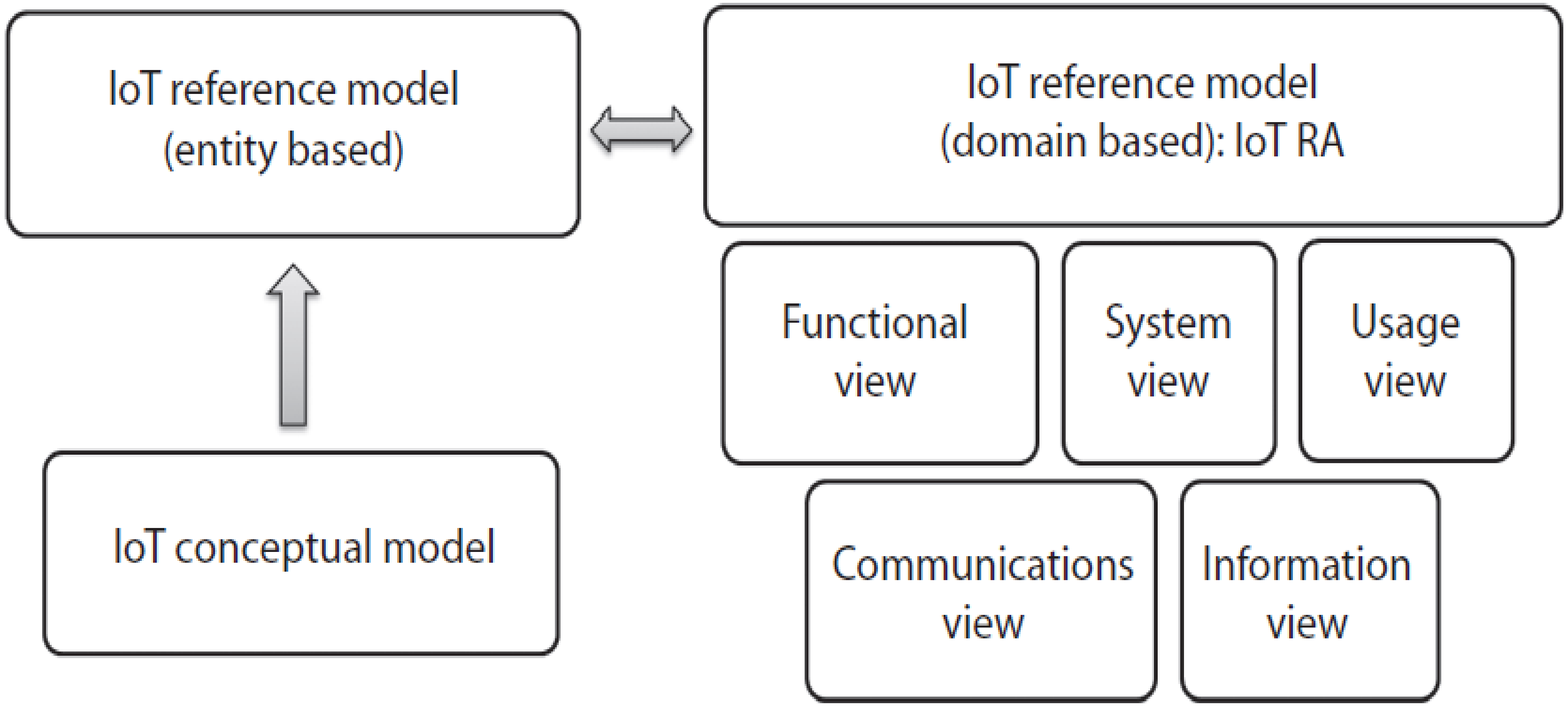
- The RA of IoT-A mainly consists of “views” and “perspectives,” which vary depending on the requirements of each specific application.
- Figure illustrates that the perspectives “evolution and interoperability,” “performance and scalability,” “trust, security, and privacy,” and “availability and resilience” are applied to all the views: the “functional” view, the “information” view, and the “deployment and operation” view, respectively.
- While applying perspectives to views, not every view is impacted by the perspectives in the same manner or grade. For example, the perspectives have a high impact when applied to the operation

IoT RA

- IoT RA, created by the ISO/IEC* (CD 30141), envisions the construction of an IoT system based on a generic IoT conceptual model (CM) that includes the most important characteristics and domains of IoT.
- Then, it uses the CM as a basis to create a high-level system-based RM.
- This reference model is, in turn, structured in five architectural views (functional view, system view, user view, information view, and communication view) from different perspectives, which compose the RA itself.
- Figure shows the relation between these three components (CM, RM, and RA).

- In essence, the IoT RA provides the basics to create a concrete system architecture.
- he IoT RA is considered an application-specific architecture or a “target system architecture” since the RAncan adapt to the requirements of a specific system, like agricultural system, smart home/building, smart city, and so forth.

Relation between CM, RM, and RA.



IEEE P2413

- IEEE P2413 is based on ISO/IEC/IEEE 42010:2011: “Systems and Software Engineering Architecture Description.”*
- The goal is not to create a new standard but to address common aspects of different application domains of the IoT.
- The IEEE working group is collaborating with ISO, ITU-T, and the Industrial Internet Consortium (IIC), among others, with the common goal of achieving better standards for the IoT in all its areas of application.
- The focus is on achieving interoperability, together with other quality attributes, such as protection, privacy, security, and safety.

Industrial Reference Architectures

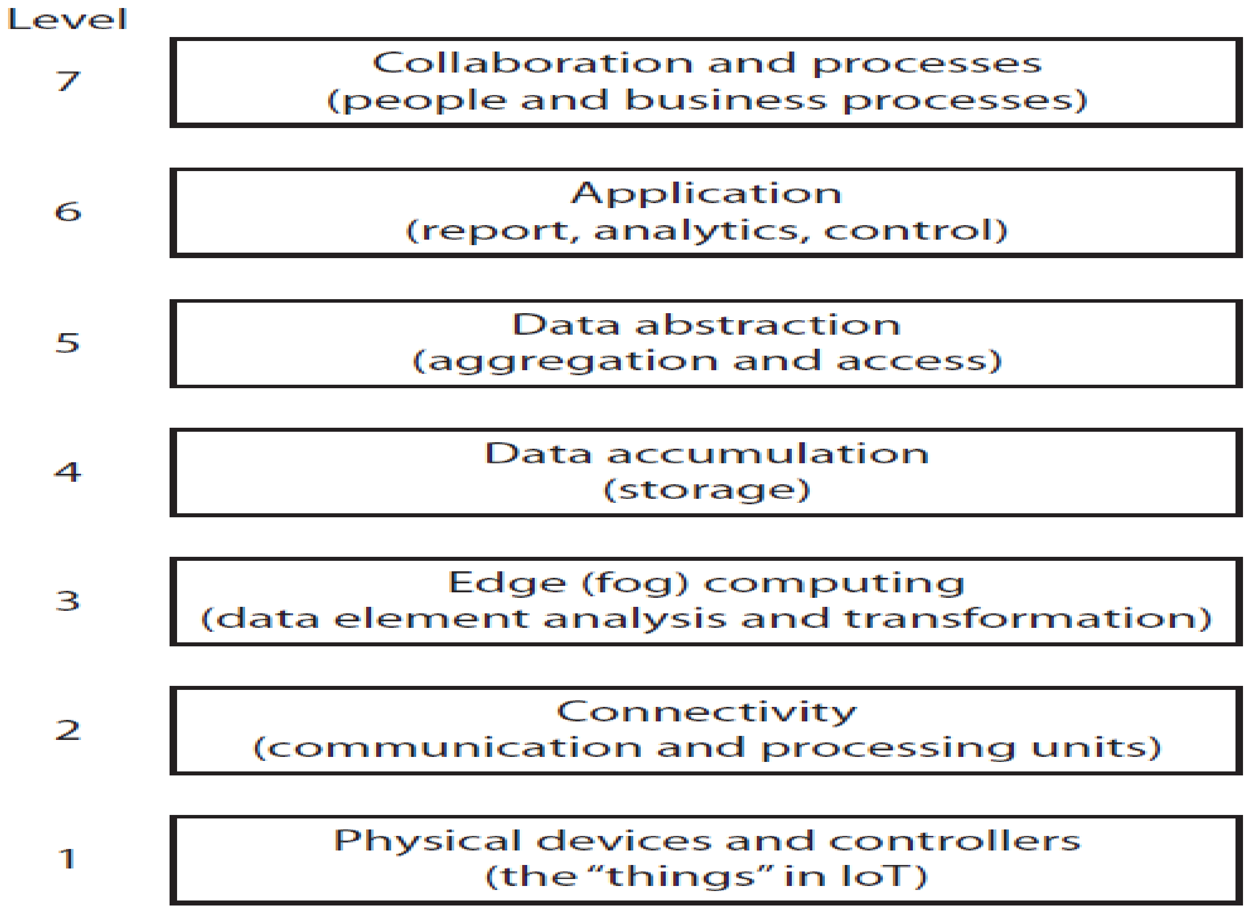
- The IIRA† is a standard-based open architecture for Industrial Internet Systems (IISs), proposed by the IIC Technology Working Group, whose members are companies like AT&T, Cisco, IBM, General Electric, and Intel.
- The Industrial Internet is considered an IoT system, enabling intelligent industrial operations and focusing on key characteristics for this type of systems: safety, security, and resilience. IISs cover energy, healthcare, manufacturing, the public sector, transportation, and related industrial systems

- The Industrial Internet Architecture Framework (IIAF) is based on ISO/IEC/IEEE 42010:2011, and as such, it uses the same constructs and common terms, such as viewpoints, concerns, and stakeholders, as well as views and models.‡
- The IIRA is the result of applying IIAF to the Industrial IoT systems
- . Table 1.1 shows an overview of the IIRA. Each viewpoint influences the viewpoints below it. In turn, lower viewpoints validate and sometimes cause revisions in the higher viewpoints.
- There are some crosscutting concerns, such as security and safety, which are discussed in other reports from the IIC.

Other Reference Models and Architectures for IoT
Cisco Reference Model

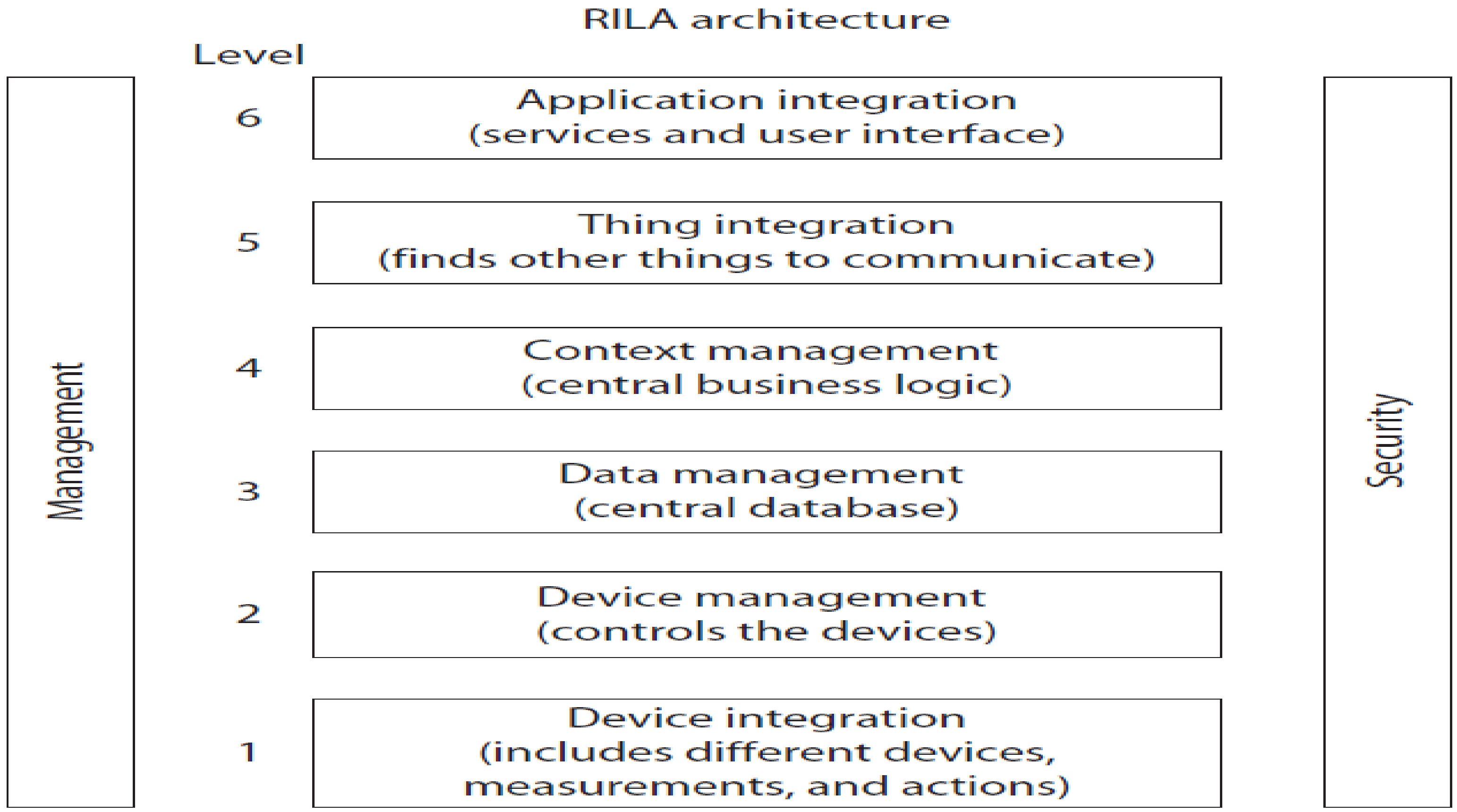
- In 2014, Cisco proposed a seven-layer RM (Cisco, 2014), which is represented in Figure , giving a more practical point of view.
- The lowest level includes the physical devices and controllers (the *things*); then there is connectivity and, above that, edge (fog) computing, where some initial aggregation, elimination of data duplication, and analysis can be carried out.
- The lower three levels, in turn, are considered operational technology (OT).
- The top four levels relate to the IT. The lowest level in the IT part of the stack is storage, and this is followed, going toward the top, by data abstraction, applications, and collaboration and (business) processes

IoT RM proposed by Cisco. (Adapted from Cisco)



Level	
7	Collaboration and processes (people and business processes)
6	Application (report, analytics, control)
5	Data abstraction (aggregation and access)
4	Data accumulation (storage)
3	Edge (fog) computing (data element analysis and transformation)
2	Connectivity (communication and processing units)
1	Physical devices and controllers (the “things” in IoT)

Reference IoT layered architecture



RILA architecture

Level

6 Application integration (services and user interface)

5 Thing integration (finds other things to communicate)

4 Context management (central business logic)

3 Data management (central database)

2 Device management (controls the devices)

1 Device integration (includes different devices, measurements, and actions)

Management

Security

Reference IoT Layered Architecture

- Every IoT RA must include some essential components, such as interoperability and integration components, context-aware computing techniques, and security guidelines for the whole architecture .
- The resulting proposed architecture is RILA. RILA is a more concrete architecture, intended to be easier to comprehend for customers and industry than the high-level IoT-A.
- It not only provides guidelines of how to put IoT-A in practice but also demonstrates that this architecture can really be implemented using actual use cases. RILA acts between things, devices, and the user.

- RILA consists of six layers, as depicted in Figure . Besides these layers, there are two cross section layers, “security” and “management,” that affect all other layers.
- The *device integration layer* includes all the different types of devices, receives their measurements, and communicates actions.
- This layer can be seen as a translator that speaks many languages .
- The output of the sensors and tags, as well as the input of the actuators, depends on the protocol they implement.

- The *device management layer* is responsible for receiving device registrations and sensor measurements from the device integration layer, and for communicating status changes for actuators to the device integration layer.
- Then, the device integration layer checks if the status change (i.e., the action) conforms with the respective actuator and translates the status change to the actuator.
- The device management layer controls the devices that are connected to the system; every change to a device’s registration, as well as new measurement data, should be communicated from the device integration layer to the device management layer, so the information can be updated and stored.

- Normally, the *data management layer* is a central database (but it can also be a data warehouse or even a complete data farm, in the case of larger IoT systems) that stores all data of a thing.
- Thus, the implementation of the data management layer strongly depends on the use case
- The *context management layer* defines the central business logic and is responsible for tasks like defining the goals of the thing, consuming and producing the context situations of the things, evaluating the context situation toward the goals,
- The *thing integration layer* is responsible for finding other things to communicate, verifies if communication with the new thing is possible, and is responsible for a registration mechanism.
- The *application integration layer* connects the user to the thing, being considered the service layer, or even a simple user interface.